Bitcoin: System ye kupanana mari iri electronic pahushamwari (Peer-to-Peer Electronic Cash System)

na Satoshi Nakamoto 2008/10/31

Abstract

Kupanana kwe mari iri electronic pahushamwari kunoita kuti kubhadhara pamhepo kuitike kubva kune munhu mumwe zvichienda kune mumwe pasina kuenda kune bato rezvemari. Madigitial signatures anobatsira, asi tinorasikirwa nekunaka kwekuva nemunhu wechitatu anovimbika kutarisa kuti kushandisa mari kaviri hakuitike. Tinofunga kuti mhinduro yekunetsa kwekushandisa kaviri kunoitwa nekupanana nenzira yeshamwari-ku-shamwari(peer-to-peer). Network inoshandisa timestamps transaction nenzira yekumabatanidza kuita chain iri hash-based, ichigadzira record isingazoshandurwa pasina kuita proof-of-work zvakare. Chain yakareba kupfura ese ndoinomirira proof yezvese zvaitika uyezve inomirira kuti yakabva papool ikuru inobva paCPU. Kana simba rakanyanya richitongwa nemanodes asiri kushanda kuvhiringidza network, inogadzira chain yakareba kuti ikunde varikuedza kuikwadza. Network yacho inofanira kuva ne minimal structure. Tsamba dzinotumirwa pa best effort basis, manodes anobva achidzotserwa panetwork paanodira, achibvumira proof-of-work yakarebesa seproof yezvakaitika aenda.

Mavambo

Kutenga nekutengeserana(commerce) painternet inofanira kushandisa mapato anoona nezvemari(financial institutions) anoshanda sevanhu vakavimbika kuita kuti kubhadhara pamhepo kuitike. System iyi inoshanda pamatransactions akawanda zvakanaka, asi pachine matambudziko anouya nekushandisa trust based model. Matransactions asingadzoserwe (non-reversible) haakwanise kusavapo zvachose, sezvo mapato emari(financial institutions) haakwanise kurega kugadzirisa kusawirirana kungaitike. Kugadzirisa kusawirirana kungavapo kunokwidza mitengo yekuita matransactions, zvichiita kuti kuderera kwemitengo wematransactions kunetse, uye kuite kuti mikana wematransactions madiki asavapo. Kune kunetsekana kwakanyanya kunouya nekusavapo kwematransactions asingadzoserwe nemaservices asingadzoserwe. Mikana yekudzosera matransactions kunoreva kuti kuvimbika kunofanira kuvapo. Vanotengesa vanofanira kugamuchira kuti vatengi vachavakumbira ruzivo runopfurikidza ravanofanira kunge vachipihwa. Pane chidimbu chehutsotsi hunotarisirwa kuitika, uye chinhu chatinofanira kugamuchira. Matambudziko akaita seaya haawanikwe kana wakatenga zvinhu panzvimbo nemari yebepa, asi hapana mechanism inoita kuti kutenga pacommunications channel pasina munhu akavimbika.

Chinodiwa isystem yekubhadhara pamhepo(electronic payment system) pa cryptographic proof pane kuregera vanhu vaviri vanoda havo kutenga kana kutengeserana pasina munhu wechitatu(third party). Matransactions asingakwanise kudzoserwa anobatsira vanotengesa kuti vasabirwe, uye maroutine escrow mechanisma anokwanisa kuiswa kuti vanotenga vasabirwewo. Mubepa rino, tinoedza kupa mhinduro kukushandisa kaviri(double-spending) tichishandisa shamwari-ku-shamwari(peer-to-peer) distributed timestamp server kuti igadzire computatitonal proof ye chronological order of transactions. System yakachengetedzeka chero paine mahonest nodes anoshanda pamwe kushandisa CPU power yakawanda pane chero bato remaattacker nodes.

