Bitcoin: Urungano rwurungano rwa sisitemu ya elegitoroniki

by Satoshi Nakamoto 2008/10/31

Ibisobanuro

Urungano rwurungano rwamafaranga ya elegitoronike yemerera kwishura kumurongo woherejwe muburyo butandukanye bitanyuze mubigo by'imari. Imikono ya digitale itanga igice cyigisubizo, ariko inyungu zingenzi ziratakara mugihe uwundi muntu wizewe agikenewe kugirango akumire kabiri. Turasaba igisubizo cyikibazo cyo gukoresha kabiri dukoresheje urungano rwurungano. Urusobekerane rwibihe byogukora mubisunika mumurongo uhoraho wa hash-ishingiye kubikorwa-byakazi, gukora inyandiko idashobora guhinduka utabanje kugabanya ibyemezo-byakazi. Urunigi rurerure ntabwo rukora gusa nk'ikimenyetso cyerekana uko ibintu byakurikiranye, ahubwo ni gihamya ko byaturutse muri pisine nini ya CPU. Mugihe cyose ubwinshi bwimbaraga za CPU bugenzurwa numutwe udafatanya gutera urusobe, bazabyara urunigi rurerure hamwe nabatera. Umuyoboro ubwawo usaba imiterere mike. Ubutumwa butangazwa ku mbaraga nziza, kandi imitwe irashobora kugenda kandi igasubira murusobe uko bishakiye, ikemera urunigi rurerure-rwerekana akazi nkikimenyetso cyibyabaye mugihe bagiye.

Intangiriro

Ubucuruzi kuri interineti bwaje gushingira gusa kubigo by'imari bikora nk'abandi bantu bizewe kugirango bishyure hakoreshejwe ikoranabuhanga. Mugihe sisitemu ikora neza kubikorwa byinshi, iracyafite ibibazo byintege nke zicyitegererezo. Ibikorwa bidasubirwaho rwose ntibishoboka rwose, kubera ko ibigo byimari bidashobora kwirinda gukemura amakimbirane. Igiciro cyo kunga cyongera ibiciro byubucuruzi, bigabanya ingano yubucuruzi ifatika kandi bikagabanya amahirwe yo gucuruza bisanzwe, kandi harikiguzi kinini mugutakaza ubushobozi bwo kwishyura bidasubirwaho kuri serivisi zidasubirwaho. Hamwe nibishoboka byo guhinduka, gukenera kwizera gukwirakwira. Abacuruzi bagomba kwitondera abakiriya babo, bakabashakira ibisobanuro birenze ibyo bakeneye. Ijanisha runaka ryuburiganya ryemewe nkutakwirindwa. Ibi biciro hamwe no kutamenya neza ubwishyu birashobora kwirindwa imbonankubone ukoresheje ifaranga ryumubiri, ariko ntaburyo buhari bwo kwishyura muburyo bwitumanaho nta shyaka ryizewe.

Igikenewe ni uburyo bwo kwishyura bwa elegitoronike bushingiye ku bimenyetso bifatika aho kwizerana, kwemerera impande zombi zishaka gukorana hagati yazo bitabaye ngombwa ko hagira undi muntu wizewe. Ihererekanyabubasha ridashobora guhindurwa ryarinda abagurisha uburiganya, kandi uburyo bwa escrow busanzwe bushobora gushyirwa mubikorwa kurinda abaguzi. Muri iyi nyandiko, turasaba igisubizo cyikibazo cyo gukoresha kabiri dukoresheje

urungano rwurungano rwatanzwe na seriveri kugirango tubyare ibimenyetso byerekana uko ibihe byakurikiranye. Sisitemu ifite umutekano mugihe cyose inyangamugayo zishyize hamwe zigenzura imbaraga za CPU kuruta itsinda iryo ari ryo ryose rikorana.

