

Bitcoin: A Peer-to-Peer Electronic Cash System

by Satoshi Nakamoto [2008/10/31](#)

Ndemanga

Ndalama zapa computer za anzawo ndi anzawo zimalola kuti malipiro a pa intaneti atumizidwe kuchokera kugulu lina kupita ku lina popanda kupita ku bungwe lazachuma. Ma signature a digital amapereka gawo la yankho, koma phindu lalikulu limatayika ngati munthu wina wodalirika akufunikabe kuti apewe kuwononga kawiri. Tikupereka njira yothetsera vuto la kugwiritsa ntchito ndalama kawiri pogwiritsa ntchito intaneti ya anzawo. Network imatsimikizira nthawi yochitira zinthu powathamangitsa muunyolo wokhazikika wa umboni wa ntchito, kupanga mbiri yomwe singasinthidwe popanda kubwerezano umboni wa ntchito. Unyolo wautali kwambiri sikuti umangokhala umboni wotsatizana wa zochitika zomwe zachitiridwa umboni, koma umboni wakuti zidachokera ku dziwe lalikulu kwambiri la mphamvu za CPU. Malingana ngati mphamvu zambiri za CPU zikuwongoleredwa ndi ma node omwe sagwirizana kuti awononge maukonde, amatulutsa owukira atali kwambiri komanso owukira kunja. Maukonde pawokha amafunikira kapangidwe kakang'ono. Mauthenga amaulutsidwa molimbika kwambiri, ndipo ma node amatha kuchoka ndikujowinanso maukonde pakufuna kwawo, kuvomereza unyolo wautali kwambiri wotsimikizira ntchito ngati umboni wa zomwe zidachitika atapita.

Mawu Oyamba

Malonda pa intaneti adalira kwambiri mabungwe azachuma omwe amagwira ntchito ngati anthu ena odalirika kuti azikonza zolipira pakompyuta. Ngakhale dongosololi limagwira ntchito bwino pazochita zambiri, limakhalabe ndi zofooka zamtundu wa trust based model. Zochita zosasinthika kwenikweni sizingatheke, chifukwa mabungwe azachuma sangapewe kuyimira mikangano. Mtengo wa mkhalapakati umachulukitsa ndalama zogulira, kuchepetsa kukula kwamalonda ndikuchepetsa kuthekera kwa zochitika zing'onozing'ono, ndipo pamakhala mtengo wokulirapo pakutayika kwa kuthekera kolipira kosabweza kwa ntchito zomwe sizingabwezedwe. Ndi kuthekera kwa kusinthika, kufunika kokhulupirira kumafalikira. Amalonda ayenera kusamala ndi makasitomala awo, kuwavutitsa kuti adziwe zambiri kuposa momwe akanafunira. Chinyengo china chachinyengo chimavomerezedwa kukhala chosapeŵeka. Kusatsimikizika kwamitengo iyi ndi zolipirira zitha kupewedwa pamasom'pamaso pogwiritsa ntchito ndalama zenizeni, koma palibe njira yolipirira njira yolumikizirana popanda munthu wodalirika.

Chofunikira ndi njira yolipirira pakompyuta yozikidwa paumboni wa cryptographic m'malo mokhulupirira, kulola maphwando awiri omwe ali okonzeka kuchita zinthu mwachindunji popanda

kufunikira kwa munthu wina wodalirika. Zochita zomwe sizingachitike kuti zisinthe zingateteze ogulitsa ku chinyengo, komanso njira zanthawi zonse za escrow zitha kukhazikitsidwa kuti ziteteze ogula. Mu pepalali, tikupereka yankho ku vuto la kugwiritsa ntchito ndalama kawiri pogwiritsa ntchito masitampu a anzawo ndi anzawo kuti apange umboni wokwanira wa dongosolo la zochitika. Dongosololi ndi lotetezeka bola ngati ma node okhulupilika pamodzi akuwongolera mphamvu zambiri za CPU kuposa gulu lililonse logwirizana la owukira.

Zochita

Timatanthauzira ndalama yamagetsi ngati siginecha ya digito. Mwiniwake aliyense amasamutsa ndalamayo kupita kwa wina posaina pa digito hashi ya zomwe zachitika m'mbuyomu ndi kiyi yapagulu ya mwini wake ndikuwonjezera izi kumapeto kwa ndalamazo. Wolipidwa akhoza kutsimikizira siginecha kuti atsimikizire kuchuluka kwa umwini.