Matransactions (Kutenga nekutengerwa)

Electronic coin ichain yemadigital signatures. Muridzi wega wega anotumira coin kune mumwe digitally nekusaina hash yetransaction yaitika ne public key yemuridzi achateera achizomapamidzira kwekupedzisira kwecoin. Munhu abhadhara(payee) anokwanisa kuongorora masignatures aya nekutarisa chain yevaridzi vacho.

Dambudziko riripo nderekuti munhu abhadhara haakwanise kuona kuti mumwe wevaridzi haana kutenga kana kutengesa coin racho kaviri. Mhinduro inowanzo kushandiswa kuva nebato rakavimbika, bato rinogadzira macoins(mint), rinotarisa transaction yekushandisa kaviri kwese kunoitwa. Panopera transaction ipi ne ipi, coin inofanira kudzoserwa kunebato rinogadzira macoins(mint) kuti coin itsva ipihwe, zvichireva kuti macoins abva kubato rinogadzira macoins(mint) ndoanotarisirwa kuti haana kushandiswa kaviri(double-spent). Zvinonetsera mhinduro iyi ndezvekuti bato rezvemari rinovimba nebato rinogadzira macoins(mint), sezvo transaction yega yega ichifanira kutanga yaenda kwavari, sebhanga.

Tinofanira kuwana nzira yekuti munhu abhadhara azive kuti vaimbova varidzi havana kunge vasaina mamwe matransactions kumwe. Kuti zvisanetse, transaction yekutanga ndiyo inebasa, saka hatina basa neanozoshandiswa kaviri. Nzira yekuziva kuti pane transaction isipo, kuziva matransactions ese aripo. Mumint based model, bato rinogadzira macoins(mint) rangarichiziva matransactions ese aitika. Kuti matransactions aitwe pasina bato rakavimbika, matransactions anofanira kuziviswa kuvanhu vese [1], uye kunofanira kuva nesystem yekuti vanoita matransactions vabvumirane pane ruzivo rwekare rumwe(single history) maererano nekuuya kwazvikaita. Munhu abhadhara anofanira kunge aine zvinoratidza kuti panguva yetransaction ipi ne ipi, manodes mazhinji abvuma kuti ndiyo transaction yekutanga.

Timestamp Server

Mhinduro yatauya nayo inotanga netimestamp server. Timestamp server inoshanda nekutora hash yeblock yezvinhu zvichaiswa matimesamps nekuisa hash kwese, kunge mubepanhau kana Usenet post[2-5]. Timestamp yega yega ine timestamp yekare muhash mayo, inozogadzira chain, netimestamp yese ichazoiswa kutsigira angaripo kare.

Proof of Work

Kuisa distributed timestamp server pa shamwari-ku-shamwari(peer-to-peer) basis, tinofanira kushandisa proof-of-work system yakafanana neAdam Back's Hashcash[6], kunze kwebepanhau kana maUsenet posts. Proof-of-work inosanganisira kuscanner hashed value, sekunge ne SHA-256, hash inotanga nemazero bits. Basa rinotarisirwa kuitwa rinoramba richiwedzera(exponential) mazero bits anodiwa uye kunoongororwa nekuexecuter single hash.

Patimestamp network, tinoisa proof-of-work nekupamidzira nonce mublock kusvikira value inopa mazero bits kuhash yeblock yawanikwa. Kana mabasa ese eCPU ashandiswa paproof-of-work, block haichakwanise kushandurwa pasina kugadzirwa basa(work) pakare. Kana mablocks anotevera abatanidzwa, basa rinozoitwa kushandura block rinoda kuti mablock ese agadzirwe patsva.

