Sharraxid: Bitcoin Whitepaper

Waa sharrax hufan oo kala saar-saaran, oo si waafi ah u faahfaahinaya xaashida cad ee Bitcoin ee la qoray sanaddii 2008-dii. Bitcoin Whiteaper waa xaashi si weyn u saameeyay dunida dhaqaalaha, waana xaashi xallinaysa dhibaatooyin waa-weyn oo dhaqaale, oo muddo badan jiray.

Nabadi korkaaga ha ahaato.

Kadib markii anaga oo ah "CryptoYahan.com↗" turjumnay xaashida ama Whitepaper-ka Bitcoin, waxaynu dareenay in aanay turjumaanimadoo qudha ku filnayn, si ay bulshadeena soomaaliyeed u fahamto cilmi-baadhistan.

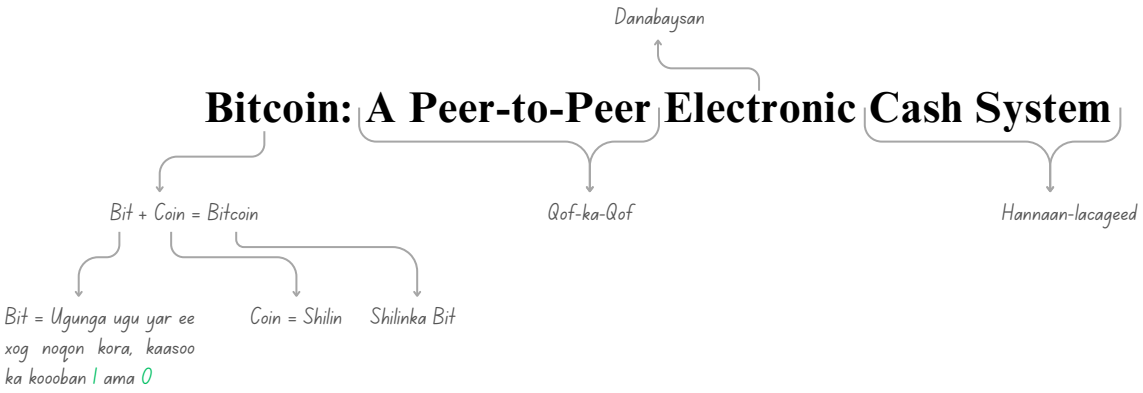
Sidaa darteed, waxaynu mar labaad isa saarnay xil kale, oo ah inaynu sharraxno, oo aynu faahfaahino, oo aynu kala dhig-dhigno aragtiyooyinka waa-weyn, dhinacyada kala duwan, sida xisaabta, tignoolajiyadda, iwm, si si qoto dheer leh oo buuxda loo fahmo.

Xaashidan ama Paper-kan oo la qoray sannadii 2008-dii, taasoo ka kooban 9 bog, waxay noqotay mid ka mid ah is-bedelada ugu waa-weyn ee dhaqaale, ee dhacay qarnigan 21-aad, xaashidaasoo si cilmiyaysan u sharraxaysa hannaan-lacageed cusub oo danabaysan (Electronic), oo qof-ka-qof ah (P2P), iyadoon loo baahnayn wax dhaxdhexaadin ah haba yaraatee.

Xaashidan waxay xanbaarsan tahay aragtiyo waa-weyn, oo u muuqda inay adag yihiin, taasoo keensanaysa in xittaa hadii la turjumo aysan ka fursan karin in la sii sharraxo oo la sii faahfaahiyo, waana sababta keentay inaynu sharraxno.

Hordhac intaa ha inagaga ekaado… aynu si toos ah u guda-galno sharraxa...

Sharraxid: Bitcoin Whitepaper



Bitcoin: Hannaan Lacageedka Danabaysan Ee Qof-Ka-Qof

Abstract. *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.*

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.*

Satoshi ayaa hadalkiisa ku bilaabay, Bitcoin waa hannaan suuragalinaya in ay laba qof ama laba qolo si toos ah wax isu-waydaarsadaan, iyadoon dhexdooda ku jirin qolo saddexaad.

Wuxuuna Satoshi rabaa in la helo hannaan lacageed oo madax-bannaan, kana madax-bannaan cid kasta, haday noqon lahayd urur maaliyadeed, bangi, dawlad, amaba si guud qolo kasta oo dhexdhexaadiye ah, oo kalsooni leh, oo lacag-dirisyada la sii dhex marsiiyo.

TS, Maanta haddii aad rabto inaad lacag dirto, adigoo adeegsanaya adeegyada lacag-bixineed ee dhaqameedka ah, ee danabaysan, lacag kasta oo aad dirto waxay sii dhex martaa cidda aad adeegooga adeegsanayso, oo ah qolodii dhexe, iyagoo awood u leh inay lacag-diristaada xannibaan, ama xayiraan, ama in muddo ah hakiyaan, amaba diidaan, iwm.

Satoshi-na wuxuu rabaa in la helo hannaan lacag-bixineed oo si buuxda u madax-bannaan, oo loo wada siman yahay, isla mar ahaantaana dadka u ogolaanaya in si toos ah wax isku dhaafsadaan, iyagoon ku khasbanayn in ay u baahdaan qolo saddexaad, si uu is-dhaafsigoodu u hirgalo.

Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

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.

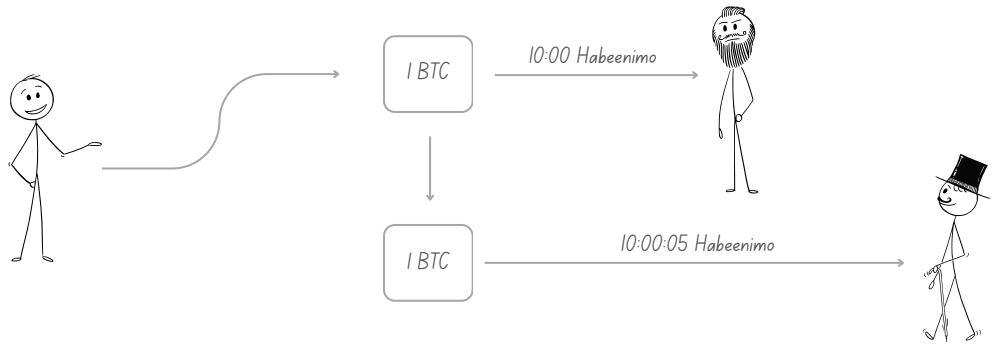
Halkan wuxuu Satoshi u tallaabay qaabkii loo hirgalin lahaa, isagoo ka bilaabay farsamooyinka, sida "Digital Signatures", oo la mid ah saxiixyadii caadiga ahaa ee aynu naqaanay, kaasoo cadaynayay aqoonsiga qofka, ama ogolaanshiyahiisa.

Sidaas oo kale, Digital Signatures waxay caddaynayaan aqoonsiga qofka diray lacagta, taasoo xaqiijinaysa in cidda dirtay lacagta ay ahayd ciddii sida dhabta ahayd u lahayd, maxaa yeelay waxaa ku yaala saxiixeeda, iyadoon la ogaanayn cidda ay sida dhabta ah yihiin, sida magacooda, da'dooda, goobta ay joogaan, iwm.

Isagoo Satoshi sii wada hadalkiisa wuxuu yidhi, waxaa la lumin doonaa dheefihii ugu waa-weynaa hadii ay wali sii jirto baahidii loo qabay qolo saddexaad, oo kalsooni leh, si ay uga hortagaan kharashgaraynta laban-laaban.

Double Spending-kan ama kharashgarayntan laban-laaban ee uu Satoshi ka hadlayo waa dhib weyn oo si guud bilawgii lacagaha danabaysan (Digital Money) u haysatay, halkaas oo la awoodi jiray in isla lacagtii la-laba jeer adeegsado. Waana in isla lacagtii wax ka badan hal jeer la kharashgareeyo, ama la diro.