Vuto ndiloti wolipirayo sangathe kutsimikizira kuti m'modzi mwa eni ake sanagwiritse ntchito ndalamazo kawiri. common solution ndi o yambitsani akuluakulu apakati odalirika, kapena timbewu ta timbewu tating'ono, timene timayang'anira zochitika zonse za kuwononga ndalama kawiri. Pambuyo pa malonda aliwonse, ndalamazo ziyenera kubwezeredwa ku timbewu tonunkhira. perekani ndalama yatsopano, ndipo ndalama zokhazo zoperekedwa mwachindunji kuchokera ku timbewu ta timbewu timene timakhulupirira kuti sizidzagwiritsidwa ntchito kawiri. Vuto ndi yankho ili ndikuti tsogolo la ndalama zonse zimatengera kampani yomwe ikuyendetsa timbewuting'onoting'o chilichonse chimwe chimayenera kuchitika monga bank.

Tikufuna njira yoti wolipidwa adziwe kuti eni ake am'mbuyomu sanasaine zomwe zachitika kale. Pazolinga zathu, kugulitsa koyambirira ndi komwe kumafunikira, kotero sitisamala za kuyesanso kuwononga kawiri. Njira yokhayo yotsimikizira kusakhalapo kwa malonda ndikuzindikira zochitika zonse. Muchitsanzo chokhazikitsidwa ndi timbewu ta timbewu ta timbewu ta timbewu ta timbewu ta timbewu ta timbewu ta timbewu timadzi timene timakhala tikudziwa zonse zomwe zimachitika ndipo adasankha zomwe zidafika poyamba. Kutu muchite izi popanda gulu lodalirika. zochitika ziyenera kulengezedwa poyera[1], ndipo tikufuna dongosolo kuti otenga nawo mbali agwirizane pa mbiri imodzi ya dongosolo lomwe adalandilidwa. Wolipidwa amafunikira umboni kuti panthawi yomwe ntchito iliyonse, ma node ambiri adavomereza kuti inali yoyamba kulandiridwa.

Seva ya Timestamp

Yankho lomwe timapereka limayamba ndi seva yanthawi yayitali. Seva ya timestamp imagwira ntchito potenga hashi ya block ya zinthu kuti zisinthidwe nthawi ndikufalitsa kwambiri hashi, monga m'nyuzipepala kapena positi ya Usenet[2-5]. The timestamp imatsimikizira kuti deta iyenera kuti inalipo panthawiyo, mwachiwonekere, kuti alowe mu hashi. Chidindo chilichonse chimakhala ndi sitampu yam'mbuyomu mu hashi yake, kupanga unyolo, ndi sitampu iliyonse yowonjezera yomwe imalimbitsa zomwe zidalipo kale.

Proof of Work

Kuti tigwiritse ntchito seva yapanthawi yogawidwa molingana ndi anzathu, tidzafunika kugwiritsa ntchito njira yotsimikizira ntchito yofanana ndi Adam Back's Hashcash[6], osati zolembe zamanyuzipepala kapena Usenet. Umboni wa ntchito umaphatikizapo kusanthula mtengo womwe ukakhala wofulumira, monga ndi SHA-256, hashi imayamba ndi ziro zingapo. Avereji ya ntchito yofunikira ndiyochulukirachulukira mu kuchuluka kwa ziro bits zofunika ndipo imatha kutsimikiziridwa pochita hashi imodzi.

Pa netiweki yathu ya sitampu yanthawi, timagwiritsa ntchito umboni wa ntchito powonjezera pang'ono mu block mpaka mtengo utapezeka womwe umapatsa block hash ziro bits zofunika. Khama la CPU litagwiritsidwa ntchito kuti likwaniritse umboni wa ntchito, chipikacho sichingasinthidwe popanda kuyambiranso ntchito. Monga midadada pambuyo pake amamangidwa unyolo pambuyo pake, ntchito yosintha chipikacho ingaphatikizapo kukonzanso midadada yonse pambuyo pake.

