Bitcoin: Peer-to-Peer Fedha za elektroniki Mfumo

na Satoshi Nakamoto 2008/10/31

Uhangalizi

Toleo la rika-kwa-rika la pesa taslimu za elektroniki litaruhusu malipo ya mkondoni kutumwa moja kwa moja kutoka chama kimoja hadi kingine bila kupitia taasisi ya kifedha. Digital saini hutoa sehemu ya suluhisho, lakini faida kuu hupotea ikiwa mtu wa tatu anayeaminika ni bado inahitajika kuzuia matumizi mara mbili. Tunapendekeza suluhisho kwa matumizi mawili tatizo kutumia mtandao wa wenzao. Muhtasari wa muhuri wa miamala kwa kutumia hashing kuwaingiza kwenye mlolongo unaoendelea wa uthibitisho-wa-kazi, kutengeneza rekodi ambayo haiwezi kuwa ilibadilishwa bila kufanya tena uthibitisho wa kazi. Mlolongo mrefu zaidi sio tu unathibitisha mlolongo wa hafla zilizoshuhudiwa, lakini ushahidi kwamba ilitoka kwa dimbwi kubwa zaidi la nguvu ya CPU. Kama kwa muda mrefu kama nguvu nyingi za CPU zinadhibitiwa na nodi ambazo hazishirikiani kushambulia mtandao, watatoa mlolongo mrefu zaidi na washambuliaji wa nafasi. Mtandao wenyewe unahitaji muundo mdogo. Ujumbe hutangazwa kwa msingi bora wa juhudi, na nodi zinaweza kuondoka na jiunge tena na mtandao kwa mapenzi, ukikubali mnyororo mrefu zaidi wa uthibitisho wa kazi kama uthibitisho wa nini ilitokea wakati walikuwa wameenda.

Utangulizi

Biashara kwenye mtandao imekuwa ikitegemea karibu taasisi za kifedha kutumika kama wahusika wa tatu kusindika malipo ya elektroniki. Wakati mfumo unafanya kazi vizuri ya kutosha kwa shughuli nyingi, bado inakabiliwa na udhaifu wa asili wa uaminifu mfano. Shughuli zisizoweza kurejeshwa kabisa haziwezekani, kwani ni ya kifedha taasisi haziwezi kuzuia usuluhishi wa mabishano. Gharama ya upatanishi huongeza shughuli gharama, kupunguza kiwango cha chini cha ununuzi wa vitendo na kukata uwezekano wa ndogo shughuli za kawaida, na kuna gharama pana katika upotezaji wa uwezo wa kufanya isigeuke malipo ya huduma ambazo hazibadiliki. Pamoja na uwezekano wa kubadilika, hitaji la uaminifu huenea. Wafanyabiashara lazima wawe na wasiwasi na wateja wao, wakiwashtaki kwa habari zaidi kuliko vile wangehitaji. Asilimia fulani ya ulaghai inakubaliwa kuwa haiwezi kuepukika. Gharama hizi na kutokuwa na uhakika wa malipo kunaweza kuepukwa kwa kibinafsi kwa kutumia mwili sarafu, lakini hakuna utaratibu wowote wa kufanya malipo juu ya kituo cha mawasiliano bila chama cha kuaminika.

Kinachohitajika ni mfumo wa malipo wa elektroniki kulingana na uthibitisho wa kriptografia badala ya uaminifu, kuruhusu vyama vyovyote vyenye nia ya kufanya moja kwa moja na kila mmoja bila hitaji la mtu wa tatu anayeaminika. Uuzaji ambao hauwezekani kwa hesabu kugeuza ungekuwa

kulinda wauzichadji kutoka kwa ulaghai, na mifumo ya kawaida ya escrow inaweza kutekelezwa kwa urahisi linda wanunuzi. Katika jarida hili, tunapendekeza suluhisho la shida ya matumizi mara mbili kwa kutumia rika-kwa-rika ilisambaza seva ya muhuri wa muda ili kutoa uthibitisho wa hesabu wa mpangilio wa shughuli. Mfumo huo uko salama ili mradi kama nodi za uamini kudhibiti kwa pamoja nguvu zaidi ya CPU kuliko kikundi chochote kinachoshirikiana cha nodi za washambuliaji.

