Bitcoin: Hannaan Lacageedka Danabaysan Ee Qof-ka-Qof

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Waxaa loo turjumay SOOMAALI, waxaana u turjumay "CryptoYahan.com↗"

Dulmar. Hannaan lacageedkan danabaysan ee qof-ka-qof, ama dhinac-ka-dhinac ayaa suuragalinaya in uu qof si toos ah lacag ugu diro qof kale, iyadoon loo baahanin qolo kale oo saddexaad. Digital Signatures-ku waa qeyb ka mid ah xalka, hasa ahaatee waxaa la lumin donaa dheefihii ugu waa-weynaa, hadii wali loo sii baahanayo qolo saddexaad, oo lagu kalsoonaado, si ay uga hortagaan Double Spending-ka ama kharashgaraynta laban-laaban. Waxaan dhibkan ah Double Spending-ka u soo jeedinaynaa xal, iyadoo loo marayo shabakad ama hannaan ogolaanaya in si toos ah qofba qofka kale wax waydaarsado. Hannaankan ayaa is-dhaafsi kasta (Transactions) ku shaanbadaynaya shaanbad wakhtiyaysan (Timestamps), iyadoo lagu xidhiidhinayo silsilad ama diiwaan is-daba-joog ah, oo ku salaysan wax la yidhaahdo "Proof of Work", iyadoo la adeegsanayo hab loo yaqaan "Hash", halkaas oo uu ku samaysmi doono diiwaan aan wax laga bedeli karin, ilaa dib hadana shaqo danbe loo qabto mooyee. Silsiladda ugu dheer ma ahan oo kaliya inay ka maragkacayso sida ay iskugu daba-taxan yihiin dhacdooyinka ee ay isku la xidhiidhaan, ee waxay sidoo kale ka maragkacaysaa in ay silsiladani ka timid isu-imaatinka ugu awoodda badan ee CPU. Ilaa iyo inta awoodda kombuyuutarrada (CPU) badidoodu ay gacanta ku hayyaan oo ay xakameeyaan Nodes-yada aan isku-bahaysan si ay u weeraraan shabakadda, waxay dhalin doonaan silsiladda ugu dheer, wayna ka tallaabo dheereen doonaan, kana hormari doonaan weeraryahanada. Shabakadu waa mid aan hab-dhis ama sal adag u baahnayn. Fariimaha ayaa la is kugu gudbiyaa, oo loo kala qaadaa sida ugu wax-ku-oolnimada badan, waxayna Nodes-yadu awood u leeyihiin inay si fudud shabakada uga baxaan, si fududna ugu soo laaban karaan goorta ay doonaan, iyagoo aqbalaya silsiladda ugu dheer, taasoo caddayn u ah wixii dhacay intii ay maqnaayeen.

1. Hordhac

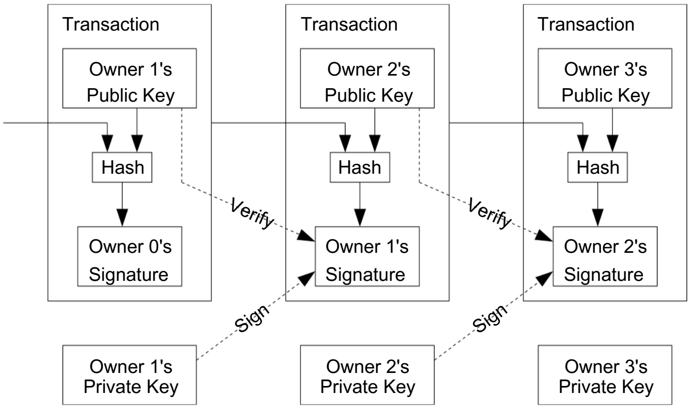
Ganacsiyada internet-ka ka jira waxay haatan ku dhawaad si weyn ugu tiirsan yihiin ururo maaliyadeed, oo ah ama u dhaqma sidii qolo saddexaad oo kale, oo kalsooni leh, si ay u hirgaliyaan, una socodsiiyaan geedi-socodka lacag-bixinada elegtarooniga ah. In kastoo qaabkan si wacan ugu shaqeeyo lacag-dirisyda (Transactions) inteeda badan, hadana wali waxaa jirta dhinacyo uu ku liito, waana salka ay ku hayso, ama ay ku salaysan tahay kalsoonidu. Lacag-dirisyada (Transactions) aan ka noqoshada aqbalin ma aha kuwo ka suuragal ah ururada maaliyadeed, waayo ururada maaliyadeed kama madh-naan karaan, oo kama fogaan karaan, oo iskama caabin karaan khilaafyada soo kala dhex gala labada dhinac. Dhexdhexaadintooduna waa kharash, kaasoo fuulaya ama lagu soo dallacayo is-dhaafsigii ama Transactions-kii, taasoo xaddidaysa, isla mar ahaantaana yaraynaysa is-dhaafsiyadii yar-yaraa, intaa waxaa dheer in ay jirto dhibaato kale oo ka weyn tii hore, oo ah in aan la heli karin adeeg lacag-diris aan ka noqoshada aqbalin, kadib markii la helay adeeg aan ka noqoshada aqbalin. Suurtagalnimada ah in lacag la diray dib loo-la noqon karo, waxay kordhisaa baahidii loo qabay kalsoonida.