TS, qof ayaa 1 Bitcoin u diraya qof kale, isla qofkii ayaa hadana isla 1-kii Bitcoin u diraya qof kale, oo aan ahayn qofkii hore, isagoo si toos ah u bedelaya xogtii lacag-bixineed, kana dhigaya in aanuu hore wax Bitcoin ah u dirin, ee ay markan tahay markii ugu horraysay.



Sidaa darteed, xalka ugu soo dhaw wuxuu ahaa in la helo qolo dhexe ama dhinac dhexe, oo saddexaad, oo lagu kalsoonaado, si ay uga hortagaan kharashgarayntan laban-laaban, ama Double Spending-ka, taasoo ka hor imanaysa aragtida Bitcoin, ileen Satoshi wuxuu rabaa inuu dhiso hannaan lacag-bixineed oo madax-bannaan, oo aan ku tiirsanayn dhinac saddexaad, si looga hortago Double Spending-ka.

> *We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.*
>
> *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.*

Kadib markii uu Satoshi sheegay in aysan Digital Signatures-ku ahayn xalka buuxa, oo aan si wax-ku-oolnimo leh uga hortagi karin Double Spending-ka, wuxuu haatan soo jeedinayaa xal, kaasoo ah in la adeegsado shabakad ama hannaan qof-ka-qof ah, ama dhinac-ka-dhinac ah.

Intaynaan u sii dhaadhicin hadalka Satoshi, aynu ereyada qaar si kooban u qeexno:

- **Timestamps:** Waa shaanbad/tiinbaro caddaynaysa wakhtiga dhabta ah ee ay dhacdo dhacday
- **Proof of Work:** Waa hab lagu sugayo, laguna xaqiijinayo runimada xogta, iyadoo la qabanayo shaqo
- **Hash:** Waa natiijo ka dhalata markii xog la bedelo, oo la sii marsiiyo hab gaar ah, si loo helo natiijo gaar ah oo aan is-bed-bedelin, si loo xaqiijiyo runimada xogta, taasoo hadii wax yar xogta laga bedelo, uu is bedelayo dhammaan Hash-kii. Waana sidii summad oo kale.

Xalkii uu Satoshi soo bandhigay ee ahaa in la adeegsado hannaan qof-ka-qof ah, si looga hortago kharashgaraynta laban-laaban, waxay u baahan tahay in Transaction kasta ama lacag-diris kasta lagu shaanbadeeyo shaanbad wakhtiyaysan, taasoo sheegaysa wakhtigii ay dhacday, iyadoo la Hash-garaynayo, kadibna lagu xidhiidhinayo silsilad ama diiwaan is-daba-joog ah oo taxane ah, iyadoo la adeegsanayo Proof of Work ama hab-sugid shaqo, taasoo abuuraysa diiwaan dheer oo is-daba-taxan oo aan wax laga bedeli karin.

Transaction kasta ama lacag-diris kasta kadib waa la Hash-gareeyaa, Hash-kaasoo ah sumad gaar ah oo lagu aqoonsanayo lacag-diristan, hadii markaa la isku dayo in wax laga bedelo lacag-dirista waxaa is bedelaya sumadii lacag-dirista, hadii ay summadii is bedeshana waxaa is bedelaya dhamaan waxyaabihii ka danbeeyay oo idil.

Hadii wax yar laga bedelo xogta lacag-dirista, waxaa is bedelaya Hash-ka gabi ahaantii, xitaa hadii isla hal shibane wax laga bedelo sida "**N**" → "**n**", ama lagu daro wax yar "**N.**", sidan halkan hoosaba ka muuqata:

Isbedel kastoo yar oo lagu sameeyo xogta, waxaa gabi ahaanba is bedelaya Hash-ka, taasoo ina tusinaysa runnimada xogta, sababtoo ah hadii xogta lacag-dirista wax yar laga bedelo waxaa gabi ahaanba is-bedelaya Hash-kii.

Hannaanka uu Satoshi soo bandhigay waa lacag-dirisyo is-daba taxan oo xidhiidhsan, hadii mid ka mid ah wax laga bedelo waxaa is bedelaya dhammaan wixii ka danbeeyay, waana sabata loo yidhi "Chain Hash-based" silsilad is-daba taxan oo ku dhisan Hash ama sumad.

Waxaana habkaas oo idil, laga bilaabo lacag-dirista, shaanbadaynta, Hash-garaynta, ilaa lagu xidhiidhinayo lacag-dirisyadii ka horreeyay, sidaasina lagu samaynayo silsilad ama diiwaan is-daba-taxan oo xidhiidhsan loo yaqaanaa "Proof of Work", hadii aynu soomaaliyeenana noqonaysa hab-sugid shaqo.

Si loo Proof gareeyo ama loo sugo runimada lacag-dirisyada waa in la qabto shaqo, shaqadaasoo sida aynu hore u soo sheegnay ka kooban dhowr shaqo oo is-daba-taxan.

Waxaana sidaas ku samaysmaya diiwaan is-daba-taxan, oo midba midka kale ku xidhiidhsan yahay sidii silsiladda, hadii la rabana in wax laga bedelo ama wax lagu biiriyo, waa in hadana shaqo kale la qabto.

> *The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.*
>
> *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.*

Isagoo Satoshi sii xoojinaya hadalkiisa wuxuu tilmaamay in aysan silsiladda ugu dheer ama diiwaanka ugu dheer ahayn oo kaliya diiwaan caddaynaya sida ay iskula xidhiidhsan yihiin dhacdooyinka ama lacag-dirisyda, ee waxay sidoo kale caddaynayaan in ay ka timid isku-imaatinka ugu weyn ee shabakadda.

Satoshi wuxuu dajiyay xeer ah in silsiladda ugu dheer ay mar waliba tahay tan quman ee ay shabakaddu mar waliba qaadanayso, maxaa yeelay silsiladda oo loola jeedo Blockchain ee ugu dheer, waxay muujinaysaa in ay tahay silsilad la galiyay shaqadii ugu badnayd, haday noqon lahayd wakhti, iyo tamar badan, ama awood kumbiyuutar badan.

Bitcoin sida kaliya ee ay ku aqoonsato silsiladda quman waa dhererkeeda. Had iyo jeer silsiladda ama Blockchain-ka ugu dheer baa ah kan ay shabakaddu qaadanayso, una tixgalinayso inay tahay tan quman, waa hadii se ay silsilad kale ka soo barbar baxdo.

Maxaa yeelay waxaa mararka qaar suuragal ah in laba Block isku mar la wada helo, halkaas oo ay ka dhalanayso silsilad kale oo barbar socota silsiladii hore.

Labada silsiladood waxy u muuqan karaa laba quman, hasa yeeshee shabakadu iyadu xeer kale ayay leedahay, qumanaantana waxay u taqaanaa dhererka, haddaba sidii loo socdaba ugu danbayn khasab labada silsiladood midkood ayaa hor heli doona Block cusub, iyadoo noqon doonta silsiladda ugu dheer, taasoo ay shabakadu u aqoonsanayso inay tahay tan quman, isla mar ahaantaana qaadanayso.

Waayo silsiladda ugu dheer had iyo jeer waxay tusinaysaa in ay dad badan ka hawlgaleen, sidoo kalena la galiyay tamar badan, qofnana meel aan waxba ka jirin ma uusan galiyeen tamar badan, ama wakhti badan.

Sidaa darteed, silsiladda ama Blockchain-ka ugu dheer kaliya markhaati kama ah runimada lacag-dirista, ee sidoo kale waxay markhaati ka tahay in ay ka timid isku-imaatinka ugu weyn ee shabakadda.