Miamala

Tunafafanua sarafu ya elektroniki kama mlolongo wa saini za dijiti. Kila mmiliki huhamisha sarafu ijayo kwa kusaini dijiti hashi ya manunuzi ya awali na ufunguo wa umma wa mmiliki wa pili na kuongeza hizi hadi mwisho wa sarafu. Mlipaji anaweza kuthibitisha saini kwa thibitisha mlolongo wa umiliki.

Shida ni kwamba mpokeaji hawezi kudhibitisha kuwa mmoja wa wamiliki hakutumia mara mbili sarafu. Suluhisho la kawaida ni kuanzisha mamlaka kuu inayoaminika, au mnanaa, ambayo huangalia kila shughuli kwa matumizi mara mbili. Baada ya kila shughuli, sarafu lazima irudishwe mnara kutoa sarafu mpya, na sarafu tu zilizotolewa moja kwa moja kutoka kwa mnanaa zinaaminika sio tumia mara mbili. Shida na suluhisho hili ni kwamba hatima ya mfumo mzima wa pesa inategemea kampuni inayoendesha mnanaa, na kila shughuli inapaswa kupitia kama benki.

Tunahitaji njia ya mlipaji kujua kwamba wamiliki wa zamani hawakusaini mapema yoyote shughuli. Kwa madhumuni yetu, shughuli ya mwanzo ndio inayohesabiwa, kwa hivyo hatufanyi hivyo kujali juu ya majaribio ya baadaye ya kutumia mara mbili. Njia pekee ya kuthibitisha kutokuwepo kwa a shughuli ni kujua shughuli zote. Katika mtindo wa msingi wa mnanaa, mnanaa alikuwa akijuashughuli zote na kuamua ni yupi aliyefika kwanza. Kukamilisha hii bila chama cha kuaminika, shughuli lazima zitangazwe hadharani [1], na tunahitaji mfumo wa washiriki kukubali kwenye historia moja ya utaratibu ambao walipokelewa. Mlipaji anahitaji uthibitisho kuwa saa wakati wa kila shughuli, sehemu nyingi zilikubaliana kuwa ndio kwanza ilipokelewa.

Seva ya muhuri wa wakati

Suluhisho tunalopendekeza linaanza na seva ya timestamp. Seva ya timestamp inafanya kazi na kuchukua hash ya kizuizi cha vitu kuwa na muhuri wa wakati na kuchapisha hashi, kama vile katika gazeti au chapisho la Usenet [2-5]. Timestamp inathibitisha kuma data lazima ilikuwapo wakati huo, ni wazi, ili kuingia kwenye hashi. Kila timestamp inajumuisha ya awali timestamp katika hash yake, kutengeneza mlolongo, na kila muhuri wa nyongeza unaimarisha hizo mbele yake.

Uthibitisho wa Kazi

Ili kutekeleza seva iliyosambazwa ya timestamp kwa msingi wa rika-kwa-rika, tutahitaji kutumia mfumo wa uthibitisho wa kazi sawa na Hashcash ya Adam Back [6], badala ya gazeti au Usenet machapisho. Uthibitisho-wa-kazi unajumuisha skanning ya thamani ambayo inapoharibiwa, kama vile na SHA-256, hashi huanza na idadi ya sifuri. Kazi ya wastani inayohitajika ni ufafanuzi katika idadi ya bits sifuri inahitajika na inaweza kuthibitishwa kwa kutekeleza mojahash.

Kwa mtandao wetu wa timestamp, tunatekeleza uthibitisho-wa-kazi kwa kuongeza nonce katika kuzuia mpaka thamani ipatikane ambayo inapeana hashi ya kuzuia bits zinazohitajika sifuri. Mara CPU juhudi imetumika kuifanya itosheleze uthibitisho wa kazi, kizuizi hakiwezi kubadilishwa bila kufanya upya kazi. Kama vizuizi vya baadaye vimefungwa minyororo baada yake, kazi ya kubadilisha kuzuia ni pamoja na kufanya upya vitalu vyote baada yake.