Ganacsatadu waa inay ka digtoonaadaan macaamiishooda, feejignaan badanna muujiyaan, waxayna taasi ku khasbaysaa inay macaamiishooda waydiiyaan su'aalo iyo xogo dheeraad ah, oo ka badan inta ay u baahnaayeen. Xaddi go'an ama heer cayyiman oo ka mid ah khiyaanada ayaa loo arkaa inay tahay xaddi aan laga baaqsan karin, ama aan laga fursan karin. Sida kaliya ee looga fogaan karo khilaafooyinkana waa in si fool-ka-fool ah la isku waydaarsado lacagta, iyadoo la adeegsanayo lacag jidhitaan jidheed leh, hasa yeeshee ilaa haatan ma jirto hab ama hannaan lacag-bixineed oo online ah, oo u kala goosha qaaradaha, isla mar ahaantaana loo marayo kanaalada is-gaarsiinta, iyadoon jirin qolo dhexe oo lagu kalsoon yahay.

Waxa kaliya ee loo baahan yahay waa hannaan lacag-bixineed oo danabaysan (Electronic) oo ku salaysan "Cryptographic Proof", halkii ay ku salaysnaan lahayd kalsooni (Trust), taasoo laba dhinac kasta oo doonaya in midba midka kale si toos ah ula macaamilo, u ogolaanaysa in ay si toos ah u macaamiloodaan, iyadoon loo baahanin qolo saddexaad oo lagu kalsoonaado. Lacag-dirisyada aan ka noqoshada aqbalin, ama aan laga noqon karin xisaab ahaan markii loo eego, waxay iibiyayaasha ka ilaalinayaan khiyaamooyinka iyo dhagaraha iibsadayaasha, isla mar ahaantaana waxaa si fudud loogu dhisi karaan hannaanada amni ee "Escrow" , si markan iibsadaha looga ilaaliyo iibiyaha. Xaashidan ama cilmi-baadhistan waxaan ku soo jeedinaynaa xal cusub oo aynu ku wajjahayno dhibaatada ah in isla hal lacag laba jeer iyo wixii ka badanba la kharash gareeyo (Double Spending), iyadoo la adeegsanayo shabakad qeyb-qeybsan (Distributed) oo wakhtiyaysan (Timestamp) oo qof-ka-qof (Peer-to-Peer), si loo curiyo diiwaan sugan oo wakhtiyaysan oo is-daba-taxan, oo muujinaya sida ay u kala horreeyaan is-dhaafsiyada (Transactions). Hannaanku waa mid amaan ah, ilaa iyo inta ay Nodes-yada daacada ahi si wada-jir ah gacanta ugu hayyaan, oo ay u xakamaynayaan awoodda shabakadda inteeda badan, ama awoodda kumbiyuutarada (CPU), in ka badan inta ay gacanta ku hayyaan kooxaha isku bahaysanaya in ay shabakadda weeraraan.

2. Lacag-dirisyada

Waxaynu lacagaha danabaysan (Electronic) ku qeexi karnaa inay yihiin silsilado is-daba-taxan oo ka kooban saxiixyo dhijitaal ah (Digital Signatures). Milkiile kasta wuxuu lacagtiisa u wareejin karaa milkiilaha xiga, isagoo si dhijitaal ah u saxiixaya Hash-ka lacag-diristii hore, iyo furaha guud (Public Key) ee milkiilaha cusub, isagoo abuuraya Transaction-ka, kadibna u diraya shabakadda. Dhanka kale loo-diraha ama qofka lacagta helaya wuxuu si fudud u hubin kara saxiixyada, si uu u sugo lahaanshaha lacagta.

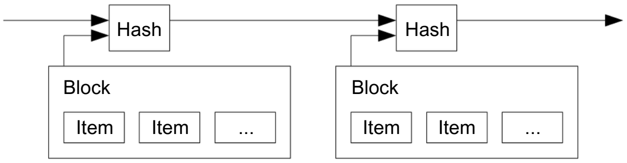


Halkan dhibaatada jirta ayaa ah in uusan loo-diruhu hubin karin in milkiilayaashii hore aysan lacagta la-laba jeer kharashgarayn, oo aanay samaynin Double Spending. Sida caadada ahna, xalku wuxuu noqonayaa in la helo maamul dhexe, oo lagu kalsoonaan karo ama "Mint", kuwaasoo u xil saaran in ay kormeeraan sidoo kalena xaqiijiyaan lacag-diris kasta, si looga hortago Double Spending-ka. Lacag-diris kasta kadib, waa in lacagta dib loogu soo celiyaa warshadii soo saartay, ama madbacadii (Mint), si ay u soo saarto lacag kale oo cusub, lacagaha kaliya ee lagu kalsooon yahay in aan hore loo adeegsan, oo aan la-laba kharashgarayn (Double Spending) waa lacagaha sida tooska ah uga soo baxa Mint-ga. Dhibaatada xalkan ayaa ah in cidhib-danbeedka hannaan-lacageedkan gabi ahaantii uu ku tiirsan yahay shirkadda ama qolada maamusha Mint-ga, iyadoo lacag-diris kasta ay tahay in uu iyaga soo dhex maro, si la mid ah bangiyada.