Ibikorwa

Turasobanura igiceri cya elegitoronike nkurunigi rwumukono wa digitale. Buri nyirubwite yimura igiceri kurikindi asinyisha digitale hash kumurongo wambere hamwe nurufunguzo rusange rwa nyirubwite hanyuma ukongeraho ibyo kurangiza igiceri. Uwishyuwe arashobora kugenzura imikono kugirango agenzure urunigi rwa nyirubwite.

Ikibazo birumvikana ko uwishyuwe adashobora kugenzura ko umwe muri ba nyirayo atakoresheje inshuro ebyiri igiceri. Igisubizo rusange ni ukumenyekanisha ubuyobozi bukuru bwizewe, cyangwa mint, igenzura buri gikorwa cyo gukoresha kabiri. Nyuma ya buri gikorwa, igiceri kigomba gusubizwa mint kugirango gitange igiceri gishya, kandi ibiceri byonyine biva muntoki byizewe ko bitazakoreshwa kabiri. Ikibazo niki gisubizo nuko amaherezo ya sisitemu yimari yose biterwa nisosiyete ikora mint, hamwe nibikorwa byose bigomba kubinyuramo, nka banki.

Dukeneye inzira kugirango abishyuwe bamenye ko ba nyirubwite batigeze basinya ibyakozwe mbere. Kubwintego zacu, ibikorwa byambere byambere nibyo bibara, ntabwo rero twitaye kubigerageza nyuma yo gukoresha kabiri. Inzira yonyine yo kwemeza ko hatabayeho gucuruza ni ukumenya ibikorwa byose. Muri moderi ishingiye kuri mint, mint yari izi ibikorwa byose hanyuma ihitamo icyambere. Kugira ngo ibyo bigerweho nta shyaka ryizewe, ibikorwa bigomba gutangazwa kumugaragaro [1], kandi dukeneye sisitemu kugirango abitabiriye amahugurwa bumvikane kumateka imwe yuburyo bakiriye. Uwishyuwe akeneye gihamya ko mugihe cya buri gikorwa, ubwinshi bwumutwe bwemeye ko aribwo bwakiriwe bwa mbere.

Seriveri ya Timestamp

Igisubizo dusaba gitangirana na seriveri ya timestamp. Seriveri ya timestamp ikora ifata hash kumurongo wibintu kugirango ushireho igihe kandi utangaze cyane hash, nko mubinyamakuru cyangwa kuri Usenet[2-5]. Ingengabihe yerekana ko amakuru agomba kuba yarabayeho icyo gihe, biragaragara, kugirango yinjire muri hash. Buri gihe cyagenwe kirimo igihe cyabanjirije igihe cyacyo, kigakora urunigi, hamwe na buri gihe cyongeweho gishimangira icyabanjirije.

Icyemezo cy'akazi

Kugirango dushyire mubikorwa seriveri yagabanijwe kuri urungano rwurungano, tuzakenera gukoresha sisitemu yakazi-isa na Hashcash ya Adam Back [6], aho gukoresha ibinyamakuru

cyangwa Usenet. Icyemezo-cyakazi gikubiyemo gusikana agaciro iyo kwogeje, nka hamwe na SHA-256, hash itangirana numubare wa zeru. Impuzandengo yimirimo isabwa iragaragara mumibare ya zeru zisabwa kandi irashobora kugenzurwa no gukora hash imwe.

Kumurongo wigihe cyigihe, dushyira mubikorwa ibyemezo-byakazi twongera nonce muri blok kugeza igihe habonetse agaciro gatanga hash hasabwa zeru zisabwa. Iyo imbaraga za CPU zimaze gukoreshwa kugirango zuzuze ibimenyetso-byakazi, guhagarika ntibishobora guhinduka utongeye imirimo. Nkuko nyuma ibice byafunzwe nyuma yacyo, akazi ko guhindura umurongo karimo kugabanya ibice byose nyuma yacyo.