Maadaama uu Satoshi xaashidan qoray 2008, wakhtigaas waxaa la adeegsan jiray kumbiyuutaro CPUs leh, si loo sugo lacag-dirisyada ama loo sameeyo Proof of Work, hasa yeeshee haatan 2025, 16-sano 6-bilood 18-maalmood 20-saac 27-daqiiqo 26-ilbiriqsi kadib aasaaska Bitcoin waxaa la adeegsadaa qalabo ASIC ah oo aad iyo aad uga awood badan CPU-ga, iyo mararka qaar kumbiyuutaro GPUs leh oo awooddoodu dhexdhexaad tahay.

Sidaa darteed, hadii aynu marar badan aragno Satoshi oo leh CPU Power, wuxuu ula jeedaa awoodda kumbiyuutarada, taasoo maanta aad iyo aad u hormartay, heer si gaar ah loo soo saaro qalabo loogu talagalay in Proof of Work lagu sameeyo, kuwaasoo lagu magacaabo ASIC.

- **CPU:** Oo loo soo gaabiyo Central Processing Unit, waa qaybta aasaasiga ah ee mas'uulka ka ah fulinta amarada, ahna qeybta kala socodsiisa hawlaha kumbiyuutarka, waana xudunta kumbiyuutarka, hasa yeeshee wuu gaabis badan yahay, markii ay timaado Proof of Work ama Mining-ka oo ah falkii.
- **GPU:** Oo loo soo gaabiyo Graphics Processing Units, isagu wuxuu ka wax tar badan yahay CPUs-ka markii ay timaado Proof of Work, waxaana la odhan karaa wuu ku fiican yahay Mining-ka
- **ASIC:** Oo loo soo gaabiyo Application-Specific Integrated Circuits, waa qalabka wakhti xaadirkan ugu awoodda badan markii ay timaado Proof of Work, waana qalab loo sameeyay halkaas ujeedo, kaasoo ilbiriqsigii qaban kara shaqo badan

> *As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.*
>
> *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.*

Maadaama ay shabakadu mar waliba u hogaansan tahay silisladda ugu dheer, wuxuu Satoshi leeyahay amniga shabakadda waxay ku xidhan tahay kaalinta ay hayyaan qolada loo yaqaan "Nodes", oo ah kumbiyuutaro ku xidhan shabakadda Bitcoin, kuwaasoo ansixinaya is-dhaafsiyada shabakada ka dhex socda, sidoo kalena suga amniga shabakadda, waana laf-dhabarta Bitcoin.

Hadii ay Nodes-yada badankood daacad yihiin shabakaddu way sii socon doontaa, hadii kalena, shabakaddu waxay u nuglaan doontaa amni xumo, been-abuur, iyo xitaa baaba'.

TS, hadii 90% awoodda shabakadda ay gacanta ku hayyaan dadyow daacad ah oo wanaagsan, oo aan ujeedkooda ahayn inay shabakadda weeraraan, halka 10%-ka kale ay yihiin dadyaw aan daacad ahayn oo raba in ay shabakadda weeraraan, ma awoodi doonaan, maxaa yeelay waxay kaliya gacanta ku hayyaan 10%, lamana tartami karaan kuwa daacadda ah, iyadoo sidaasi uu ku dhicisoobi doono weerarka.

Sidaa darteed, Satoshi wuxuu yidhi, Ilaa iyo inta dadyowga wanaagsan ama Nodes-yada daacadda ahi gacanta ku hayyaan awoodda shabakadda inteeda badan, shabakaddu waa mid amaan ah, oo iska caabin karta weerar kasta.

> *The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*
>
> *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.*

Halkan Satoshi wuxuu tilmaamayaa in aysan shabakaddu u baahnayn qaab-dhismeed adag, oo kakan, oo qallafsan, iyo in waddooyin badan la maro si ay shabakaddu si hufan ugu shaqayso, waana sababta uu u yidhi: "The Network Itself Requires Minimal Structure".

Fariimaha ama Messages-yada uu Satoshi ka hadlayo waa Transactions-yada iyo Blocks-yada, kuwaas oo la iskugu kala gudbiyo sidii ugu wax-tarka badnayd.

In kastoo aan la isku hallayn karin, oo 100% loo damaanad qaadi karin in ay fariimuhu si degdeg leh u gaadhi doonaan dhammaan Nodes-yada shabakadda ku jira, hadana shabakaddu waxay ku dadaali doontaa in ay fariimaha u gaadhsiiso sidii ugu wax-ku-oolnimada badnayn.

Halkan Satoshi wuxuu leeyahay, maadaama aysan jirin xarun dhexe oo laga maamulo geedi-socodka shabakadda ka socda, fariintaada ama lacag-diristaada 100% looma damaanad qaadi karo in ay si dhakhso leh u arki doonaan Nodes-yada shabakada ku jira, hasa yeeshee shabakaddu waxay ku dadaali doontaa in sidii ugu dadaalka badnayd fariimahaaga u gaadhsiiso Nodes-yada, fariimahaas oo loo la jeedo lacag-dirisyada iyo Blocks-yada ay ku jiraan lacag-dirisyada, maxaa yeelay Block kasta waxaa ku jira tiro lacag-dirisyo ah.

Sidoo kale Satoshi wuxuu xusay in ay Nodes-yadu xor yihiin, oo ay awoodaan inay si fudud oo shuruud la'aan ah uga baxaan shabakada, sidaa si la mid ahna ugu soo laaban karaan, waliba goor allaale goorta ay doonaa, iyagoon u baahanin ogolaanshiyo.

Mar allaale markii uu Node-ku shabakadda ku soo laabto, uma baahna inuu cid kale wax waydiiyo, oo uu warsado wixii dhacay intii uu maqnaa, kaliya wuxuu aqbalayaa silsiladda ugu dheer, taasoo loo aqoonsan yahay inay tahay silsiladda ama Blockchain-ka ugu dheer ee ay isku raaceen Nodes-yadii kale ee shabakadda ku sii jiray, markii uu isagu hawada ka maqnaa.

Hadii aynu si kale u dhigno, Markuu Node-ku dib ugu soo noqdo shabakadda, ma jiro qof uu wacayo, si uu u helo xogtii dhaaftay intuu maqnaa, mana jiro Server ama maamul dhexe oo uu codsiga u gudbinayo, kaliya wuxuu si toos ah u arkayaa silsiladda ugu dheer ee ay shabakaddu sii dhistay intii uu maqnaa, wuuna aqbalayaa.

Nodes-yada iyagoon is aqoon, iyagoon isku wakhti ahayn, iyagoon isku deegaan ahayn, iyagoon isku xidhnayn, iyagoon isku tirsanayn, ee uu mid waliba si madax-banaan u taagan yahay ayay hadana si hufan isku la shaqeeyaan, oo uu mid waliba goorta uu doono ka bixi karaa shabakadda, kuna soo laaban karaa, isagoon cidna ogolaanshiyo waydiisan, waana sababtaas sababta uu Satoshi u yidhi: "Shabakaddu uma baahna hab-maarayn adag, si ay u shaqayso".

1. Introduction (Hordhac)

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

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.

Qeybtan 1-aad, wuxuu qoraagu ku sheegayaa in ganacsiyada internet-ka ka jira aysan 100% u madax-bannaanayn ganacsigooda, maadaama ay ku khasban yihiin in ay ku tiirsanaadaan qolo saddexaad oo fudaydisa lacag-bixinada.

Halkan Satoshi wuxuu rabaa inuu aragtidiisa ka dhaadhiciyo ganacsatada Online-ka ah, isagoo ku baraarujinaya dhibaatada haysata, ee ah baahida loo qabo qolo saddexaad, oo lagu kalsoonaado, si ay u fudaydiyaan lacag-dirisyada u dhaxaysa macmiilka iyo ganacsadaha.