Waxaynu u baahannahay waddo ama qaab uu loo-diruhu ama qofka lacagta helaya uu ku ogaan karo in milkiilayaashii ka horreeyay isaga aysan hore u adeegsan lacagta, oo aysan hore u saxiixin lacag-dirisyo hore. Yoolkeenu ama ujeedkeenu waa in aynu kaliya tixgalino lacag-dirista ama Transaction-ka ugu horreeya, sidaa darteed, iskuma hawlayno isku-dayada danbe ee lagu doonayo in lacagta lagu laba jeer adeegsado. Sida kaliya ee lagu ogaan karo in aan hore lacagta loo-laba kharashgaraynna, waa in aqoon buuxda loo leeyahay, lagana warqabo dhammaan lacag-dirisyda (All Transactions). Hannaankii ku tiirsanaa warshadda lacagta ama Mint-ga wuxuu ogaa oo uu hayyay dhammaan lacag-dirisyadii dhacay (Transactions), wuxuuna si fudud u go’aamin karayay lacag-diristii ugu horraysay. Haddaba hadii aynu rabno inaynu sidan oo kale samayno, iyadoon la adeegsanaynin dhinac saddexaad oo kalsooni leh, waa in aynu dhammaan lacag-dirisyada ka dhignaa kuwo shaacsan, oo baahsan [1], waxaynuna sidoo kale u baahannahay hannaan (System) ay ka qeybgalayaashiisu ama dadyawga xubnaha ka ahi isku raacaan, oo ay ku hishiiyaan diiwaan midaysan oo sheegaya sida ay Transactions-yadu u kala horreeyeen. Loo-diruhu ama qofka lacagta helaya wuxuu u baahan yahay caddayn sheegaysa in marka Transaction-ka la diray, ugu badnaan Nodes-yadu ay ogolaadeen oo ay isku raaceen in lacag-diristani ay tahay tii ugu horraysay ee nooceeda ah.

3. Shaanbadda Wakhtiyaysan (Blockchain)

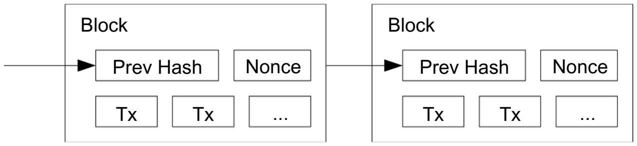
Xalka aynu soo jeedinayno wuxuu ka bilaabmayaa Timestamp Server (Blockchain). Timestamp Server-ku waxay shaqadiisu tahay inuu xidhmo (Block) xogo ah Hash gareeyo, si shaanbad wakhtiyaysan loogu yeelo, kadibna si baahsan loo shaaciyo oo loo daabaco, sida wargaysyada ama Usenet Post [2-5]. Shaanbada wakhtiyaysan waxay caddaynaysaa in xogta la Hash-gareeyay ay ahayd mid wakhtigaas jirtay, sida iska cadna wax lama Hash-garayn karo xog la’aan. Timestamp (Block) kasta wuxuu la xidhiidhaa Hash-ka Timestamp (Block) ka horreeyay, Timestamp kastana wuxuu xoojinayaa runimada kii ka horreeyay, sidaasina waxaa ku samaysmaysa silsilad.



4. Hab-sugid Shaqo

Si loo hirgaliyo shabakad qeyb-qeybsan (Distributed) oo wakhtiyaysan (Timestamp) isla mar ahaantaana ku salaysan mabda’a qof-ka-qof (Peer-to-Peer), waxaynu u baahannahay hab-sugid shaqo (Proof of Work), oo la mid ah hannaanka "Adam Back's Hashcash" [6], bedelkii wargaysyada ama Usenet Post. Hab-sugidda shaqo (PoW) waxay koobsanaysaa raadinta qiimo go’an oo ka bilaabmaysa tiro ebero ah oo Hash ah, sida SHA-256. Celceliska shaqo ee loo baahan yahay in la qabto waxay ku jibbaarmaysaa (Exponential) inta eberaad ee loo baahan yahay in la helo, waxaana lagu xaqiijin karaa in kaliya la sameeyo hal Hashing.

Markii la joogo shabakadeena Timestamp-ka ah, Proof of Work waxaa lagu helaa iyadoo marba marka ka danbaysa "Nonce" lagu kordhinayo Block-ka ilaa iyo inta laga helayo Hash leh tiro ebero (Zeros) ah oo markaa loo baahan yahay. Mar allaale markii la kharashgareeyo, oo la bixiyo dadaal iyo tamar (CPU), si loo helo Hash-kii bartilmaameedka ahaa, oo loo buuxiyo shuruudihii hab-sugidda shaqo (Proof of Work), lama awoodi doono in wax laga bedelo Block-ga, iyadoon hadana dib shaqo labaad loo qaban mooyee. Maadaama ay Block-yada danbe la xidhiidhsan (Chained) yihiin kuwii ka horreeyay, hadii la rabo in wax laga bedelo Block waxaa lagu khasban yahay in hadana dib loo bedelo dhammaan Block-yadii ka danbeeyay oo dhan.