Icyemezo-cyakazi nacyo gikemura ikibazo cyo kumenya guhagararirwa mubyemezo byinshi. Niba ubwinshi bwari bushingiye kuri IP-imwe-imwe-imwe-imwe, birashobora guhindurwa numuntu wese ushobora gutanga IP nyinshi. Icyemezo-cyakazi ni kimwe-CPU-ijwi rimwe. Icyemezo cyinshi gihagarariwe nurunigi rurerure, rufite imbaraga zikomeye-zakazi-shoramari. Niba ubwinshi bwimbaraga za CPU bugenzurwa nu nyangamugayo, urunigi rwinyangamugayo ruzakura vuba kandi rusumba iminyururu irushanwa. Kugirango uhindure igice cyashize, uwagabye igitero yagomba kongera kwerekana-akazi-kahagaritswe na bice byose nyuma yacyo hanyuma agafata kandi akarenga kumurimo winyangamugayo. Tuzerekana nyuma ko amahirwe yo gutera gahoro gahoro gufata bigabanuka cyane nkuko byongeweho nyuma.

Kugirango wishyure byongera umuvuduko wibikoresho hamwe ninyungu zinyuranye mugukoresha umwanya mugihe, gihamya-y-akazi igenwa nimpuzandengo yimuka igereranya umubare ugereranije wahagaritswe kumasaha. Niba byabyaye vuba, ingorane ziriyongera.

Umuyoboro

Intambwe zo kuyobora umuyoboro nizi zikurikira:

1. Ibikorwa bishya byerekanwa kuri node zose.
2. Buri node ikusanya ibikorwa bishya mubice.
3. Buri node ikora mugushakisha ibimenyetso bitoroshye-byakazi kubikorwa byayo.
4. Iyo node ibonye gihamya-yakazi, isakaza umurongo kuri node.
5. Umutwe wemera guhagarika gusa niba ibikorwa byose birimo bifite agaciro kandi bitarakoreshwa.
6. Ipfundo ryerekana ko ryemera ko bahagarika akazi mugukora urwego rukurikiraho mumurongo, ukoresheje hash yahagaritswe nkuko byashize.

Umutwe uhora utekereza urunigi rurerure kugirango arirwo rukwiye kandi ruzakomeza gukora kururambura. Niba imitwe ibiri isakaza verisiyo zitandukanye zumwanya ukurikira icyarimwe, imitwe irashobora kwakira imwe cyangwa iyindi mbere. Muricyo gihe, bakora kumurongo wambere bakiriye, ariko uzigame irindi shami mugihe bibaye birebire. Ikaruvati izavunika mugihe ubutaha

ibimenyetso-byakazi bibonetse kandi ishami rimwe riba rirerire; imitwe yakoraga ku rindi shami izahita ihindura ndende.

Ibiganiro bishya byubucuruzi ntibikenewe byanze bikunze kugera kumurongo wose. Igihe cyose bageze kuri node nyinshi, bazinjira mumwanya muto. Guhagarika ibiganiro nabyo byihanganira ubutumwa bwataye. Niba node itakiriye blok, izabisaba mugihe yakiriye ahakurikira hanyuma ikamenya ko yabuze imwe.

Gutera inkunga

Mubisanzwe, igicuruzwa cyambere muguhagarika nigikorwa kidasanzwe gitangira igiceri gishya gifitwe nuwashizeho blok. Ibi byongeramo imbaraga zo gushyigikira urusobe, kandi bitanga uburyo bwo kubanza gukwirakwiza ibiceri mukuzunguruka, kubera ko nta bubasha bukuru bwo kubitanga. Kwiyongera guhoraho kwinshi kw ibiceri bishya birasa nabacukuzi ba zahabu bakoresha umutungo kugirango bongere zahabu mukuzenguruka. Ku bitureba, ni igihe cya CPU n'amashanyarazi bikoreshwa.