Isagoo hadalkiisa sii watta, wuxuu yidhi in kastoo qaabkan inteeda badan mira-dhalkiisu wacan yahay, hadana wali wuxuu leeyahay dhinac aad u liidata, waana in uu ku tiirsan yahay kalsooni.

Satoshi wuu qirsan yahay in qaabkan kalsoonida ku tiirsan wali wax-ku-ool yahay, hadana wuxuu tilmaamayaa in aysan sal adag ku taagnayn.

Maxaa yeelay Satoshi wuxuu rabaa in kalsoonida ama is-aaminidda (Trust) waxa la yidhaahdo uu gabi ahaanteed meesha ka saaro, wuxuuna u arkaa dhibaato weyn.

Waayo kalsoonidu waxay u nugushahay waxyaabo badan: waa la wiiqi karaa, waa la dhimi karaa, waa la burburin karaa, sidoo kale siyaabo khaldan ayaa loo adeegsan karaa. Sidaa darteed ma ahan sal ama qaab-dhismeed adag oo wax lagu dhisi karo.

Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services.

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.

Qoraagu halkan wuxuu tilmaamayaa dhibaato kale, oo uu hannaankan dhexe ee kalsoonida u baahan leeyahay, waana in uusan lahayn lacag-bixin aan ka noqoshada aqbalin, iyo kharashyada dheeraadka ah ee ka dhasha dhexdhexaadinta.

Satoshi wuxuu leeyahay hannaankan dhexe ee kalsoonida ku tiirsan kuma habboona lacag-dirisyada, sabab la xidhiidha in laga noqon karo darteed.

TS, hadii uu qof si Online ah wax u iibsado, wixii uu iibsadayna uu ku doodayo in uusan helin, ama uu helay iyadoo ay wax ka dhiman yihiin, amaba ay jaban yihiin, iwm, bangigii ama qolodii dhexe ee ay lacagtu sii dhex martay ayaa soo fara-galinaya, si uu xal ugu helo khilaafkan soo kordhay.

Taasi micnaheedu waa in uu bangigu ama qoloda dhexe ay awood u leedahay in ay lacagta dib ugu celiso hadii uu macmiilku ku guulaysto doodda, halkaasina uu ganacsadihii ku waayo lacagtii.

Sidaa darteed, bangigu ama qoloda dhexe waxay awood u leeyihiin in ay dib u celiyaan lacag-dirisyadii fulay, hadii ay cabasho ama muran soo kordho, oo soo kala dhex galo labadii qolo ee ay u dhaxeeyeen ee kala ahaa macmiilka iyo ganacsadaha ama iibsadaha iyo iibiyaha.

Intaa uun ma ahee, xallinta iyo dhexdhexaadinta khilaafyada soo kala dhex gala labada dhinac ee iibsadaha iyo iibiyaha ah, waa kharash fuushan oo saaran lacag-diristii.

Faragalinta uu samaynayo bangigu ama qolada dhexe waa kharash ku kordhaya qiimaha lacag-dirista, si ay u xalliyaan murankii soo kordhay, taasi waxay meesha ka saaraysaa lacag-dirisyadii yar-yaraa, maadaama aysan wax micno weyn oo saas ah soo kordhinayn, sida lacag-diris qiimaheedu yahay $0.30, khidmadeeduna tahay $0.30 amaba mararka qaar ka badan oo go’an (fixed).

TS kale, hadii uu qof ku doodayo in la khiyaamay, ama uu ku doodayo in aanuu helin badeecadii ama adeegii uu iibsaday, wuxuu bangigu ku khasban yahay inuu arinkan soo faragaliyo, isagoo hubinaya sidii ay wax u dhaceen, wuxuuna bangigu ku khasban yahay inuu yeesho hawl-wadeeno qaabilsan cabashda macaamiisha, kuwaasoo sameeya baadhitaano dheeraad ah, oo mararka qaar qaadan kara maalmo iyo todobaadyaba, waxaana socda kharash iyo wakhti, kaasoo fuulaya lacag-diristii.

Sidaa darteed, lacag-dirisyadii yar-yaraa iyagu meesha way ka baxayaan, waayo waxa la bixinayo iyo kharashka soo dallacmaya iskuma miisaanna, ama iskuma habboona, sida lacag-diristii deeqda ahayd ee $0.20 ee fuulayay $0.40, amaba si guud iibsiga waxyaabaha yar-yar, taasoo keensanaysa in laga tanaasulo.

Wuxuu kaloo Satoshi yidhi, intaas waxaa dheer, in ay jirto dhibaato kale oo ka weyn tii hore, waana in adeegyada aan laga noqon karin aysan iyagu lahayn hab lacag-bixineed oo aan laga noqon karin (Non-reversible Payment), taasoo keenaysa in adeeg-bixiyuhu uu had iyo jeer niyad-samaanin, halka uu iibsaduhu haysto fursad uu dib ula soo laaban karo lacagtii kadib markii uu helay adeega.

TS, hadii uu qof si Online ah u iibsado adeeg aan laga noqon karin, sida tababar la helay, filim la daawaday, Software la adeegsaday, oo dhammaantood ah adeeg mar hadii la bixiyo aan dib looga noqon karin, kadibna uu cabasho ka keeno, isagoo ku doodaya in uusan sidii uu rabay ahayn, isla mar ahaantaana codsanaya in lacagta dib loogu soo celiyo, waxaay taasi halis ku tahay adeeg-bixiyaha, maadaama uu bixiyay adeegii.

Halkan Satoshi wuxuu tilmaamayaa in hannaanka hadda jira uu kaliya ilaaliyo iibsadaha, balse uu khatar galinayo adeeg-bixiyaha aan adeegiisa ka noqoshada aqbalin. Hadiiba la awoodi karo in lacagta dib loo celiyo mar waliba, markaa iyada ah ma jirto meel uu adeeg-bixiyuhu si buuxda ugu kalsoonaan karo in lacagta uu helayo aan dib looga ceshan doonin.

> *With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.*
>
> *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.*

Hadiiba lacag la diray dib loo soo celin karo (Reversal), waxaa sii kordhaysa baahidii loo qabay kalsoonida. Mar alaale markii dhibaato hor leh soo baxdo, hadii loo sii baahanayo kalsooni badan, oo ay kalsoonidu iyo is-aaminaadu noqoto xalka ugu horreeya ee loo jeesto, kalsoonidaas oo aan waliba 100% xallinayinin dhibaatada, wuxuu hannaankaas u nugul yahay god-doloolooyin badan.

Wuxuuna Satoshi yidhi waa inay ganacsatadu ama iibiyayaashu ka feejignaadaan macaamiishooda ama cidda ay wax ka iibinayaan, kana digtoonaadaan dhagaraha ay maleegayaan, si aysan khasaaro u soo gaadhin.

Taasina waxay keensanaysaa in aan si fudud kolka hore macmiilka lagu aaminin, ilaa laga uruuriyo xogo dheeraad ah, sida magaca, iimaylka, iyo mararka qaar aqoonsiga qofka iyo cinwaanka gurigiisa, iwm, oo baaqsan lahaa hadii la heli lahaa hannaan aan kalsooni ku dhisnayn.

Waxayna waxaas oo idil wax kala iibsigii ka dhigayaan mid culus, oo gaabis badan, oo xaddidan, oo mararka qaar wali u sii baahan kalsooni badan, maxaa yeelay waxaa suuragal ah in xittaa xogihii la uruurinayay laga been-abuuro, taasoo keensanaysa in hadana kalsooni dheeraad ah loo sii baahdo.

Satoshi hadalkiisa oo kooban, wuxuu rabaa inuu dadka ka dhaadhiciyo ilaa iyo inta uu hannaanku ku tiirsan yahay kalsooni iyo is-aaminaad, hannaankaas waa mid liitta, oo aan mira-dhal wacan lahayn.