Uthibitisho wa kazi pia hutatua tatizo la kuamua uwakilishi katika uamuzi wa wengi kutengeneza. Ikiwa wengi waliegemea kwenye-IP-anwani-kura-moja, inaweza kupotoshwa na mtu yeyote anayeweza kutenga IP nyingi. Uthibitisho wa kazi kimsingi ni CPU-kura moja. Uamuzi wa wengi unawakilishwa na mlolongo mrefu zaidi, ambao una uthibitisho mkubwa zaidi wa kazi juhudi zilizowekwa ndani yake. Ikiwa nguvu nyingi za CPU zinadhibitiwa na nodi za uaminifu, waaminifu mnyororo utakua kwa kasi zaidi na kupita minyororo yoyote inayoshindana. Ili kurekebisha kizuizi cha zamani, amshambulizi atalazimika kufanya tena uthibitisho wa kazi ya kizuizi na vizuizi vyote baada yake na kasha catch up na kuvuka kazi ya nodi waaminifu. Tutaonyesha kwamba baadaye. Uwezekano wa mshambulizi polepole kupatana hupungua kwa kasi kama vizuizi vinavyofuata zinaongezwa.

Ili kufidia kuongeza kasi ya maunzi na maslahi tofauti ya kuendesha nodi wakati, ugumu wa uthibitisho wa kazi huamuliwa na wastani wa kusonga unaolenga wastani idadi ya vitalu kwa saa. Ikiwa zinazalishwa haraka sana, ugumu huongezeka.

Network

Hatua za kuendesha mtandao ni kama ifuatavyo:

1. Shughuli mpya zinatangazwa kwa nodi zote.
2. Kila nodi inakusanya shughuli mpya kwenye kizuizi.
3. Kila nodi inafanya kazi katika kutafuta uthibitisho mgumu wa kazi kwa kizuizi chake.
4. Wakati nodi inapata uthibitisho wa kazi, inatangaza kizuizi kwa nodi zote.
5. Nodi kukubali kuzuia tu kama shughuli zote ndani yake ni halali na si tayari kutumika.
6. Nodi zinaonyesha kukubali kwao kwa kizuizi kwa kufanya kazi katika kuunda kizuizi kinachofuata mnyororo, kwa kutumia heshi ya kizuizi kilichokubaliwa kama heshi iliyotangulia.

Nodi kila wakati huzingatia mnyororo mrefu zaidi kuwa ndio sahihi na itaendelea kufanya kazi kuipanua. Ikiwa nodi mbili zitatangaza matoleo tofauti ya kizuizi kinachofuata kwa wakati mmoja, zingine nodi zinaweza kupokea moja au nyingine kwanza. Katika kesi hiyo, wanafanya kazi kwa kwanza wao imepokelewa, lakini hifadhi tawi lingine ikiwa litakuwa refu. Tai itavunjwa lini uthibitisho unaofuata wa kazi unapatikana na tawi moja linakuwa refu; nodi zilizokuwa kufanya kazi kwenye branch lingine basi itabadilika kuwa refu zaidi. Matangazo mapya ya shughuli si lazima yafikie nodi zote. Ilimradi wao kufikia nodi nyingi, wataingia kwenye kizuizi kabla ya muda mrefu.

Matangazo ya kuzuia pia yanastahimili ya meseji zilizodondoshwa. Ikiwa nodi haipati kizuizi, itaomba wakati inapokea kuzuia inayofuata na kugundua ilikosa moja.

Motisha

Kwa makubaliano, shughuli ya kwanza katika kuzuia ni shughuli maalum ambayo huanza sarafu mpya inayomilikiwa na muundaji wa kuzuia. Hii inaongeza motisha kwa nodi kusaidia mtandao, na hutoa njia ya awali ya kusambaza sarafu katika mzunguko, kwa kuwa hakuna kati mamlaka ya kuzitoa. Aidha ya kutosha ya mara kwa mara ya kiasi cha sarafu mpya ni sawa na wachimbaji dhahabu wanaotumia rasilimali kuongeza dhahabu kwenye mzunguko. Kwa upande wetu, ni Muda wa CPU na umeme unaotumika.