Inkunga irashobora kandi guterwa amafaranga yo gucuruza. Niba ibyasohotse mubicuruzwa bitarenze agaciro kinjiza, itandukaniro ni amafaranga yubucuruzi yongewe kumurongo wo gushimangira urimo ibikorwa. Iyo umubare wateganijwe mbere yibiceri winjiye mu kuzenguruka, gushimangira birashobora guhinduka rwose kumafaranga yubucuruzi kandi bikaba ari inflation yuzuye.

Inkunga irashobora gufasha gushishikarizwa gukomeza kuba inyangamugayo. Niba igitero kirarikira gishobora gukusanya imbaraga za CPU kuruta inyangamugayo zose, yagomba guhitamo hagati yo kuyikoresha kugirango abeshye abantu, cyangwa kuyikoresha kugirango atange ibiceri bishya. Agomba kubona ko gukinisha gukurikiza amategeko, amategeko nk'aya amutonesha ibiceri bishya kurusha abandi bose hamwe, kuruta guhungabanya gahunda n’ubutunzi bwe bwite.

Kugarura Umwanya wa Disiki

Iyo igicuruzwa giheruka mugiceri gishyinguwe munsi ihagije, ibikorwa byakoreshejwe mbere yuko bijugunywa kugirango ubike umwanya wa disiki. Kugirango woroshye ibi utabanje kumeneka hash, ibikorwa byogejwe mugiti cya Merkle [7] [2] [5], hamwe numuzi gusa ushizemo hash. Ibice bishaje birashobora guhuzwa no gutema amashami yigiti. Imbere yimbere ntabwo ikeneye kubikwa.

Guhagarika umutwe udafite ibikorwa byaba hafi 80 bytes. Niba dukeka ko bloks zikorwa buri minota 10, 80 bytes * 6 * 24 * 365 = 4.2MB kumwaka. Hamwe na sisitemu ya mudasobwa igurishwa hamwe na 2GB ya RAM guhera muri 2008, kandi Amategeko ya Moore avuga ko izamuka rya 1.2GB buri mwaka, ububiko ntibukwiye kuba ikibazo nubwo imitwe yo guhagarika igomba kubikwa mumutwe.

Kugenzura Kwishura Byoroheje

Birashoboka kugenzura ubwishyu udakoresheje umurongo wuzuye. Umukoresha akeneye gusa kubika kopi yimitwe yimitwe miremire-yerekana-akazi, ashobora kubona mubaza imiyoboro kugeza igihe yizeye ko afite urunigi rurerure, kandi akabona ishami rya Merkle rihuza ibikorwa na blok ntishobora gushyirwaho igihe. Ntashobora kugenzura ibyakozwe wenyine, ariko muguhuza ahantu hamwe mumurongo, arashobora kubona ko umuyoboro wabyemeye, hanyuma ugahagarika nyuma yo kwemeza ko umuyoboro wemeye.

Nkibyo, igenzura ryizewe mugihe cyose inyangamugayo zigenzura urusobe, ariko biroroshye cyane iyo umuyoboro utsinzwe nigitero. Mugihe imiyoboro y'urusobekerane ishobora kugenzura ibyakozwe ubwabo, uburyo bworoshe burashobora gushukwa nigitero cyibihimbano mugihe cyose uwagabye igitero ashobora gukomeza kunesha umuyoboro. Uburyo bumwe bwo kwirinda ibi byaba ari ukwemera imenyesha riva kumurongo mugihe babonye umurongo utemewe, bigatuma porogaramu yumukoresha ikuramo ibibujijwe byose hamwe nibikorwa byamenyeshejwe kugirango byemeze ko bidahuye. Abashoramari bakira ubwishyu kenshi birashoboka ko bazakomeza gukora imitwe yabo kubwumutekano wigenga no kugenzura byihuse.