> *A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.*
>
> *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.*

Heer go'an oo khiyaanada ka mid ah waxaa loo arkaa wax aan laga baaqsan karin, sidaa darteed, Satoshi wuxuu yidhi hannaanada dhaqameedka ah, waxay si dabiici ah u aqbalaan boqolley go'an oo ka mid ah khiyaamada, maxaa yeelay hannaankan si kastoo kalsooni badan loo siiyo, si 100% ah loogama baaqsan karo khiyaamada.

Satoshi-na xal uma arko aqbalaadda, xitaa hadii ay tahay in yar. Marba hadii uusan hannaanku iska caabin karin, iskana difaaci karin wax yar oo khiyaano ah, hannaankaas waa mid liitta.

Isagoo hadalkiisa sii watta wuxuu yidhi, sida kaliya ee looga baaqsan karo khiyaanada, ama ugu yaraan hoos loo dhigi karo, oo la gaarsiin karo heer aad iyo aad u hoosaysa waa in si fool-ka-fool ah wax loo kala iibsado, iyadoo waliba la adeegsanayo lacag jidhitaan jidheed leh, sida lacagta xaashida ah, ama tan shilimaadka ah.

Maxaa yeelay, hadii si fool-ka-fool ah wax loo kala iibsado, isla mar ahaantaana la adeegsado lacag jidhitaan jidheed leh waxaa hoos u dhacaysa heerkii khiyaanada, ilaa ay ka gaadhayso eber, waayo labada qolaba way is-hor-joogaan, waxa ay is-dhaafsanayaanna gacantay ku kala hayyaan. Wuxuuna Satoshi yidhi, ilaa haatan (2008) ma jirto hab ama hannaan lacag-bixineed oo Online ah, oo madax-bannaan, oo aan ku tiirsanayn kalsooni.

Satoshi wakhtigiisii ma aysan jirin hannaan lacag-bixineed oo Online ah oo madax-bannaan, oo buuxinaya dhammaan shuruudihii looga baahnaa hannaan sidiisa oo kale ah, hasa yeeshee waxaa jiray isku-dayo dhowr ah oo Bitcoin ka horreeyay, oo dhammaadkii guuldarraystay, sababo la xidhiidha in laga waayay shuruudihii qaar.

Sidaa darteed, Bitcoin ma ahan isku daygii ugu horreeyay, ee lagu doonayay in lagu abuuro hannaan lacag-bixineed oo madax-bannaan, hasa yeeshee waa isku daygii ugu horreeyay ee guulaystay, ee buuxiyay dhammaan shuruudihii.

> *What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.*
>
> *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.*

Haatan Satoshi xalkii buu sii guda-galayaa, wuxuuna yidhi waxa kaliya ee loo baahan yahay waa hannaan lacag-bixineed oo danabaysan oo ku salaysan wax la yidhaahdo "Cryptographic Proof", halkii ay ku salaysnaan lahayd kalsooni.

Cryptographic Proof: Waa hab xisaabeed oo loo adeegsado in lagu ogaado runimada xogta, iyadoo aan lagu khasbanayn in la ogaado xog-hoosaadyada kale, ee aan xidhiidhka la lahayn, sida qofka lacagta diray magaciisa, ama qofka loo diray magaciisa, ama cinwaanka gurigiisa, iwm.

Habkan ku salaysan "Cryptographic Proof", wuxuu qof kasta oo doonaya in uu si toos ah qof kale wax waydaarsado, siinayaa awoodii ay isku waydaarsan lahaayeen, si la mid ah in si fool-ka-fool wax la isku waydaarsaday oo kale, iyadoon loo marin qolo saddexaad. Kaliya iibsadaha iyo iibiyaha.

> *Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.*
>
> *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.*

Halkan Satoshi wuxuu rabaa in uu hal dhagax laba shinbirood mar qudha ku wada dilo, isagoo raba in uu ilaaliyo xuquuqda iibiyaha, isla mar ahaantaana ilaaliyo xuquuqda iibsadaha.

Hadii la helo hannaan lacag-bixineed oo aan laga noqon karin, waxaa sidaasi lagu ilaaliyay xuquuqda iibiyaha, maxaa yeelay lacagtaasi la-lama noqon karo. Dhanka kale, si loo ilaaliyo xuquuqda iibsadaha waa in la adeegsadaa wax la yidhaahdo "Escrow".

Escrow: Waa sidii koonto ama akoon si ku-meel-gaar ah lacagta loogu haynayo, ilaa labada dhinac ay soo buuxiyaan shuruudihii ay ku hishiiyeen, waana tan Decentralized-ka ah, ee Smart Contract ahaan ama Code ahaan loo qorayo, kaasoo ah hishiis si iskii ah u fulaya markii la buuxiyo shuruudihii lagu hishiiyay, waana sidii bangiyada ama qoloda dhexe oo kale, se aan ahayn.

Waa Code la qorayo oo madax-bannaan, oo lacagta si ku-meel-gaar ah u haynaya ilaa shuruudihii la buuxiyo, hadii shuruudaha la buuxiyo waxaa lacagta loo wareejinayaa iibiyaha, hadii kalena dib ayaa loogu soo celinayaa iibsadihii, ileen waxbaba muusan iibsan.

Halkan Satoshi, wuxuu mudnaanta koowaad siinayaa iibiyaha, maxaa yeelay iibiyuhu si uu xuquuqdiisa u ilaashado uma baahna inuu Code ama Smart Contract (Hishiis Si Iskii Ah U Fula) dhiso, halka uu iibsaduhu isagu u baahan yahay si uu xuquuqdiisa u ilaashado.

Waayo iibiyuhu waa kan inta badan khasaaraha ugu weyni soo gaadho, hadii lacag la celiyo wuxuu luminayaa badeecaddii ama adeegii, gaar ahaan hadii ay yihiin kuwo aan ka noqoshada aqbalin, wuxuu sidoo kalena luminayaa wakhti, sumcad, iyo kharash dheeri ah, hadii ay jirto badeecad la celinayo, iyo isla lacagtii la celiyay lafteeda, halka iibsaduhu uu isagu kaliya khasaari lahaa lacagta.

Hadii la adeegsanayo hannaan lacag-celinta aqbalaya (Reversible), waxaa halis ku jira iibiyaha, hadii se la adeegsanayo hannaan aan lacag-celinta aqbalin (Non-reversible), waxaa halis ku jira iibsadaha.

Hasa yeeshee, xaaladan iibsaduhu wax buu la dheer yahay iibiyaha, taasoo ah in uu iibsaduhu iska hubin karo iibiyaha ka hor inta uusan wax ka iibsan, isagoo dooran kara iibiye sumcad fiican leh, halka uusan iibiyuhu tan awoodin, isagoo ku khasban in uu iibsade kaste aamino.

Sidaa darteed, maadaama uu iibsaduhu iska hubin karo iibiyaha ka hor inta aannuu wax ka iibsan, sidoo kalena uu haysto doorasho ah in uu doorto iibiye sumcad fiican leh, waxaa mudnaanta koowaad la siiyay iibiyaha, waana siday tahay. Sidaas oo ay tahayna iibsaduhu wuxuu haystaa xal, kaasoo ah in uu adeegsado "Escrow".

> *In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.*
>
> *Xaashidan ama cilmi-baadhistan waxaan ku soo jeedinaynaa xal cusub oo aynu ku wajjahayno dhibaatada ah in isla hal lacag laba jeer iyo wixii kabadanba 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.*

Satoshi wuxuu qeybtan hordhaca ah ku soo gabgabaynayaa in uu xal u keenay kharash garaynta laba-laaban iyadoo la adeegsanayo diiwaan qeybsan oo fidsan, oo Decentralized ah, oo haatan loo yaqaan "Blockchain".