Umboni wa ntchito umathetsanso vuto lodziyimira pawokha popanga zisankho zambiri. Ngati ambiri adatengera IP-adilesi-imodzi-voti, zitha kusokonezedwa ndi aliyense wokhoza kugawa IPS yambiri. Umboni-wa-ntchito kwenikweni ndi CPU-voti imodzi. Chisankho chochuluka chikuyimiridwa ndi unyolo wautali kwambiri, womwe uli ndi chitsimikiziro chachikulu cha ntchito yomwe idayikidwamo. Ngati mphamvu zambiri za CPU zikuwongoleredwa ndi mfundo zowona mtima, unyolo wowona mtima umakula mwachangu ndikupitilira unyolo uliwonse womwe ukupikisana nawo. Kuti asinthe chipika chapitachi, wowukirayo amayenera kubwerezanso umboni wa block ndi midadada yonse pambuyo pake ndikugwira ndikuposa ntchito zamanodi oona mtima. Tidzawonetsa pambuyo pake kuti kuthekera kwa wowukira pang'onopang'ono kugwira kumachepa kwambiri ngati midadada yotsatira awonjezedwa.

Kulipiritsa kuwonjezereka kwa liwiro la hardware ndi chidwi chosiyana choyendetsa ma node pakapita nthawi, vuto la umboni wa ntchito limatsimikiziridwa ndi chiwerengero chosuntha cholunjika pa avareji. Chiwerengero cha midadada pa ola. Ngati apangidwa mwachangu kwambiri, zovuta zimawonjezeka.

Network

Njira zoyendetsera netiweki ndi izi:

1. Zochita zatsopano zimawulutsidwa ku node zonse.
2. Node iliyonse imasonkhanitsa zochitika zatsopano mu block.
3. Node iliyonse imagwira ntchito pakupeza umboni wovuta wa ntchito.

4. Node ikapeza umboni wa ntchito, imawulutsa chipika ku mfundo zonse block yake.
5. Node amavomereza chipika pokhapokha ngati zonse zomwe zili mmenemo zili zovomerezeka ndipo sizinagwiritsidwe ntchito kale.
6. Ma Node amasonyeza kuvomereza kwawo chipikacho pogwira ntchito popanga loko iunyolo, pogwiritsa ntchito hashi ya chipika chovomerezeka ngati hashi yapitayi.

Ma Node nthawi zonse amawona unyolo wautali kwambiri kukhala wolondola ndipo amayesetsa kuukulitsa. Ngati mfundo ziwiri zikuwulutsa mitundu yosiyanasiyana ya block yotsatira nthawi imodzi, ma node ena amatha kulandira imodzi kapena ina poyamba. Zikatero, amagwirirapo ntchito yoyamba imene analandira, koma nthambi inayo amasunga ngati ingatalike. Taye idzathyoledwa pamene umboni wotsatira wa ntchito ukupezeka ndipo nthambi imodzi imakhala yaitali, mfundo zomwe zinkagwira ntchito pa nthambi ina zidzasinthira ku yaitali. Kuwulutsa kwatsopano sikuyenera kufikira ma node onse.

Bola iwo akafika m'malo ambiri, amalowa mumdadada posakhalitsa. Mawayilesi a block nawonso amalolera za mauthenga ogwetsedwa. Ngati node sichilandira chipika, imapempha ikalandira chipika chotsatira ndikuzindikira kuti chinaphonya chimodzi.

Chilimbikitso

Mwamsonkhano, kugulitsa koyamba mu chipika ndikugulitsa kwapadera komwe kumayambitsa ndalama zatsopano za mlengi wa block. Izi zimawonjezera chilimbikitso kwa ma node kuti athandizire netiweki. ndipo imapereka njira yogawira ndalama zachitsulo poyambira, popeza palibe ulamuliro wapakati wozipereka. Kuwonjezedwa kosalekeza kwa ndalama zachitsulo zatsopano ndizofanana ndi ochita migodi a golide omwe amawononga chuma kapena kuwonjezera golide pakuyenda. Kwa ife, ndi nthawi ya CPU ndi magetsi omwe amagwiritsidwa ntchito.

Chilimbikitso chingathenso kulipidwa ndi ndalama zogulira. Ngati mtengo wamtengo wapatali wa malondawo ndi wocheperapo kusiyana ndi mtengo wake wolowa, kusiyana kwake ndi ndalama zogulitsira zomwe zimawonjezedwa kumtengo wolimbikitsa wa block yomwe ili ndi malondawo. Ndalama zodziwikiratu zikayamba kugwiritsidwa ntchito, chilimbikitsocho chikhoza kusinthiratu kupita ku chindapusa ndikukhala wopanda inflation.