Proof-of-work inobatsira nyaya yekuwana kumiririrwa musarudzo yevazhinji. Kana vazhinji vari paone-IP-address-one-vote, inokwaniswa kuchinjwa nemunhu anokwanisa kupa maIPs akawanda. Proof-of-work itongori one-CPU-one-vote. Sarudzo yevazhinji inomiririrwa nechain yakareba pane ese, inova ndiyo inemabasa akawanda akaitwa pairi. Kana CPU power yakanyanya ichitongwa nemahonest nodes, honest chain ichakura nekukurumidza kupfura mamwe machain anokwikwidza. Kuti block yekare ishandurwe, attacker(mhandu) inofanira kugadzira proof-of-work yeblock pakare, nemablock ese anozotevera achipfurira basa remahonest nodes. Tichazoratidza kuti probability yemhandu inononoka kuti ibatane nevamwe inoderera zvakanyanya pese panopamidzirwa mablocks mamwe.

Kudzosera kukwira kwehardware speed neinterest inochinja mumanodes panopfura chinguva, kuoma kweproof-of-work kunobva pane moving average targeting tichitarisa huwandu hwemablocks pa awa. Kana achigadzirwa nekukurumidza, kuoma kwacho kunonyanya.

Pamhepo (Network)

Zvinhu zvekuita kuti network ishande:

1. Matransactions matsva anotumirwa kune manodes ese.
2. Node yega yega inotora matransactions matsva oisa mublock itsva.
3. Node yega yega inoshanda kutsvaga proof-of-work pablock yayo.
4. Node painowana proof-of-work, inomatumira block kumanodes ese.
5. Manodes anobvuma block kana matransactions ese arimairi ari echokwadi uye asina kumboshandiswa kare.

6. Manodes anoratidza kuti abvuma block nekugadzira block rimwe muchain, ichishandisa hash yakabvumwa sehash yakare.

Manodes anoona chain yakareba pane ese kuva chaiyo yairi kutsvaga saka inoramba ichishanda kuiwedzera. Kana manodes maviri akatumira maversion eblock inotevera akasiyana panguva imwe, mamwe manodes anowana imwe kana imwe yacho pekutanga. Kana izvi zvaitika node inoshanda pane block yayatanga kuwana, ichizochengeta rimwe sanzu racho kuitira rikazoreba kupfura rarashandira. Kuenzana kwemasanzu aya kunopera apo panobuda proof-of-work inotevera poonekwa kuti sanzu rimwe rakareba kupfura rimwe; manodes anga achishanda pane sanzu rimwe racho anobva atanga kushanda pane rakareba racho.

Matransactions matsva anotumirwa haatarisirwe kusvika kumanodes ese. Chero akasvika kumanodes mazhinji, anozongoenda mublock. Mablock broadcasts anobvumira ma dropped messages(tsamba dzadonhedzwa). Kana node yakasawana block, inoikumbira kana yawana block inotevera yoona kuti yangaisina kupihwa imwe block munguva yapfura.

Incentive

Mumaitiro anowanzoitika, transaction yekutanga mublock yakakosha sezvo iriyo inogadzira coin itsva yemunhu anogadzira block itsva. Izvi zvinopa mukana kune manodes kuti atsigire network, achizopa nzira yekuti macoin achiiswa munharaunda iyi, sezvo pasina bato rinoita izvozvo. Kuiswa kwemacoins matsva apo neapo zvakangofanana nekuwedzera kwezvinhu zvinoshandiswa kuchera goridhe navanochera goridhe kuwedzera goridhe munharaunda yavo. Apa, inguva yeCPU nemagetsi ndozvinoshandiswa.

Nzira yekugadzira macoins matsva (Incentive) inobhadharwa nemitengo wekuita matransactions. Kana value yabuda patransaction iri shoma pane value yaiswa patransaction, musiyano wacho ndomutengo wekuita transaction unozoiswa paincentive value ye block inenge ine transaction yacho. Kana macoins anotarisirwa kuvapo amo munharaunda iyi, incentive inenge yakukwanisa kushandisirwa mitengo yekuita matransactions chete, pasina kukwira kwemitengo yekuita matransactions acho.