Satoshi wuxuu adeegsaday ereyo ah "Peer-to-Peer Distributed Timestamp", oo haatan bedelkeeda loo yaqaan Blockchain (Diiwaan qeybsan oo qof-ka-qof ah).

- Peer-to-Peer = Qof-ka-Qof
- Distributed = Qeybsanaan
- Timestamp = Shaanbad Wakhtiyaysan

Wuxuuna Satoshi yidhi waxaan xaashidan ku soo bandhigayaa xal looga hortagayo kharash garaynta laban-laaban, iyadoo loo marayo Blockchain, si loo helo diiwaan is-daba-taxan oo isku xidhiidhsan, kaasoo dhacdooyinka ama lacag-dirisyada u diiwaan galinaya sida ay u kala horreeyaan, si loo ogaado lacag-diris waliba wakhtigii dhabta ahaa ee ay dhacday, si aan loo awoodin in isla lacagtaas mar labaad la adeegsado, oo sidaas looga hortago kharash garaynta laban-laaban.

Isagoo sii watta hadalkiisa, wuxuu yidhi amniga hannaankan wuxuu ku tiirsan yahay ciddii haysa awoodda shabakada inteeda badan, hadii ay badankood daacad yihiin shabakadda amnigeedu wuu sugan yahay, hadii kale se wuxuu u nugul yahay khataro culus oo waa-weyn.

TS, hadii dadka badankood isku raacaan wax khaldan wuxuu noqon doonaa wax dhaqan-gala, oo ay shabakadu qaadato, maxaa yeelay shabakadu ma kala garanayso waxa khaldan iyo waxa qumman, kaliya waxay qaadanaysaa waxa ay dadka badankood go'aamiyaan. Waayo hannaankan ma ahan hannaan dhexe, oo saldhig leh ama xarun dhexe leh oo laga maamulo, ee waa hannaan qeyb-qeybsan oo fidsan oo madax-bannaan, kaasoo loo wada siman yahay.

Sababtaas awgeed, Satoshi wuxuu yidhi shabakadu waa amni, jeer ay dadka wanaagsani ama Nodes-yada daacadda ahi gacanta ku hayyaan oo ay xakamaynayaan.

2. Transactions (Lacag-dirisyada)

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

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.

Qeybtan 2-aad Satoshi wuxuu kaga hadlayaa sida loo wareejiyo Bitcoin, isagoo markan Bitcoin ugu yeedhaya "Electronic Coin" oo macnaheedu yahay shilinkii danabaysnaa. Satoshi wuxuu aragtida Bitcoin ku soo koobay hal weedh, isagoo leh, Bitcoin waa silsilad saxiixyo ah oo is-daba-taxan, oo isku xidhiidhsan.

TS, marka aad maanta rabto inaad qof u dirto Bitcoin waa saxiixaysaa, qofka aad u dirtayna markii uu rabo inuu qof kale u diro wuu saxiixayaa, kaasina markii uu rabo inuu mid kale u diro wuu saxiixayaa. Sidaa darteed, Bitcoin waa silsilad saxiixyo ah oo is-daba-taxan, oo xidhiidhsan.

Lacag-dirista la sheegaba waa wareejinta milkiyadda, iyadoo la adeegsanayo saxiixa qofka. Hadii uu qof rabo inuu qof kale Bitcoin u diro, wuxuu kaliya wareejinayaa milkiyadda, isagoo ka wareejinaya milkiyadiisa, una wareejinaya milkiyadda qofka kale.

Miyay adag tahay?... Aynu fudaydino...

Aynu ka soo qaadno in qof uu rabo inuu qof kale u diro Bitcoin, ugu horrayn inta aanuu wax dirin, waa inuu cadeeyaa in uu yahay milkiilaha dhabta ah, isagoo saxiixaya Hash-ka lacag-diristii hore, maxaa yeelay, si uu lacag u diro waa in ay marka hore hadhaagiisa ugu jirtaa, si ay hadhaagiisa ugu jirtana waa in loo soo diraa, ama uu dhaliyaa.

Bitcoin 2 qaab oo kaliya ayaa lagu helaa, in milkiyaddaada lagu soo wareejiyo, iyo in aad dhaliso, adigoo noqonaya Miner ama qode, oo ku biiraya shabakadda, isla mar ahaantaana shaqaynaya, waxaadna abaalmarin ahaan u helaysaa tiro cusub oo Bitcoin ah, waana wixii la odhan jiray "Block Reward" oo micnaheedu yahay Abaalgudka Block-ga.

Sidaa darteed, si aad Bitcoin qof kale ugu dirto, waa inaad ugu horrayn caddaysaa halka aad ka keentay lacagtan aad rabto inaad dirto, adigoo saxiixaya Hash-ka ay ka timid, oo sumad u ah, iyooooooooo furaha guud (Public Key) qofka aad u wareejinayso.

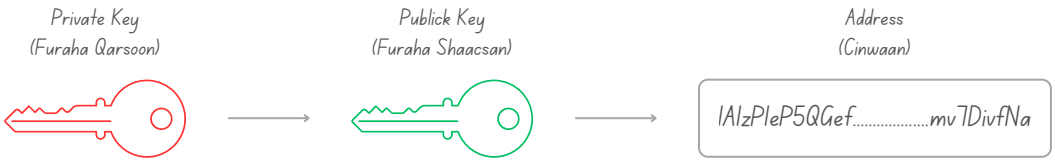
Tani waxay muujinaysaa in ay markii hore lacagtan si sharci ah kuugu soo wareegtay, isla mar ahaantaana aad hadda rabto inaad si sharci ah u wareejiso, adigoo isla saxiixaya Hash-ka lacag wareejintii hore, iyo furaha guud (Public Key) qofka aad u wareejinayso, adigoo adeegsanaya furahaaga gaarka ah (Private Key), kadibna abuuraya lacag-diristii, kadibna u gudbinaya shabakadda, sidaasina Blockchain-ka loogu daro.

Waxaa jira wax la yidhaahdo:

- **Private Key:** Waa fure gaar ah, oo ay tahay inuu qarsoonaado, oo loo adeegsado in lagu saxiixo (Sign) lacag wareejinta, si loo caddeeyo in milkiilahan uu yahay milkiilihii dhabta ahaa, ee lahaa lacagta, mar hadii furahan la helana waxaa awood loo leeyahay in lacagta gabi ahaanteed la-la wareego, sidaa darteed baa loo yidhi fure gaar ah, oo qarsoon, oo aysan ahayn in dadka lala wadaago, waana sidii Password-ka oo kale.
- **Public Key:** Waa fure guud oo shaacsan, oo loo adeegsado in lacagta lagu helo, ama lagu soo diro, qofka raba inuu lacag kuu soo diro, wuxuu ugu horrayn u baahan yahay inuu helo furahaaga shaacsan, si uu kuugu soo diro, hasa ahaatee, bedelkii la adeegsan lahaa furaha shaacsan, waxaa la adeegsadaa "Address" oo ah cinwaan kooban oo si fudud loo fahmi karo, oo u taagan furaha shaacsan, maxaa yeelay furaha shaacsan ama Public Key-ga aad buu u dheer yahay, lamana xifdin karo.