Chilimbikitso chingathandize kulimbikitsa ma node kukhala oona mtima. Ngati wachiwembu wadyera angathe kusonkhanitsa mphamvu zambiri za CPU kuposa ma node onse oona mtima, ayenera kusankha pakati pa kuzigwiritsa ntchito pobera anthu malipiro ake, kapena kuzigwiritsa ntchito popanga ndalama zatsopano. Ayenera kuona kukhala kopindulitsa kwambiri kusewera ndi malamulo, malamulo oterowo omwe amam'patsa ndalama zachitsulo zatsopano kuposa wina aliyense ataphatikizidwa, kusiyana ndi kuwononga dongosolo ndi kudalirika kwa chuma chake.

Kubwezeretsanso malo a Disk

Zomwe zachitika posachedwa mu ndalama zimakwiridwa pansu pa midadada yokwanira, zomwe

zidagwiritsidwa ntchito zisanatayidwe kuti zisunge malo a disk. Kuti izi zitheke popanda kuthyola hashi ya chipikacho, zogulitsa zimathamangitsidwa mu Mtengo wa Merkle [7] [2] [5], ndi muzu wokhawo womwe umaphatikizidwa mu hashi ya chipikacho. midadada yakale ikhoza kupangidwa podula nthambi za mtengo. Ma hashes amkati safunikira kusungidwa.

Mutu wa block wopanda zosintha ungakhale pafupifupi ma 80 byte. Ngati tikuganiza kuti midadada imapangidwa mphindi 10 zilizonse, ma byte $80 * 6 * 24 * 365 = 4.2\text{MB}$ pachaka. Ndi makina apakompyuta omwe amagulitsidwa ndi 2GB ya RAM kuyambira 2008, ndi Malamulo a Moore akuloseka za kukula kwa 1.2GB pachaka, kusungirako sikuyenera kukhala vuto ngakhale mitu ya block iyenera kukumbukiridwa.

Kutsimikizira Malipiro Osavuta

Ndizotheka kutsimikizira zolipira popanda kugwiritsa ntchito node yonse ya netiweki. Wogwiritsa amangofunika kusunga zolembe zam'ma block za unyolo wautali kwambiri wotsimikizira ntchito, womwe atha kuupeza pofunsa ma node a netiweki mpaka atatsimikiza kuti ali ndi unyolo wautali kwambiri, ndikupeza nthambi ya Merkle yolumikiza malondawo ndi chipikacho. ndi timestamped mu. Iye sangathe fufuzani ndikuchita yekha, koma kugwirizana ndi malo mu unyolo, iye akhoza kuona kuti maukonde mfundo wavomereza izo, ndi midadada anawonjezera pambuyo zina kutsimikizira maukonde walandira izo.

Momwemonso, chitsimikizirocho ndi chodalirika malinga ngati ma node owona mtima akuwongolera maukonde, koma amakhala pachiwopsezo kwambiri ngati maukonde agonjetsedwa ndi wowukira. Ngakhale ma netiweki atha kudzitsimikizira okha zomwe zachitika, njira yophweka imatha kupusitsidwa ndi zochitika zopeka za wowukirayo malinga ngati wowukirayo apitilize kugonjetsa netiweki. Njira imodzi yodzitetezera ku izi ingakhale kuvomereza zidziwitso kuchokera ku node zapaintaneti pamene awona chipika chosavomerezeka, zomwe zimachititsa kuti pulogalamu ya wosuta itulutse chipika chonse ndi kuchenjeza zochitika kuti zitsimikizire kusagwirizana. Mabizinesi omwe amalandila ndalama pafupipafupi adzafunabe kuyendetsa ma node awo kuti akhale odziyimira pawokha komanso kuti atsimikizire mwachangu.