Incentive inokwanisa kubatsira manodes kuti arambe achiita zvinhu pachokwadi. Kana attacker inokara yakawana CPU power kukunda manodes ari pachokwadi, inofanira kusarudza pakati pekushandisa simba iri kubira vanhu ichiba zvakabhadharwa, kana kuti inogadzira macoins matsva. Zvirinani kuti ione kuti zvinobatsira munhu wese kuita zviri pamutemo, sezvo mitemo iyi inozomupa macoins matsva akawanda kupfura emunhu wese akabatanidzwa, pane kusvora system nehuremu hwepfuma yayo.

Kutora Disk Space pakare

Kana transaction yenguva iyoyi irimucoin yaiswa pasi pemablock angaachitarisirwa akwana, matransactions ekare anokwanisa kuchiraswa hawo kuitira kuti disk space iwande. Kuita izvi tisina kudambura hash yeblock, matransactions anoitwa hashed muMerkle Tree[7][2][5], pachiiswa midzi chete muhash yeblock. Mablocks ekare anokwanisa kuderedzwa(compacted) nekubviswa masanzu pamuti. Hazvina basa kana mahashes emukati akasachengetwa.

Block header isina matransactions ine 80 bytes. Tongoti mablocks anogadzirwa maminitsi makumi ega ega,80bytes*6*24*365 = 4.2MB pagore. Macomputer system anowanzotengeswa aine 2GB ye RAM kubva muna 2008, ne Moore's Law ichitarisira kuwedzera ne 1.2GB pagore, pekuchengetera hapanetse chero mablock headers achifanira kuchengetedzwa mundangariro(memory).

Kutarisa zvabhadharwa kwakareruka(Simplified Payment Verification)

Zvirinyore kubvumira kuti chinhu chibhadharwe pasina kushandisa network node yakazara. Munhu anoshandisa network anofanira kungochengeta copy yemablock headers yeproof-of-work chain yakareba pane ese aripo, yaanokwanisa kuwana nekugadzira manetwork kusvikira aona kuti agadzira chain yakareba pane ese, achiwana sanzu reMerkle achizobatanidzatransaction kutimestamped block. Haakwanise kucherechedza transaction yake ega, asi pakubatanidza pachain, anoona kuti network node yaibvuma, uyezve mablocks anozopamidzirwa anoratidza kuti network yaibvuma.

Zvinoreva kuti verification yakavimbika kana mahonest nodes ariwo arikutonga zvenetwork, asi inonetsa kana yakakurirwa neattacker(mhandu). Sezvo manetwork nodes achikwanisa kuzvitarisirira manetwork nodes pachavo, nzira yakareruka yacho inokwanisa kutsotswa nematransactions ekunyepera eattacker kana attacker ichikwanisa kukurira network. Mhinduro inobatsira pakadai ndeye kugamuchira zviziviso zvemanetwork nodes panoonekwa kuti block nderekunyepera, zvichiita kuti munhu anoshandisa software atore full block nematransactions akaziviswa kucherechedza kusaerana kwacho.Mabhizimisi anowana mibhadharo yakawanda anenge achida kushandisa manodes awo kuitira kuzvitarisira kuti zvinhu zvaitwa nekukurumidza.

Kubatanidza nekupatsanura huremu (Combining and Splitting Value)

Macoins anokwanisa kuchengetwa akapatsanurwa serimwe nerimwe, zvinozonetsa kuti transaction yecent imwe neimwe iiswe payo yega. Kuita kuti huremu hupatsanurwe nekubatanidzwa kuitike, matransactions ane mainputs ne maoutputs akawanda. Kazhinji pane input imwe inobva kune transaction ikuru pane iripo kana kuti mainputs madiki akabatanidzwa, zvichigumira pa mainputs maviri: imwe input inenge iri yekubhadharwa kwaitwa, imwe iri yezvasara pabhadharwa, kana paine zvasara, kudzosera atumira.