Motisha pia inaweza kufadhiliwa na ada za muamala. Ikiwa thamani ya pato la shughuli nichini ya thamani yake ya ingizo, tofauti ni ada ya muamala ambayo huongezwa kwa motisha thamani ya kizuizi kilicho na shughuli. Mara baada ya imara idadi ya sarafu na aliingia katika mzunguko, motisha inaweza mpito kabisa kwa ada ya manunuzi na kuwa kabisa bila mfumuko wa bei.

Motisha inaweza kusaidia kuhimiza nodi kukaa waaminifu. Ikiwa mshambuliaji mwenye tamaa anaweza kukusanyika nguvu zaidi ya CPU kuliko nodi zote za uaminifu, angelazimika kuchagua kati yakuitumia kuwalaghai watu kwa kuiba malipo yake, au kuitumia kutengeneza sarafu mpya. Anapaswa kupata faida zaidi kucheza na sheria, sheria kama hizo ambazo zinampendelea zaidi sarafu mpya kuliko kila mtu mwingine pamoja, kuliko kudhoofisha mfumo na uhalali wa utajiri wake mwenyewe.

Kurudisha Nafasi ya Diski

Mara baada ya shughuli ya hivi karibuni katika sarafu kuzikwa chini ya vitalu vya kutosha, shughuli zilizotumika kabla ya kutupwa ili kuhifadhi nafasi ya diski. Ili kuwezesha hili bila kuvunja kuzuia hashi, miamala huharakishwa katika Mti wa Merkle [7][2][5], na mzizi pekee umejumuishwa kwenye hash ya kuzuia. Kuzuia vya zamani vinaweza kuunganishwa kwa kukata matawi ya mti. Hashes za ndani hufanya hazihitaji kuhifadhiwa.

Kichwa cha kuzuia kisicho na miamala kitakuwa takriban baiti 80. Ikiwa tunadhani kuzuia

yanayotokana kila dakika 10, 80 baiti * 6 * 24 * 365 = 4.2MB kwa mwaka. Na kompyuta mifumo ya kawaida inauzwa na 2GB ya RAM kama ya 2008, na Sheria ya Moore inayotabiri sasa ukuaji wa 1.2GB kwa mwaka, hifadhi haipaswi kuwa tatizo hata kama vichwa vya kuzuia vinapashwa kuwekwa kwenye kumbukumbu.

Uthibitishaji wa Malipo Uliorahisishwa

Inawezekana kuthibitisha malipo bila kuendesha nodi kamili ya mtandao. Mtumiaji anahitaji tu weka nakala ya vichwa vya kuzuia vya mlolongo mrefu zaidi wa uthibitisho wa kazi, ambao anaweza kupata kuhoji nodi za mtandao hadi athibitishwe kuwa ana msururu mrefu zaidi, na kupata Merkle branch linalounganisha muamala kwenye kizuizi ambacho umetiwa muhuri wa wakati. Hawezi kuangalia muamala kwa ajili yake mwenyewe, lakini kwa kuiunganisha na mahali kwenye mlolongo, anaweza kuona kwamba nodi ya mtandao ina iliikubali, na vizuizi vilivyoongezwa baada ya kuthibitisha zaidi mtandao umeikubali.

Kwa hivyo, uthibitishaji ni wa kuaminika mradi tu nodi za uaminifu zidhibiti mtandao, lakini ni zaidi hatarini iwapo mtandao ukizidiwa nguvu na mshambulizi. Wakati nodi za mtandao zinaweza kuthibitisha shughuli zao wenyewe, njia iliyorahisishwa inaweza kudanganywa na mshambulizi iliyoundwa shughuli kwa muda mrefu kama mshambuliaji anaweza kuendelea kuushinda mtandao. Mkakati mmoja kulinda dhidi ya hii itakuwa kukubali arifa kutoka kwa nodi za mtandao wakati wanagundua kizuizi batili, kinachosababisha programu ya mtumiaji kupakua kizuizi kamili na kuarifiwa shughuli za kuthibitisha kutokwenda. Biashara zinazopokea malipo ya mara kwa mara zitapokealabda bado wanataka kuendesha nodi zao kwa usalama huru zaidi na haraka uthibitishaji.