Si kooban:

- **Private Key:** waa fure qarsoon, waxaana laga sii dhex sameeyaa Public Key
- **Public Key:** waa fure shaacsan, waxaana laga sii dhex sameeyaa Address
- **Address:** waa cinwaan kooban oo u taagan furaha guud

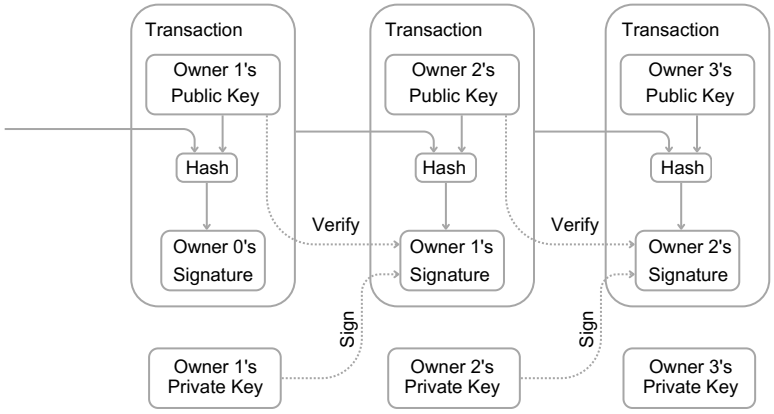


Aynu magacyo adeegsano, si uu fahamku u soo dhawaado, CAWIL ayaa raba inuu CIGAAL 1 Bitcoin u diro, ugu horrayn waa inuu CAWIL caddeeyaa in 1-ka Bitcoin ee uu rabo inuu diro, mar keedii hore halkuu ka keenay, isagoo keenaya Hash oo ah summad sheegaysa in uu 1 Bitcoin ka helay CAYNAASHE, ama 2 Bitcoin, ama 3, ama wuxuu ahaadaba, haddana raba inuu 1 Bitcoin diro CIGAAL, inta kalena uu reebto, isagoo isla saxiixaya summadii ama Hash-kii CAYNAASHE iyo Public Key-ga CIGAAL, isagoo adeegsanaya furihiisa gaarka ah ama Private Key-giisia, kadibna abuuraya lacag-diristii, kuna baahinaya shabakadda, sidaasina Blockchain-ka loogu daro, sidaasina 1 Bitcoin oo markii hore ka mid ahayd milkiyadda CAWIL hadda u wareegtay milkiyadda CIGAAL.

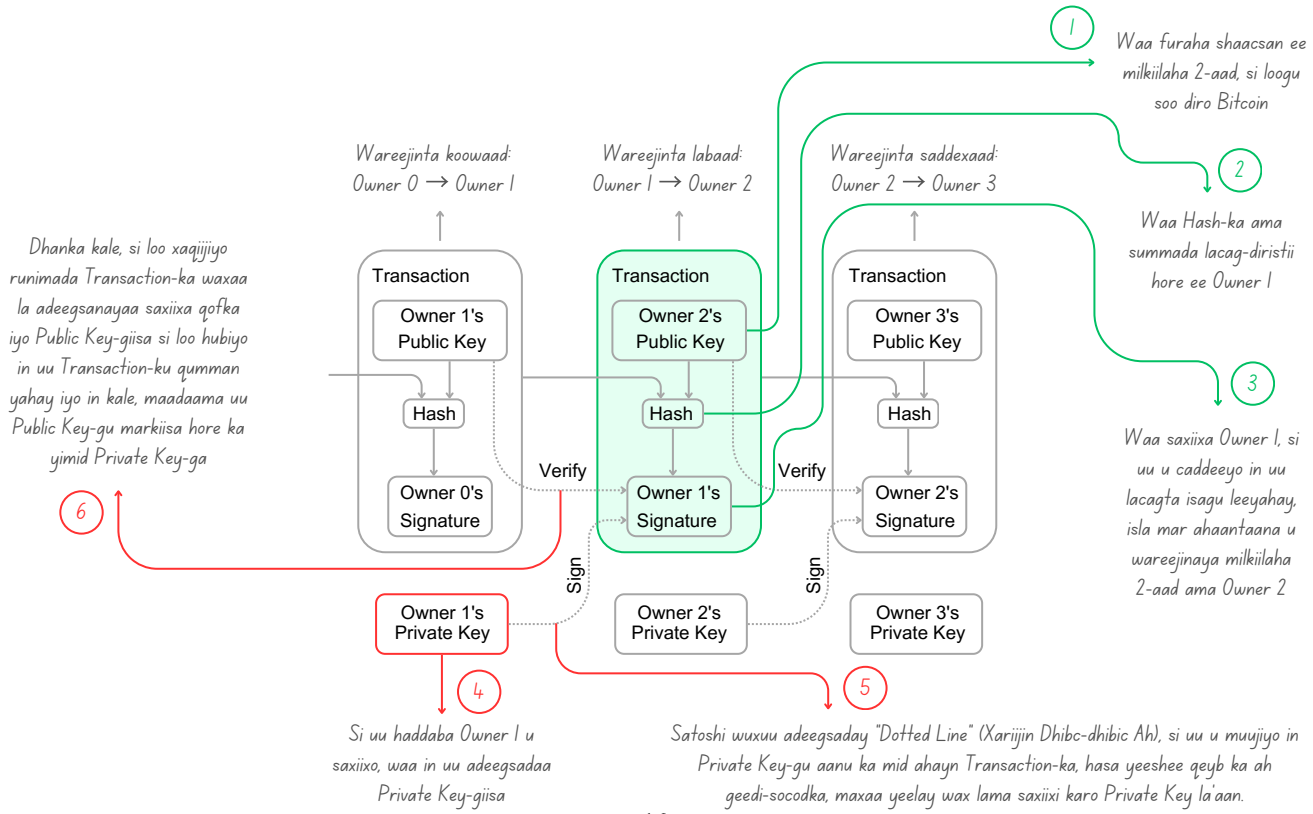
Lacag-dirista la sheegayaba waa wareejinta milkiyad, qof baa milkiyadiisa u wareejinaya qof kale, qofkaasina qof kale, qofkaas kalena qof kale, kaaasina ku kale, kaa kalena ku kale, kaaaaaaa…..

Habkani wuxuu meesha ka saarayaa baahidii loo qabay qolo saddexaad, oo xaqiijisa runimada lacag-dirisyada, maxaa yeelay si otomaatig ah bay lacag-diris kasta ugu xidhiidhsan tahay lacag-diristii ka horraysay, iyadoo mid waliba ay wadato Hash ama summad sheegaysa halka ay ka timid.

Dhanka kale, Payee-ga ama loo-diraha, ama qofka lacagta helaya si fudud buu u xaqiijin karaa in lacagta uu helay, ay tahay lacag jirta oo dhab ah, oo si buuxda uga soo guurtay milkiyadda qofkii hore, isagoo hubinaya Blockchain-ka, halkaas oo uu ka arki doono sida ay lacagtiisu qofba qofka kale uga soo gudbaysay, ilaa ay ugu danbayntii isaga soo gaadhay. Sida halkan kaaga muuqataba:



Aynu kala dhig-dhigno, inagoo diiradda saarayna TX 2-aad:



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent.

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 ah, 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.

Halkan Satoshi wuxuu leeyahay xitaa hadii la helo Blockchain ama silsilad saxiixyo ah oo is-daba-taxan, oo isku xidhiidhsan, wali waxaa jirta dhib kale, oo ah in aan la caddayn karin in aysan milkiilayaashii hore lacagtan laba kharash garayn, oo aysan samayn Double Spend.

Waa run, lacagtii si buuxda ayay uga soo guurtay milkiyadiisa, oo ay u guurtay milkiyadda qofka kale, hasa yeeshee sideen ku ogaan karnaa in aan la-laba kharashgarayn, oo aan hore meelo kale loogu adeegsan. Sidaa darteed, buu Satoshi u lahaa saxiixyada ama Digital Signatures-ku waa qeyb ka mid ah xalka, ee ma wada ahan xalka oo buuxa.

TS, qof baa 1 Bitcoin u diray qof kale, qofkii loo diray ama Payee-ga si uu u xaqiijiyo in si dhab ah loogu soo diray 1 Bitcoin wuxuu booqanayaa Blockchian-ka, halkaas oo uu ka arki doono in si sharci ah milkiyaddiisa loogu soo wareejiyay, hase ahaatee sidee buu ku ogaan karaa ee uu ku xaqiijin karaa in 1-kan Bitcoin aan la-laba kharashgarayn, oo aan la samayn Double Spending, waana halkan halka uu Satoshi ka hadlayo, sidee logu ogaan karaa oo looga hortagi karaa Double Spending-ka?