Zvinofanira kuziikanwa kuti fan-out, iyo ine transaction inotsigirwa nemamwe matransactions, matransactions iwayo achitsigirwa nemamwewo, hainetse pakadai. Hapana chingaite kuti ruzivo rwese rwezvakaitika patransaction rutorwe.

Kuchengetedzwa kweruzivo rwematransactions aitika

Bhanga rinokwanisa kuchengetedza ruzivo rwematransactions anenge aitika, rinokwanisa kuita izvi nekungozivisa vanhu vaita matransactions aya chete nebato rakavimbika rechitatu. Kuzivisa vanhu vese matransactions aitwa kunofanira kuchiitwa kunonetsa kuzoita kana machengeterwo eruzivo rwematransactions kukaitwa nenzira yebhanga, asi kuchengetedzeka uku kunokwanisa kuitwa kana mafambiro eruzivo urwu ukapatsanurwa pamwe:kuita kuti mapublic keys asaziikanwe zvachose. Ruzhinji runokwanisa kuona kuti pane munhu akutumira mari kune mumwe, asi pasina ruzivo rwekuti ndiani atumira kana kutumirwa. Izvi zvakangofanana neruzivo runoziikanwa kumastock exchanges, uko nguva nesize yekutenga kana kutengeswa ,"tape", inoziviswa ruzhinji, asi pasina kuiswa mazita evanhu vatenga kana kutengesa mastocks.

Kupamidzira kusimba kwekuchengetedza ruzivo, key pair itsva inofanira kushandiswa patransaction imwe ne mimwe kuitira kuti muridzi wayo asazozivikanwa. Kuziva muridzi wekey kunokwanisa kuzozivikanwa nemamulti-input transactions ayo anoratidza kuti mainputs aiva ani. Dambudziko riripo nderekuti kana muridzi wekey akuzivikanwa, kubatanidza kunoita kuti mamwe matransactions emunhu akuzivikanwa azivikanwe zvakare.

Calculations

Takutarisa chiitiko cheattacker(mhandu) irikuedza kugadzira chain imwewo inokurumidza kudarika honest chain. Chero zvikaitika sekudaro, hazvirevi kuti system inokwanisa kungoshandurwa, sekungogadzira huremu hunongobva kusingaziikanwe kana kutora mari isina kumbobvira yave yeattacker. Manodes haagamuchire transaction yenhando semubhadharo, uyezve mahonest nodes haambo gamuchire block ine matrasanctions enhando.

Attacker inokwanisa kungochinja transaction yayo chete kutora mari yayakamboshandisa pasina nguva yakawanda yapfura. Makwikwi ari pakati peattacker chain nehonest chain yakangofanana ne Binomial Random Walk. Kubudirira kwechiitiko ndokupamidzirwa kwehonest chain neblock rimwe, ichienda mberi ne+1, kukundikana kwe chiitiko ndokupamidzirwa kwe attacker chain neblock rimwe, ichidzosera chain kumashure ne -1.

Mukana wekuti attacker iringane nemamwe machains kubva kumashure kwakangofanana ne Gambler's Ruin problem. Tongoti gambler ane chikwereti chisingaperi anotanga asina mari otamba kasingaperi kusvikira akwanisa kuwana mari yaakatamba.

Tinogona kuongorora mukana wekuti haazombowane mari yaakabheja, kana kuti attacker inokwanisa kuzosvika panhanho yehonest chain, seizvi[8]::

$$\begin{aligned} p &= \text{mukana wekuti honest node inowana block inotevera} \\ q &= \text{mukana wekuti attacker node inowana block inotevera} \\ q_z &= \text{mukana wekuti attacker node icharingana honest node ichibva kumashure ne z } z \text{ blocks} \end{aligned}$$

$$q_z = \begin{Bmatrix} 1 & kana\ p \le q \\ (q/p)^z & kana\ p > q \end{Bmatrix}$$

Zvichibva pakuti tati $p > q$

, Mukana uyu unoderera nekukurumidza zvakanyanya apo mablocks ekuti attacker izoita kuti iringane nemahonest chains achipamidzirwa. Sezvo paine mukana mudiki chaizvo wekuti attacker node inozosvika pane mahonest nodes, kana ikasawana rombo rakanaka rwekuenda mberi pekutanga, mukana uyu unoramba uchiita hudiki kuti ichazosvikako.