Hab-sugidda shaqo (Proof of Work), waxay sidoo kale xallinaysaa dhibka ah go’aaminta go’aan-qaadashada aqlabiyadda. Hadii aqlabiyadda lagu saleeyo mabda’ ah hal IP hal cod (One IP address, one vote) waxaa hannaankan burburin kara qof kasta oo awood u leh inuu uruuriyo IP-yo badan. Hab-sugidda shaqana salkeedu waa hal CPU hal cod. Go’aan-qaadashada aqlabiyadda ama go’aan-qaadashada ugu badan waxay u taagan tahay silsiladda ugu dheer, taas oo lagu bixiyay shaqadii iyo tamartii (CPU) ugu badnayd. Haddii aqlabiyadda awoodda CPUs ay gacanta ku hayaan Nodes-yada daacadda ahi, silsiladda dhabta ah ayaa si degdeg ah u kori doonta oo ka horrayn doonta silsiladaha kale. Si Block hore u jiray wax looga bedelo, waa in uu weeraryahanku mar kale dib u sameeyaa shaqadii Proof of Work, kuna sameeyaa dhammaan Block-yadii ka danbeeyay, kadibna uu kula tartamaa Nodes-yada daacadda ah. Wakhti kadib, waxaynu arkaynaa in ay si tartiib-tartiib ah u soo yaraanayso suurtagalnimada uu weeraryahanku ku gaadhi karo kuwa daacadda ahi, iyadoo ay awoodiisu si weyn hoos ugu dhacayso mar allaale markii Blocks-yo dheeraad ah la soo biiriyo.

Si loo xakameeyo korodhka xawaaraha qalabka kumbiyuutarada iyo is-bed-bedelka Nodes-yada ee ay marna shabakadda ka baxayaan, marna ku soo laabanayaan, waxaa heerka adkida Proof of Work lagu go’aamiyaa celcelis si joogto ah isu-bed-bedalaya, kaas oo ujeedadiisu tahay in lagu helo celcelis tiro go’an oo Block-yo ah saacaddii. Hadii Block-ga si aad u dhakhso badan loo soo saaro, heerka adkida ayaa kordhaysa.

5. Shabakadda

Tallaabooyinka shaqada shabakadda waa kuwan:

1) Lacag-diris kasta oo cusub waxaa loo diraa Nodes-yada oo dhan.
2) Node kasta wuxuu lacag-dirisyada cusub ku uruurinayaa Block.
3) Node kasta wuxuu ka shaqaynayaa sidii uu Block-giisa ugu heli lahaa hab-sugid shaqo oo adag.
4) Markii uu Node helo Block, Block-gaas waxaa loo dirayaa Nodes-yda kale oo dhan.
5) Hadii xogta ku jirta Block-ga ay qumman tahay, oo aan hore loo kharash garayn, Block-ga waa la ansixinayaa.
6) Marka Block-ga la ansixiyo oo la aqbalo, Nodes-yadu waxay si toos ah u bilaabaan shaqada Block-ga xiga, iyagoo ku xidhiidhinaya Hash-ka Block-gii la aqbalay.

Nodes-yadu waxay mar waliba silsilada ugu dheer u tixgaliyaan inay tahay tan ugu qumman, waxayna ka shaqeeyaan sidii ay u sii ballaadhin lahaayeen. Haddii laba Node ay si isku mar ah u soo saaraan laba nuqul oo kala duwan oo ah Block-ga xiga, qaar ka mid ah Node-yada ayaa arki doona mid ka mid ah labada nuqul. Xaaladdan oo kale, Node walba wuxuu bilaabi doonaa inuu ka shaqeeyo Block-ga uu hor helay, isagoo kayd ahaan u haysan doona Block-ga kale ama laanta kale ee silsiladda, si hadii ay taasi u noqoto silsiladda ugu dheer loogu wareego. Xaaladan ayaa la jabin doonaa ama laga bixi doonaa markii mid ka mid ah uu noqdo silsiladda ugu dheer, ee hab-sugidda shaqo ee ugu badan lagu bixiyay, waxayna Nodes-yada kale ee ka shaqaynayay laanta kale u soo guuri doonaan laanta ama silsilada ugu dheer.

Lama huraan ama khasab ma ahan in lacag-dirisyada ama Transactions-yada cusub ay gaadhaan dhammaan Nodes-yada shabakadda. Ilaa iyo inta ay ka gaadhayaan tiro Nodes-yo ah, ugu danbayntii wakhti aan dheerayn waxay gali doonaan Block-ga. Sidoo kale, shabakadu waxay dulqaad u leedahay Block-yada aan la helin. Hadii uusan Node gaar ahi helin Block, dhib ma leh, markii Block-ga uusan heli ma ahee Block-ga xiga uu helo, ee uu ogaado in ay silsiladiisu wax ka maqan yihiin ayuu codsanayaa.