Guhuza no Gutandukanya Agaciro

Nubwo byashoboka gutunganya ibiceri kugiti cyawe, ntibyoroshye gukora transaction itandukanye kuri buri ijana muri transfert. Kwemerera agaciro kugabanwa no guhuzwa, ibikorwa birimo ibyinjira byinshi nibisohoka. Mubisanzwe hazaba hari igitekerezo kimwe kiva mubikorwa binini byabanjirije cyangwa ibyinjijwe byinshi bihuza amafaranga make, kandi nibisohoka bibiri: kimwe cyo kwishyura, naho kimwe gisubiza impinduka, niba gihari, gusubira kubohereje.

Twabibutsa ko abafana, aho gucuruza biterwa nibikorwa byinshi, kandi ibyo bikorwa biterwa nibindi byinshi, ntabwo ari ikibazo hano. Ntabwo ari ngombwa gukuramo kopi yuzuye ya kopi yamateka yubucuruzi.

Amabanga

Uburyo bwa banki gakondo bugera ku rwego rw’ibanga mu kugabanya amakuru ku baburanyi babigizemo uruhare ndetse n’abandi bantu bizewe. Gukenera gutangaza ibyakozwe byose birabuza ubu buryo, ariko ubuzima bwite burashobora gukomeza kuburizwamo amakuru mu rindi. ikibanza: mugukomeza urufunguzo rusange ntirumenyekana. Rubanda rushobora kubona ko umuntu yohereje amafaranga kubandi, ariko nta makuru ahuza ibikorwa numuntu uwo ariwe wese. Ibi bisa nurwego rwamakuru yatangajwe nivunjisha, aho umwanya nubunini bwa ubucuruzi ku giti cye, " kaseti ", bishyirwa ahagaragara, ariko utabwiye amashyaka abo ari bo.

Nka firewall yinyongera, urufunguzo rushya rugomba gukoreshwa kuri buri gikorwa kugirango birinde guhuzwa na nyirubwite. Guhuza bimwe biracyakwirindwa hamwe nibikorwa byinshi byinjiza, byanze bikunze byerekana ko inyongeramusaruro zabo zari nyirazo. Ingaruka ni uko niba nyir'urufunguzo agaragaye, guhuza bishobora guhishura ibindi bikorwa bya nyirabyo.

Kubara

Twihweje ibintu byibitero bigerageza kubyara urunigi rwihuta kuruta urunigi rwinyangamugayo. Nubwo ibyo bigerwaho, ntabwo itera sisitemu gufungura impinduka uko bishakiye, nko guha agaciro umwuka mubi cyangwa gufata amafaranga atigeze aba uwagabye igitero. Umutwe ntushobora kwakira ibikorwa bitemewe nkubwishyu, kandi inyangamugayo ntizigera zemera guhagarika zirimo. Igitero gishobora kugerageza guhindura imwe mubikorwa bye kugirango agarure amafaranga aherutse gukoresha.

Irushanwa riri hagati yumunyangamugayo nuruhererekane rwibitero birashobora kurangwa nkurugendo rwa Binomial. Intsinzi yibikorwa ni urunigi rwinyangamugayo rwaguwe numurongo umwe, rwongera kuyobora kuri +1, naho ibyananiranye ni urunigi rwibitero byongerewe umurongo umwe, bigabanya icyuho -1.

Birashoboka ko igitero cyafata icyuho cyatanzwe nikibazo cyumukino wumukino. Dufate ko umukinyi wumukino ufite inguzanyo itagira imipaka atangirira ku gihombo kandi akina ibigeragezo bitagira ingano kugirango agerageze kugera kumena. Turashobora kubara amahirwe ashobora kugera kuri breakeven, cyangwa ko igitero cyigeze gifata urunigi rw'inyangamugayo, nkibi bikurikira:

$$
\begin{aligned}
p &= \text{birashoboka ko inyangamugayo inyangamugayo isanga ubutaha} \\
q &= \text{birashoboka ko uwagabye igitero abona ahakurikira} \\
q_z &= \text{birashoboka ko igitero kizigera gifata kuva } z \text{ guhagarika inyuma}
\end{aligned}
$$

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

Ukurikije uko tubitekereza $p > q$, ibishoboka bigabanuka cyane nkuko umubare wibibuza igitero ugomba gufata hamwe no kwiyongera. Hamwe n'ibibazo bimurwanya, niba adakoze amahirwe yo gutera imbere hakiri kare, amahirwe ye aba make uko agenda asubira inyuma.