Kuchanganya na Kugawanya Thamani

Ingawa itawezekana kushughulikia sarafu kibinafsi, itakuwa ngumu kutengeneza muamala tofauti kwa kila senti katika uhamisho. Ili kuruhusu thamani kugawanywa na kuunganishwa, miamala ina pembejeo na matokeo mengi. Kwa kawaida kutakuwa na pembejeo moja kutoka kwa muamala mkubwa wa awali au pembejeo nyingi zinazochanganya kiasi kidogo, na zaidi matokeo mawili: moja kwa ajili ya malipo, na moja kurudisha mabadiliko, kama yapo, kurudi kwa mtumaji.

Ikumbukwe kwamba shabiki-nje, ambapo shughuli inategemea shughuli kadhaa, na shughuli hizo zinategemea nyingi zaidi, sio shida hapa. Kamwe hakuna haja ya toa nakala kamili ya pekee ya historia ya muamala.

Faragha

Mtindo wa kitamaduni wa benki hufikia kiwango cha faragha kwa kuzuia ufikiaji wa habari kwa pande zinazohusika na mtu wa tatu anayeaminika. Umuhimu wa kutangaza shughuli zote inazuia hadharani njia hii, lakini faragha bado inaweza kudumishwa kwa kuvunja mtiririko wa habari mahali pengine: kwa kuweka funguo za umma bila majina. Umma unaweza kuona hilo mtu anatuma kiasi kwa mtu mwingine, lakini bila maelezo ya kuunganisha muamala kwa mtu yeyote. Hii ni sawa na kiwango cha habari iliyotolewa na hisa kubadilishana, ambapo muda na ukubwa wa biashara ya mtu binafsi, "mkanda", ni kwa umma, lakini bila kueleza vyama ni akina nani.

Kama ngome ya ziada, jozi mpya ya vitufe inapaswa kutumika kwa kila shughuli ili kuziweka kutoka kwa kuhusishwa na mmiliki wa kawaida. Baadhi ya kuunganisha bado hakuwezi kuepukika kwa pembejeo nyingi shughuli, ambazo lazima zifichue kwamba pembejeo zao zilimilikiwa na mmiliki mmoja. Hatari ni kwamba ikiwa mmiliki wa ufunguo utafichuliwa, kuunganisha kunaweza kufichua miamala mingine ambayo ilikuwa ya mmiliki mmoja.

Mahesabu

Tunazingatia hali ya mshambulizi anayejaribu kutengeneza msururu mbadala kwa haraka zaidi kuliko mlolongo wa uaminifu. Hata kama hii imekamilika, haitoi mfumo wazi kwa kiholela mabadiliko, kama vile kuunda thamani kutoka kwa hewa nyembamba au kuchukua pesa ambazo hazikuwa za mshambuliaji. Nodi hazitakubali muamala batili kama malipo, na nodi za uaminifu haitakubali kamwe kizuizi kilicho nazo. Mshambulizi anaweza tu kujaribu kubadilisha moja yake shughuli za kurejesha pesa alizotumia hivi karibuni.

Mbio kati ya mlolongo wa uaminifu na mnyororo wa washambuliaji inaweza kuwa na sifa kama Kutembea kwa nasibu kwa Binomial. Tukio la mafanikio ni mlolongo wa uaminifu unaopanuliwa na mmoja kuzuia, ikiongeza uongozi wake kwa +1, na tukio la kutofaulu ni mlolongo wa mshambuliaji unaopanuliwa kwa kuzuia moja, kupunguza pengo kwa -1.

Uwezekano wa mshambuliaji kupata nakisi fulani ni sawa na Mcheza kamari Tatizo la uharibifu. Tuseme mcheza kamari aliye na mkopo usio na kikomo anaanza na upungufu na anacheza. Uwezekano wa idadi isiyo na kikomo ya majaribio ya kujaribu kufikia uvunjaji. Tunaweza kuhesabu uwezekano atawahi kufikia uvunjaji, au kwamba mshambuliaji atawahi kupatana na waaminifu mlolongo, kama ifuatavyo [8]:

p = uwezekano wa nodi ya uaminifu hupata kizuizi kinachofuata
q = uwezekano mshambuliaji hupata kizuizi kinachofuata
q_z = uwezekano wa mshambuliaji atawahi kupata kutoka kwa vitalu z z nyuma

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

Kwa kuzingatia dhana yetu kwamba p>q, uwezekano hupungua kwa kasi kadri idadi ya vizuizi ambavyo mshambuliaji anapaswa kupatana na ongezeko. Pamoja na uwezekano dhidi yake, ikiwa hatasonga mbele mapema, nafasi yake inakuwa ndogo sana anapobaki nyuma zaidi.