6. Dhiirigalinta

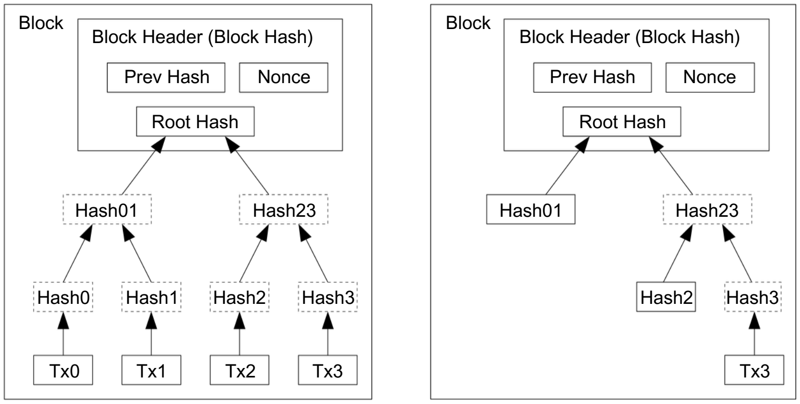
Sida xeerku yahay, Transaction-ka ugu horreeya ee Block kasta waa Transaction gaar ah, waana kan dhalinaya ama soo-saaraya lacagta cusub, kaasoo si toos ah ugu dhaca gacanta Block-ga soo-saaraha. Tani waxay dhiirigalinaysaa Nodes-yada si ay u sii wadaan taageeridda shabakadda, waxayna sidoo kale abuuraysaa hab ama qaab ay lacagtu suuqa ku imanayso, una noqonayso kuwo u nugul in la is-waydaarsado, maadaama aysan jirin maamul dhexe oo soo-saara lacagta. In si joogto ah oo go'an loo soo-saaro lacag cusub, waxay la mid tahay macdan qodoyaasha adeegsanaya agabka dahabka lagu soo-saaro oo kale, si ay dahab cusub u soo-saaraan, suuqana u soo galiyaan. Hasa yeeshee xaalkeenu waa inaynu adeegsanayno oo aynu bixinayno CPU Time iyo koronto.

Sidoo kale Block curiyaha (Miner) waxaa lagu dhiirigalinayaa khidmadaha (Fees) lacag-dirisyada. Hadii lacagta baxaysa (Output), ay ka yar tahay lacagta la adeegsanayo (Input), farqigaas wuxuu noqonayaa ujuurada ama khidmadda ama Fee-ga Transaction-ka, taasoo lagu darayo tirada dhiirigalinta guud ee Block-ga, kaasoo ka kooban tiro Transactions-yo ah. Marka tiro go'an, oo lacagta (Bitcoin) ka mid ah la soo galiyo suuqa, waxay dhiirigalintu gabi ahaanteed u wareegaysaa khidmadaha ama Fees-ka lacag-dirisyada oo kaliya, wuxuuna hannaanku noqonayaa mid gabi ahaanteed ka madax-bannaan sicir-barar.

Dhiirigalintu waxay Nodes-yada ku dhiirigalinaysaa inay daacad sii ahaadaan. Hadii weeraryahan damac badan uu awoodo inuu uruuriyo awood CPUs ka badan kuwa daacaddda ah, waa in uu kala doortaa in uu awooddiisa u adeegsado si uu dadka u khiyaameeyo, isagoo lacag-dirisyadiisii hore dib u soo ceshenaya, ama in uu u adeegsado si uu u dhaliyo ama uu u soo-saaro lacago cusub. Waa in uu ogaadaa in raacista xeerarka ay ka faa'ido badan tahay, xeerarkaasoo isaga ka dhigaysa inuu helo lacago cusub oo badan, oo ka badan isku-darka kuwa kale, halkii uu ka curyaamin lahaa hannaanka, dabeetana uu hoos u dhigi lahaa kalsoonida hantidiisa.

7. Badbaadinta Qeyb Ka Mid Ah Kaydka

Marka Transaction-ka ugu danbeeya ee lacagta la galiyo Block ku filan, Transactions-yadii hore waa la tirtiri karaa, si loo badbaadiyo qeyb ka mid ah kaydka kumbiyuutarka ama Disk-ga. Si tan ay u suuragasho iyadoon la lumin oon la jabin Hash-ka Block-ga, waxaa la adeegsanayaa "Merkle Tree" (Geedka Merkle) [7][2][5], iyadoo xididka kaliya lagu darayo Block-ga. Intaa kadib, Block-yadii hore ee duugoobay waa la sii cadaadin karaa, iyadoo laamaha hoose ee geedka la jarayo. Loomana baahna in la kaydiyo Hash-yada gudaha.



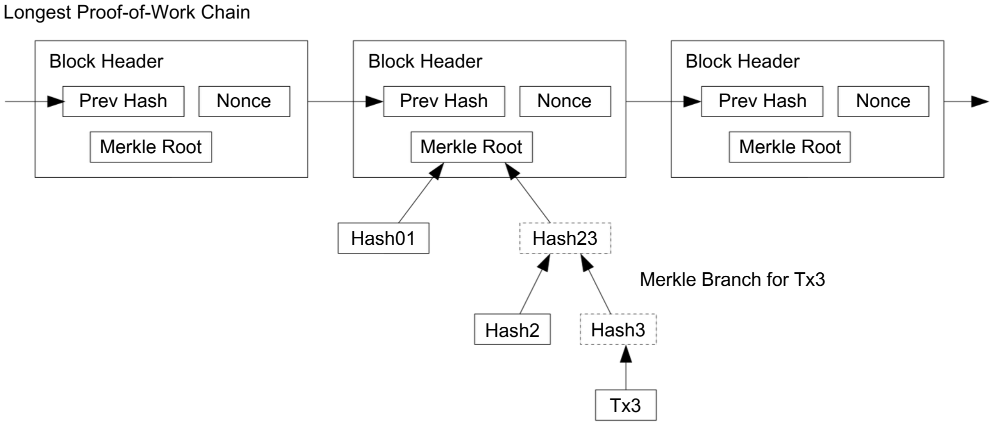
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

Madaxa (Header) Block-ga haddii uusan xambaarsaneyn wax Transaction ah wuxuu culeys ahaan noqonayaa 80 bytes. Hadii aynu ka soo qaadno in Block kasta la curiyo ama la dhaliyo 10 daqiiqo kasta, 80 bytes * 6 * 24 * 365 = 4.2MB sannadkii. Iyadoo kumbiyuutarada caadiga ahi maanta lagu iibinayo 2GB oo RAM ah, laga bilaabo 2008, wuxuuna xeerka Moore saadaalinayaa in uu 1.2GB ku kordhi doono sanad kasta, kaydintu waa inaysan noqonin dhibaatada, xittaa hadii loo baahdo in la kaydiyo madaxyada Block-ga (Block Headers).