Kuphatikiza ndi Kugawa Mtengo

Ngakhale kuti zingakhale zotheka kugwiritsa ntchito ndalama zachitsulo payokha, sikungakhale kovuta kupanga malonda osiyana pa senti iliyonse posamutsa. Kuti mtengo ugawidwe ndikuphatikizidwa, zochitika zimakhala ndi zolowetsa ndi zotuluka zingapo. Nthawi zambiri pamakhala kulowetsa kumodzi kuchokera kuzinthu zazikulu zam'mbuyomu kapena zolowetsa zingapo kuphatikiza ndalama zing'onozing'ono, komanso zotuluka ziwiri: imodzi yolipira, ndi ina yobwezera zosintha, ngati zilipo, kubwerera kwa wotumiza.

Tiyenera kudziwa kuti fan-out, pomwe kugulitsa kumadalira zochitika zingapo, ndipo zomwe zimachitika zimadalira zina zambiri, si vuto pano. Sipafunikanso kutulutsa mbiri yodziyimira yokha yambiri yamalonda.

Zazinsinsi

Mabanki achikhalidwe amakwaniritsa chinsinsi pochepetsa mwayi wopeza zidziwitso kwa omwe akukhudzidwa ndi anthu ena odalirika. Kufunika kolengeza zochitika zonse poyera kumalepheretsa njirayi, koma chinsinsi chikhoza kusungidwabe pophwanya kufalikira kwa chidziwitso kumalo ena: posunga makiyi a anthu onse mosadziwika. Anthu amatha kuwona kuti wina akutumiza ndalama kwa munthu wina, koma popanda chidziwitso cholumikizira: aliyense. Izi ndizofanana ndi kuchuluka kwa chidziwitso chomwe chimatulutsidwa ndi kusinthanitsa katundu, kumene nthawi ndi kukula kwa malonda a munthu payekha, "tepi", amapangidwa poyera, koma osauza omwe maphwandowo anali.

Monga chowotcha chowonjezera chowonjezera, makiyi atsopano ayenera kugwiritsidwa ntchito pazochita zilizonse kuchokera pakulumikizidwa ndi eni ake wamba. Kulumikizana kwina sikungalephereke ndi zolowetsa zambiri, zomwe zimawonetsa kuti zolowa zawo zinali za eni ake. Choopsa ndi chakuti ngati mwini wake wa kiya awululidwa, kulumikiza kungavumbulutse zochitika zina zomwe zinali za mwiniwakeyo.

Kuwerengera

Timalingalira zochitika za wowukira akuyesera kupanga unyolo wina mwachangu kuposa unyolo wowona mtima, Ngakhale izi zitakwaniritsidwa, sizimatsegula dongosolo kuti lisinthe mosasamala, monga kupanga phindu kuchokera kumlengalenga kapena kutenga ndalama zomwe sizinali zake. t wowukira. Ma Node sangavomereze kugulitsa kosavomerezeka ngati malipiro, ndipo ma node oona mtima sangavomereze chipika chomwe chili nawo. Wowukira atha kungoyesa kusintha chimodzi mwazomwe adachita kuti abweze ndalama zomwe adawononga posachedwa.

Mpikisano pakati pa unyolo wowona mtima ndi unyolo wowukira ukhoza kudziwika ngati Binomial Random Walk. Chochitika chopambana ndi unyolo wowona mtima womwe ukukulitsidwa ndi chipika chimodzi, ndikuwonjezera kutsogola kwake ndi +1, ndipo cholephera ndi unyolo wa owukirawo womwe umakulitsidwa ndi chipika chimodzi, kuchepetsa kusiyana ndi -1.

Kuthekera kwa wowukirayo kutengera kupereŵera komwe kwapatsidwa kumafanana ndi a Gambler kuwononga vuto. Tiyerekeze kuti wotchova njuga yemwe ali ndi ngongole zopanda malire amangoyamba kupereŵera ndipo amaseŵera mwina chiwerengero chosawerengeka cha mayesero kuti ayesetse kuti GB awonongeke. Titha kuwerengera mwayi womwe angakumane

nawo, kapena kuti wowukirayo angakumane ndi owona mtima unyolo, motere[8]:

p = mwayi wowona mtima upeza block

q = kutheka kuti wowukirayo apeza mwayi wotsatira wa block

q_z = kuti wowukirayo apeze z blocks behind

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

Poganizira maganizo athu kuti $p > q$

, kuthekera kumatsika mokulirapo pomwe kuchuluka kwa midadada yomwe wowukirayo akuyenera kuthana nayo pakuwonjezeka. Ndizovuta zotsutsana naye, ngati sapanga mwayi wopita patsogolo, mwayi wake umakhala wochepa kwambiri pamene akugwera kumbuyo.