Sasa tunazingatia muda ambao mpokeaji wa muamala mpya anahitaji kusubiri kabla ya kuwa na uhakika wa kutosha kuwa mtumaji hawezi kubadilisha muamala. Tunadhania kuwa mtumaji ni mvamizi ambaye anataka kumfanya mpokeaji aamini kuwa alimlipa kwa muda, kisha abadilishe ili alipe yeye mwenyewe baada ya muda kupita. Mpokeaji ataarifiwa hilo likifanyika, lakini mtumaji anatumai kuwa kutakuwa kumechelewa.

Mpokeaji hutengeneza jozi mpya za vitufe na humpa mtumaji ufunguo wa umma muda mfupi kabla ya kutia sahihi. Hii humzuia mtumaji kuandaa msururu wa vitalu kabla ya wakati kwa kuifanyia kazi mfululizo hadi atakapobahatika kufika mbele ya kutosha, kisha kutekeleza shughuli hiyo wakati huo. Baada ya muamala kutumwa, mtumaji asiye mwaminifu anaanza kufanya kazi kwa siri kwenye msururu sambamba ulio na toleo lingine la muamala wake.

Mpokeaji husubiri hadi muamala uongezwe kwenye kizuizi na vizuizi z vimeunganishwa baada yake. Hajui kiwango kamili cha maendeleo ambacho mshambuliaji amefanya, lakini kwa kuchukulia kuwa vizuizi vya uaminifu vilichukua muda uliotarajiwa kwa kila kuzuia, maendeleo yanayoweza kutokea ya mshambuliaji yatakuwa usambazaji wa Poisson na thamani inayotarajiwa:

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

Ili kupata uwezekano kwamba mshambuliaji bado anaweza kufikia sasa, tunazidisha msongamano wa Poisson kwa kila kiwango cha maendeleo ambacho angefanya kwa uwezekano ambao angeweza kupata kutoka kwa hatua hiyo:

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

Inapanga upya ili kuzuia kujumlisha mkia usio na kikomo wa usambazaji...

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

Inabadilisha kuwa msimbo 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;
}
```

Kwa kutumia baadhi ya matokeo, tunaweza kuona uwezekano ukishuka kwa kasi kwa 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
```

Inatatua kwa P chini ya 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
```

Hitimisho

Tumependekeza mfumo wa miamala ya kielektroniki bila kutegemea uaminifu. Tulianza na mfumo wa kawaida wa sarafu zilizotengenezwa kutoka kwa saini za dijiti, ambayo hutoa nguvu udhibiti wa umiliki, lakini haujakamilika bila njia ya kuzuia matumizi ya mara mbili. Kusuluhisha hili, tulipendekeza mtandao wa rika-kwa-rika kwa kutumia uthibitisho wa kazi kurekodi historia ya umma miamala ambayo haraka inakuwa isiyowezekana kwa mvamizi kubadilisha ikiwa nodi za uaminifu hudhibiti nguvu nyingi za CPU. Mtandao ni imara katika isiyodhibitiwa yake usahili. Nodi hufanya kazi zote mara moja na uratibu mdogo. Hawahitaji kutambuliwa, kwa kuwa ujumbe hauelezwi mahali fulani mahususi na unahitaji tu kuwasilishwa kwa msingi bora wa juhudi. Nodi zinaweza kuondoka na kujiunga na mtandao kwa hiari, kukubali uthibitisho wa kazimnyororo kama uthibitisho wa kile kilichotokea wakiwa wamekwenda. Wanapiga kura kwa nguvu zao za CPU, kueleza kukubali kwao vitalu halali kwa kufanyia kazi kuvirefusha na kukataa vitalu batili kwa kukataa kuvifanyia kazi. Sheria na motisha zozote zinazohitajika zinaweza kutekelezwa na utaratibu huu wa makubaliano.

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.