8. Fududaynta Xaqiijinta Lacag-bixinada

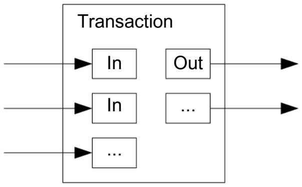
Waa suurtagal in la xaqiijiyo lacag-bixinnada iyada oo aan loo baahnayn Node dhammaystiran (Full Node). Adeegsaduhu wuxuu kaliya u baahan yahay inuu helo nuqul ka mid ah madaxyada Block-ga ee silsiladda ugu dheer, ee ku timid hab-sugid shaqo (Proof of Work), isagoo waydiisanaya Nodes-yada shabakadda ku jira ilaa iyo inta uu ku qancayo inay tahay silsiladda ugu dheer, iyo laanta Merkle ee Transaction-ka ku xidhiidhinaysay Block-ga. Adeegsaduhu isagu si iskii ah uma hubin karo Transaction-ka, hasa yeeshee isagoo galinaya ama ku xidhiidhinaya meel ka mid ah silsiladda, wuxuu arki doonaa Nodes-yo hore u aqbalay, Block-yada danbana waxay sii xoojinayaan runimadooda.



Sidaas darteed, ilaa iyo inta ay Nodes-yada daacadda ahi gacanta ku hayyaan oo ay xakameynayaan awoodda shabakadda, runimada shabakaddu waa mid la isku halleyn karo, hasa yeeshee hadii ay shabakaddu u gacan-gasho weeraryahanno waxay noqonaysaa mid u nugul halis. In kastoo ay Nodes-ku awoodaan inay si gaar ah u hubiyaan Transaction-yada, hadana habkan fudud ee lacag-dirisyada lagu xaqiijin karo ee (Simple Payment Verification), ayaa lagu khiyaami karaa, hadii uu weeraryahanku abuuro Transactions-yo been-abuur ah, waana khatar sii jiri doonta ilaa iyo inta uu weeraryahanku awood u leeyahay inuu gacanta ku sii hayyo shabakadda. Mid ka mid ah hababka looga hortagi karo waa in la aqbalo oo lagu baraarugo digniinada ka soo baxaysa Nodes-yada shabakadda marka ay arkaan Block aan sax ahayn, taasoo Software-ka adeegsadaha ku dhiirigalinaysa inuu soo dajiyo dhammaan Blocks-yada, iyo Transaction-kii lagu sheegayay inay khaldanaayeen, si loo xaqiijiyo is haleel la'aantii jirtay. Ganacsatada sida joogtada ah u helaya lacag-bixino waxay u badan tahay inaysan ka maarmi doonin, oo aysan ka fursan doonin in ay Nodes-yo iyaga u gaar ah samaystaan, si ay u helaan ammaan dheeraad ah oo madax-bannaan iyo xaqiijin degdeg ah.

9. Isku-darka Iyo Kala Reebidda Lacagta

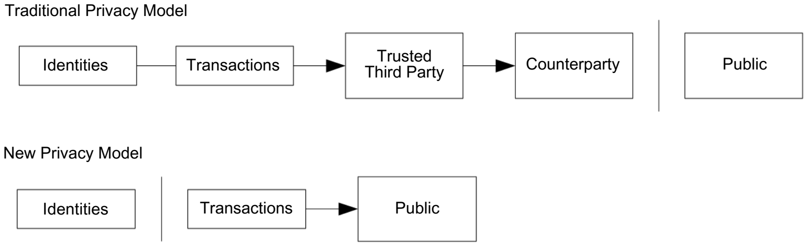
Inkasta oo ay suurtagal noqon karto in lacag kasta si gaar ah loo maareeyo, hadana waxay taasi noqon lahayd mid aan wax-ku-ool ahayn in "Sent" ($0…) kasta si gaar ah loo maareeyo, loona sameeyo Transaction u gaar ah. Si ay suurtagal u noqoto in lacagta la kala qeyb-qeybiyo, oo la kala reeb-reebo, ama la isku qaado oo la isku geeyo, Transaction kasta wuxuu ka kooban yahay dhowr galitaano (Inputs) iyo dhowr bixitaano (Outputs). Sida caadada ah waxaa jiri doona hal galitaan (Input) oo ka yimid Transaction hore oo weyn, ama dhowr galitaano (Inputs) oo la isku geeyay, iyo ugu badnaan laba bixitaano (Output): midkood waxaa loogu talagalay lacag-bixin, midka kalena waxaa loogu talagalay in hadhaaga lagu soo celiyo, hadii uu jiro, oo dib loogu celiyo diraha (Sender).