Tsopano tikuganizira utali woti wolandira ntchito yatsopano adikire nthawi yayitali asanatsimikize kuti wotumizayo sangasinthe ntchito. Tikuganiza kuti wotumizayo ndi wachiwembu yemwe akufuna kupangitsa wolandirayo kukhulupirira kuti adamulipira kwakanthawi, kenako nkusintha kuti abweze kwa iye pakapita nthawi. Wolandira adzachenjezedwa izi zikachitika, koma wotumizayo akuyembekeza kuti kuchedwa.

Wolandirayo amapanga makiyi atsopano ndipo amapereka kiyi yapagulu kwa wotumiza posachedwa kusaina. Izi zemalepheretsa wotumizayo kukonzekera midadada yambiri pasadakhale pogwira ntchito pa izo mosalekeza mpaka iye ali ndi mwayi wokwanira kuti apite patsogolo mokwanira, ndiyeno kupha transaction panthawiyo. Ntchito ikatumizidwa, wotumiza wachinyengo amayamba chinsinsi chogwira ntchito pa unyolo wofanana womwe uli ndi mtundu wina wamalonda ake.

Wolandirayo amadikirira mpaka malonda awonjezedwe ku block ndipo z blocks akhala olumikizidwa pambuyo pake. Sakudziwa kuchuluka kwake komwe wowukirayo wapanga, koma poganiza kuti midadada yowona mtima idatenga nthawi yomwe ikuyembekezeka pa block iliyonse, kupita patsogolo kwa wowukirayo kudzakhala kugawa kwa Poisson komwe kumayembekezeredwa:

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

Kuti tipeze mwayi woti wowukirayo atha kugwirabe, timachulukitsa kuchuluka kwa Poisson pakupita patsogolo kulikonse komwe akanatha kuchita ndi mwayi womwe adatha mfundo imeneyo:

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

Kukonzekeranso kupewa kufotokoza mwachidule mchira wopandamalire wa kugawa...

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

Kusintho kukhala C kodi....

```
#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;
}
```

Potsatira zotsatira zina, tittha kuwona kutsika kwakukulu ndi z.

```
q=0.1
z=0    P=1.00000000
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=1.00000000
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
```


$z=50$ $P=0.0000006$

Solving for P less than 0.1%...

$P < 0.001$

$q=0.10$ $z=5$

$q=0.15$ $z=8$

$q=0.20$ $z=11$

$q=0.25$ $z=15$

$q=0.30$ $z=24$

$q=0.35$ $z=41$

$q=0.40$ $z=89$

$q=0.45$ $z=340$

Mapeto

Takonzwa dongosolo la zochitika pakompyuta popanda kudalira chidaliro. Tinayamba ndi ndondomeko yanthawi zonse ya ndalama zopangidwa kuchokera ku siginecha za digito, zomwe zimapereka ulamuliro wamphamvu wa umwini, koma ndi zosakwanira popanda njira yopewera kuwononga kawiri. Kuti tithane ndi izi, tidakonzwa zoti pakhale ma netiweki a anzawo ndi anzawo pogwiritsa ntchito umboni wa ntchito kuti alembe mbiri yapagulu ya zochitika zomwe zimachitika mwachangu kuti woukirayo asinthe. Node oona mtima amawongolera mphamvu zambiri za CPU. Maukonde ndi olimba mu kuphweka kwake kosakonzedwa Node zimagwira ntchito zonse mwakamodzi popanda kulumikizana pang'ono. Iwo safunikira kuzindikiridwa, popeza kuti mauthenga samatumizidwa kumalo enaake ndipo amangofunikira kuperekedwa kokha mwa khama. Ma Node amatha kuchoka ndikujowinanso maukonde pakufuna kwawo, kuvomereza unyolo wotsimikizira ntchito ngati umboni wa zomwe zidachitika atapita. Amavota ndi mphamvu zawo za CPU, kuwonetsa kuvomereza kwawo midadada yovomerezeka poyesetsa kukulitsa ndikukana midadada yosavomerezeka pokana kuigwira. Malamulo ndi zolimbikitsa zilizonse zofunika zitha kutsatiridwa ndi mgwirizanowu.

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.