Takutarisa kuti munhu arikutumirwa transaction itsva anomira nguva yakareba sei kuti azoziva zvechokwadi kuti munhu atumira haachakwanise kuchinja transaction. Tinongotora kuti munhu atumira ndiye attacker irikuda kuti munhu arikutumirwa ave nechivimbo chekuti abhadharwa kwenguva irefu, ozozvichinja kuti azozvitumira pakare kana pane chinguva chapfura. Munhu atumirwa anozoziviswa kana zvazoitika, asi munhu atumira anongotarisira kuti zvinenge zvisisina basa.

Munhu atumirwa anogadzira key pair itsva opa public key kune munhu amutumira achizosaina kana apedza izvozvo. Izvi zvinoita kuti munhu atumira asazogadzira chain yemablocks nguva isati yakwana nekushanda paari kusvikira azokwanisa kuenda mberi, achizoita transaction panguva iyoyo.

Kana transaction yatotumirwa, uyu anotumira asiri pachokwadi anotanga kushanda muchihwande pa parallel chain inenge ine transaction yake yenhando. Munhu anotumirwa anozomirira kuti transaction iyi ipamidzirwe kune rimwe block uye kuti ma blocks z azopamidzirwa pamusoro. Haazive mafambiro ekugadzira mablocks kwaitwa neattacker, asi kana tikati mahonest blocks atora nguva iri pakati pemashandiro anoitwa nemanodes ese kugadzira block, kubudirira kwe attacker kunoenderana ne value inotarisirwa ne Poisson distribution:

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

Kuti tizowana mukana wekuti attacker ichazosvika pane mahonest nodes izvezvi, tino multiplier Poisson density ye mashandiro abudirira ese nemukana wekuti achasvika pane mahonest nodes panguva inoyi:

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

Rearranging to avoid summing the infinite tail of the distribution...

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

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;
}
```

Running some results, we can see the probability drop off exponentially with 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
```

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
```

Magumo

Tataura nezve system ye maelectronic transactions tisingatarise kuvimbika kwawo. Tatanga ne zvemacoins ane madigital signatures, anopa muridzi kuchengetedza kwemacoin kwakazara, asi hazvina kunyatsokwana kana pasina mhinduro yedambudziko rekushandisa kaviri(double spending). Mhinduro yatakapa kudambudziko rekushandisa kaviri, yangairi network yehushamwari-ku-shamwari ichishandisa proof-of-work kuisa matransactions akaitika kare kuruzhinji zvichizodzivirira kushandurwa kwayo neattacker kana mahonest nodes aine masimba mazhinji pamusoro peCPU.

Network yakasimba nemavakirwo akarareruka ayakaitwa. Manodes anoshanda pamwe chete pasina kurongwa kwakanyanya. Manodes aya haatarisirwe kuti azivikanwe, sezvo tsamba dzacho dzisingaendeswe kune nzvimbo imwe asi dzichifanira kuendeswa pabest effort basis. Manodes anokwanisa kubva achidzoka panetwork paadira, achigamuchira proof-of-work chain sechiitiko chezvaitika paangasisipo. Manodes anosarudza achishandisa simba reCPU yayo, achishandisa kugamuchira kwaaita mablocks echokwadi nekushanda pakumapamidzira nekuramba mablocks enhando nenzira yekuramba kushanda paari. Mirairo inoda kuteedzerwa inokwanisa kuiswa nekubvumirana kweruzhinji kuripo.

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.