Ubu turasuzuma igihe uwakiriye ibikorwa bishya agomba gutegereza mbere yo kumenya neza ko uwayohereje adashobora guhindura ibikorwa. Turakeka ko uwayohereje ari igitero ashaka gutuma uwakiriye yemera ko yamwishyuye igihe gito, hanyuma akayihindura kugirango yishyure nyuma yigihe runaka. Uwakiriye azaburirwa igihe ibyo bibaye, ariko uwayohereje yizeye ko bizatinda.

Uwakiriye atanga urufunguzo rushya kandi atanga urufunguzo rusange kubohereje mbere yo

gusinya. Ibi birinda uwagutumye gutegura urunigi rwibice mbere yigihe cyo kubikora kugeza igihe azagira amahirwe yo kugera kure bihagije, hanyuma agakora transaction muricyo gihe. Igicuruzwa kimaze koherezwa, uwakohereje ubuhemu atangira gukora rwihishwa kumurongo uringaniye urimo ubundi buryo bwo gucuruza.

Uyahawe arategereza kugeza igihe ibicuruzwa byongewe kuri blok na z guhagarika byahujwe nyuma yacyo. Ntazi umubare nyawo w'igitero uwateye yateye, ariko ukeka ko inyangamugayo zafashe igihe cyo kugereranya igihe cyari giteganijwe, igitero gishobora kuba igitero cya Poisson gifite agaciro kateganijwe:

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

Kugirango tubone ibishoboka uwagabye igitero ashobora gukomeza gufata ubu, tugwiza ubwinshi bwa Poisson kuri buri terambere yashoboraga gutera bitewe nibishoboka ashobora gufata kuva icyo gihe:

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

Gutondekanya kugirango wirinde guteranya umurizo utagira ingano wo kugabura...

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

Guhindura kuri 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;
}
```

gukoresha ibisubizo bimwe na bimwe, turashobora kubona amahirwe yo kugabanuka hamwe na 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
```

Gukemura kuri P munsi 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
```

Umwanzuro

Twasabye sisitemu yo gucuruza ibikoresho bya elegitoronike tutishingikirije ku kwizerana. Twatangiriye kumurongo usanzwe wibiceri bikozwe mumikono ya digitale, itanga igenzura rikomeye rya nyirubwite, ariko ntabwo ryuzuye nta buryo bwo gukumira amafaranga abiri. Kugira ngo iki kibazo gikemuke, twasabye urungano rwurungano rwifashishije gihamya-yakazi kugirango twandike amateka rusange yubucuruzi bihita bihinduka kubara bidashoboka ko igitero gihinduka niba imitwe inyangamugayo igenzura imbaraga nyinshi za CPU. Umuyoboro urakomeye muburyo

bworoshye bwubatswe. Umutwe ukora icyarimwe hamwe no guhuza bike. Ntibakeneye kumenyekana, kubera ko ubutumwa buterekanwa ahantu runaka kandi bugomba gutangwa gusa kubikorwa byiza. Imyanya irashobora kugenda hanyuma igasubira murusobe uko bishakiye, ikemera icyemezo-cyakazi nkikimenyetso cyibyabaye mugihe bari bagiye. Batora n'imbaraga zabo za CPU, bagaragaza ko bemera guhagarika byemewe mugukora kubagura no kwanga kubuza kwanga kubakorera. Amategeko yose akenewe hamwe nubushake arashobora gukurikizwa hamwe nuburyo bwumvikanyweho.

Reba

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.