Waa muhiim in la ogaado in xaaladda loo yaqaan "fan-out", taas oo ah in halkii Transaction-ka uu ku xidhiidhsan yahay dhowr Transactions-yo kale, kuwaasina ay ku sii xidhiidhsan yihiin dhowr kale oo badan, aysan dhibaatadu ahayn. Ma jirto baahi loo qabo in la helo nuqul dhammaystiran oo madax-bannaan oo ka mid ah diiwaanka Transactions-yada.

10. Qarsoodida

Bangiyada dhaqameedka ah waxay leeyihiin heer qarsoodi gaar ah, iyagoo xogta iyo warbixinada ku xaddidaya kaliya dhinacyda ku lugta leh, iyo qolo dhexe oo kalsooni leh. Baahida loo qabo in dhamman Transactions-yada si furan (Public) loo shaaciyo suuragal kama ahan habkan, hasa yeeshee wali waa suuragal in la ilaaliyo qarsoodiga iyadoo qulqulka xogta loo bedelayo meel kale: iyadoo furayaasha furan (Public Keys) laga dhigayo kuwo sumad laawayaal ah. Dadweynuhu waxay arki karaan in uu qof lacag u diray qof kale, hasa yeeshee iyadoo aan la helin xog isku xidhaysa Transaction-ka iyo qofka wax diraya. Tani waxay la mid tahay sida suuqyada saamiyadaha ay u soo-saaraan xogaha, halkaas oo ay shaaciyaan wakhtiga ay dhacday Transaction-ka iyo xaddiga Transactions-yada, iyadoo aan la sheegin ciddii ay ahaayeen.



Si loo helo amni dheeraad ah, waa in Transaction kasta loo adeegsadaa furayaal cusub, si looga hortago aqoonsiga milkiilaha. Ogaanshiyaha qaar ayaa ah wali wax aan laga baaqan karin, hadii uu Transaction-ku ka kooban yahay dhowr galitaano (Multi-input), taasoo si ku talagal la'aan ah u muujinaysa in Inputs-yadii hore uu lahaa isla halkii qof. Khatartu waa hadii la ogaado qofka iska leh furaha, markaasna waxaa la ogaan karaa Transactions-yo kale oo isaga u gaar ah.

11. Xisaabinta

Aynu suuraysano weeraryahan isku dayaya inuu dhaliyo ama soo-saaro silsilad kale, oo ka dheer silsiladda daacadda ah. Xitaa hadii ay tani suuragasho, kama dhigna in hannaanku uu yahay mid u furan isbeddello aan loo meel dayin, sida abuurista qiimo aan jirin, ama qaadashada lacag aannuu hore u lahayn weeraryahanku. Nodes-yadu ma aqbali doonaan Transaction aan qumanayn lacag-bixin ahaan, mana aqbali doonaan Block ay ku jiraan. Weeraryahanku wuxuu isku dayi karaa oo kaliya inuu beddelo mid ka mid ah Transactions-yadiisii hore si uu dib ula soo noqdo lacagihii uu dhawaan kharash gareeyay.

Tartanka u dhexeeya silsiladda daacadda ah iyo tan weeraryahanka waxaa lagu tilmaami karaa sidii socod iska nasiib ah oo laba-geesood ah. Guushu waxay tahay marka silsiladda daacadda ah ay ku korodho hal Block, taasoo horseedaysa inay hal talaabo horey uga sii kacdo silsiladda weeraryahanka, kuna hogaamisa +1, guuldaraduna waxay tahay marka silsiladda weeraryahanka ay hesho hal Block, taasoo abuuraysa gaabis dhan -1.

Suurtagalnimada in weeraryahanku meel hoose kala soo qabsado silsiladda waxay la mid tahay xaalad la yidhaahdo Gambler's Ruin. Aynu ka soo qaadno in uu jiro khamaarle khasaare ku jira, oo haysta Credit ama lacag aan dhamaad lahayn, iyo isku day aan dhamaad lahayn, si uu is kugu dayo inuu ka soo kabsado khasaaraha, oo uu u yimaado barbardhicii, ama meesha ay lacagtiisu ka bilaabmaysay. Waynu xisaabin karnaa suurtagalnimada uu ku gaari karo barbardhaca, ama uu ku gaari karo silsiladda daacadda ah, iyadoo la raacayo [8]:

p = suurtagalnimada uu Node-ka daacadda ah ku heli karo Block-ga xiga
q = suurtagalnimada uu weeraryahanku ku heli karo Block-ga xiga
q_z = suurtagalnimada uu weeraryahanku ku gaari karo silsiladda hadii uu ka danbeeyo z Block

$$q_z = \begin{Bmatrix} 1 & \text{if } p \le q \\ \left(\frac{q}{p}\right)^z & \text{if } p > q \end{Bmatrix}$$

Inagoo ka duulayna malaheena ah in p > q, suurtagalnimada uu weeraryahanku ku soo gaadhi karo silsiladda daacada ah ayaa si xad dhaaf ah hoos ugu dhacaysa, marka uu Blocks-yo badan ka danbeeyo. Iyadoo ay markii horeba fursaduhu ka soo horjeedeen, haddii uu nasiib u yeelan waayo inuu goor hore bilaabo, fursadiisu waxay noqonaysaa mid aad u yar, mar kasta oo uu sii danbeeyo.

Haatan waxaynu ka hadlaynaa muddada ay qaadanayso in uu sugo qofka lacagta loo dirayo ka hor inta uusan si buuxda u hubin in qofka lacagta diraya uusan ka noqon karin ama wax ka bedeli karin Transaction-ka. Aynu ka soo qaadno in diraha ama qofka lacagta diraya uu yahay weeraryahan kaasoo raba in loo-diruhu ama qofka lacagta helaya u maleeyo in lacagta loo diray wakhti ka hor, oo uu kadibna qorshaha bedelo oo uu lacagta la noqdo wakhti yar ka dib. Qofka lacagta helaya ama qaataha ayaa markaaba la ogaysiinayaa in wax la bedelay, halka qofka lacagta diraya uu jeclaan lahaa in goor danbe la ogaado.

Loo-diraha wuxuu abuurayaa fure cusub oo lammaane ah (Public Key & Private Key) wuxuuna furaha guud (Public Key) u dirayaa oo uu siinayaa diraha wax yar ka hor inta uusan saxiixin. Tani waxay ka hortagaysaa in diruhu uu diyaariyo silsilad Block-yo ah wakhti yar ka hor isagoo si joogto ah uga shaqeynaya ilaa iyo inta uu nasiib ku filan u yeelanayo inuu meel fog gaadho, kadibna uu isla wakhtigaas fuliyo Transaction-ka. Mar allaale markii Transaction-ka la diro diraha aan daacadda ahayn wuxuu bilaabayaa inuu si qarsoodi ah hoos uga shaqeeyo silsilad cusub oo barbar socota tan qumman, taasoo sidda ama xanbaarsan Transactions-yo bedel ka ah kuwii qummanaa.

Loo-diraha waa inuu sugaa ilaa iyo inta Transaction-ka lagaga darayo Block, kadibna ay ka soo wareegayso z Block. Loo-diruhu ma garan karo heerka ama tallaabada dhabta ah ee uu marayo weeraryahanku, hasa yeeshee inagoo ka soo qaadayna in Block-ga daacadda ah qaato celcelis ahaan wakhti go'an oo la filayo (10 daqiiqo), markaas tirada Blocks-yada ee uu weeraryahanku abuuri karo waxaa lagu soo saaraa Poisson Distribution, iyadoo leh qiimo la filayo:

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

Si aan u ogaano suurtagalnimada uu wali weeraryahanku ku awoodi karo inuu soo gaadho silsiladda daacadda ah, waxaynu qiimeynta loo yaqaan Poisson, ku dhufanaynaa koror kasta ama tallaabo kasta ee uu awoodi karo inuu qaado weeraryahanku, iyo fursadda uu uga soo kaban karo meel kasta uu markaas joogo:

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

Xeerkii oo dib-u-habayn lagu sameeyay, lana soo koobay, si looga baaqsado suurtagalnimada yaryar ee aan dhamaadka lahayn…

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

Iyadoo Code ahaan loo rogay, gaar ahaan afka C ...

```
#include <math.h>
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;
}
```

Natiijooyinka qaar, waxaynu arki karnaa in ay suurtagalnimadu si xawli ah hoos ugu dhacayso, mar kasta oo ay tirada z korodho.

```
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
```

Suurtagalnimada ama kanshada P oo ka hoosaysa 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
```

12. Gabagabada

Waxaan soo jeedinay hannaan lacag-diris oo danabaysan (Electronic), oo aan ku tiirsanayn kalsooni. Xalkeenu wuxuu ka bilawday hannaanadii dhaqameedka ahaa, ee ku salaysnaa saxiixyada dhijitaalka ah, kaasoo si wacan u caddaynayay lahaanshaha lacagta ama cidda leh lacagta, hasa yeeshee aan dhammaystirnayn iyada oo aan la helin hab looga hortagayo kharash garaynta laban-laaban (Double Spending). Si dhibkan loo xalliyo, waxaan soo jeedinay shabakad qof-ka-qof ah (peer-to-peer) iyadoo la adeegsanayo hab-sugid shaqo (Proof of Work) si loo helo diiwaan guud oo lagu diiwaan galiyo Transactions-yada taasoo si degdeg ah u noqota mid xisaab ahaan aan suurtagal ahayn in la soo weeraro, haddii Nodes-yada daacadda ahi ay xakameynayaan awoodda CPU ee ugu badan. Awoodda shabakadda waxay ku jirtaa fudaydkeeda aan qaabaysnayn. Dhammaan Nodes-yada shabakadda isku mar bay wada shaqeeyaan iyadoo aan isku xidhnaanshiyo buuxda jirin. Looma baahna in la aqoonsado Nodes-yada, maadaama aan loo baahnayn in fariimaha meel gaar ah loo gudbiyo, ee kaliya loo baahan yahay in si wax-ku-oolnimo leh loo gudbiyo. Nodes-yadu way ka bixi karaan, dibna way ugu soo laaban karaan shabakadda goorta ay doonaan, iyagoo aqbalaya silsiladda ugu dheer, taasoo caddayn u ah wixii dhacay intii ay maqnaayeen. Nodes-yada ayaa codayn kara iyagoo adeegsanaya awoodda kumbiyuutaradooda CPU, iyagoo aqbalaya Blocks-yada qumman iyagoo ka shaqeynaya ballaarintooda sidoo kalena diidaya Blocks-yada aan qummanayn iyagoo diidaya inay ka shaqeeyaan. Wax kasta oo xeer iyo dhiirigelin ah oo loo baahan yahay waa lagu dhaqan gelin karaa hannaankan is-afgarad ee wada-jirka ah.

Tix-raacyada

[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.