Xalka ugu soo dhaw waa in dib loogu noqdo hannaan ku tiirsan kalsoonida, iyadoo loo baahan yahay in la helo dhinac dhexe ama la helo wax la yidhaahdo "Mint", oo kalsooni leh, kuwaas oo ay shaqadoodu tahay in ay kormeeraan is-dhaafsiyada dhacaya, isla mar ahaantaana xaqiijjiyaan lacag-diris kasta oo dhacda.

Mint: Waa erey markiisa hore ka yimid daabacaadda lacagta, waana warshadda ama xarunta lacagta daabacda, diiwaangalisa, kaydisa, ahna sidii hay'ad dhexe oo ka hortagta kharash garaynta laba-laaban, iyo been-abuurka lacagaha.

Hasa yeeshee haatan waxaa laga hadlayaa lacagaha danabaysan (Digital Money), wuxuuna Satoshi ereyga "Mint" u adeegsanayaa si uu fahamka u soo dhaweeyo, isagoo ula jeeda qolo dhexe oo shaqadoodu tahay kormeeridda dhaqdhaqaaqyada.

Haddaba si looga hortago kharashgaraynta laba-laaban waa in lacag-diris kasta dib loogu celiyaa Mint-gii ama warshadii ama qoladii dhexe ee soo saartay, halkaas oo uu Mint-gu hubinayo in aan hore loo adeegsan, kadibna uu burburinayo ama baabi'inayo lacagtii, bedelkeedana uu abuurayo nuqul cusub, oo aan hore loo adeegsan, halkaas oo uu uga sii gudbayo loo-dirihii ama qofkii loo dirayay.

TS, RAAGE ayaa raba in uu 1 shilin u diro ROOBLE, lacag-diristaas inta aan loo wareejin ROOBLE, waxaa dib loogu celinayaa Mint-gii soo saaray, halkaas oo uu Mint-gu hubinayo in lacagtan aan hore loo adeegsan oo aan la-laba kharashgarayn, hadii la-laba kharashgareeyay lacag-diristaas waa la diidayaa, oo lama gudbinayo, hadii se aan la-laba kharashgarayn waa la baabi'inayaa lacagtii, si nuqul cusub loogu sameeyo, kadibna loo gudbiyo ROOBLE, sidaasina ROOBLE waxaa loo soo diray lacag cusub, oo aan hore loo adeegsan.

Lacagaha kaliya ee la rumaysan yahay in aan la-laba kharashgarayn, waa lacagaha kaliya ee uu Mint-gu ansixiyo, ee uu soo saaro, sidaasina waxaa looga hortagay kharashgaraynta laba-laaban ama Double Spending.

Fiiro Gaar Ah: Haatan xalal kale oo aan "Mint" ahayn ayaa la adeegsadaa, hasa yeeshee xaashidan oo la qoray 2008-dii awgeed, xalka ugu dhaw ee wakhti xaadirkaas jiray wuxuu ahaa Mint-ga.

> *The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.*
>
> *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.*

Halkan Satoshi wuxuu leeyahay, xalkan wuxuu keensanayaa dhib ka weyn dhibka uu xallinayo, waayo wuxuu si buuxda ugu tiirsan yahay Mint-ga, hadii uu Mint-gu khalad yar ka dhaco, ama la weeraro, ama loo dhaco, ama la xidho, ama la musuq-maasuqo, ama…, hannaan-lacageedkaas gabi ahaantii sida uu u dhan yahay wuu burburayaa.

Intaas waxaa dheer, in uu Mint-gu awood u leeyahay in uu lacagaha qaar xannibo, ama xayyiro, amaba diido in uu diro sabab la'aan, si la mid ah bangiyada.

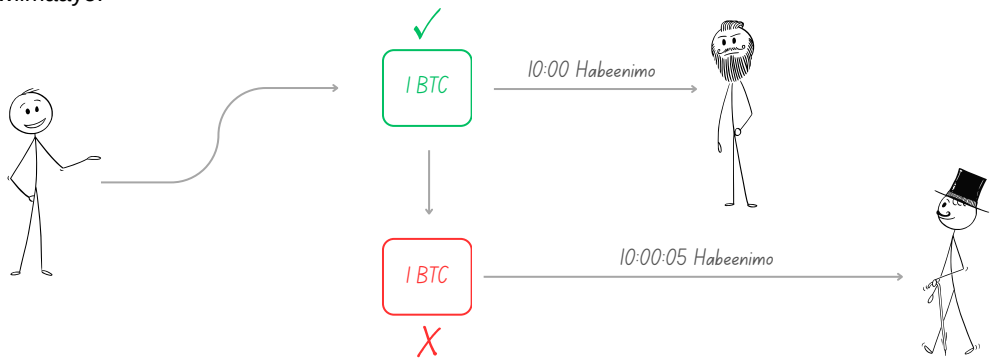
Satoshi wuxuu leeyahay, hadii aynu keeno hannaan-lacageed ku tiirsan Mint-ga, si looga hortago kharashgaraynta laba-laaban, markaas iyada ah wax cusub ma soo kordhin, waxaana sidii loo socdaba ugu danbayntii dib loogu soo noqonayaa hannaan-lacageed ku tiirsan kalsooni. Waana waxa uu ka cararayo Satoshi.

> *We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.*
>
> *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 isticmaalin 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 kharashgarayn, waa in aqoon buuxda loo leeyahay, lagana warqabo dhammaan lacag-dirisyda (All Transactions).*

Satoshi wuxuu leeyahay waa in xal wax-ku-ool ah loo helaa kharashgaraynta laba-laaban, waana in la helaa hab uu loo-diruhu (Payee) ku ogaan karo, kuna hubin karo in lacagta uu helay aysan ahayn lacag hore loo-laba kharashgareeyay.

Haddaba xalka ay Bitcoin uga hortagayso kharashgaraynta laba-laaban ama Double Spending-ka waa xeerka cad ee uu Satoshi u dajjiyay, kaasoo ah in kaliya la tixgaliyo lacag-dirista ugu horraysa.

TS, hadii uu qof rabo inuu qof kale u diro 1 Bitcoin abbaaro 10:00 habeenimo, isla mar ahaantaana uu rabo in isla 1-kii Bitcoin u diro qof kale oo aan ahayn qofkii hore, shan ilbiriqsi kadib abbaaro 10:00:05 habeenimo, si uu u sameeyo kharashgarayn laba-laaban, labada lacag-diris ayaa loo wada gudbinayaa shabakadda Bitcoin, lacag-dirista ugu horraysa ee ay shabakaddu aqbasho ayaa noqonaysa lacag-dirista dhabta ah, tan kale ee labaadna waa la iska idha-tirayaa, lana isku hawlimaayo.



Sidaa darteed, buu Satoshi u yidhi: shabakaddu iskuma hawlayso lacag-dirisyada danbe, markii mid la aqbalo, la iskuma mashquulinayo isku dayada danbe ee ka soo daba-baxaya, waayo hore ayay shabakaddu u go'aamisay cidda leh lacagta.

Haddaba si markii ay shabakaddu mid u go'aamiso, aan kuwa kale la iskugu hawlin, waa in la helaa diiwaan furan, oo ay Nodes-yadu arki karaa dhammaan wixii la xaqiijiyay iyo wixii kaleba, si aysan isku maan-dhaafin, waana halkaa halka ay ka timid in la helo diiwaan furan (Public Blockchain).

Hadii diiwaanka laga dhigo mid furan oo Public ah, si fudud bay Nodes-yadu u arki karaan dhammaan wixii la xaqiijiyay, iyo wixii aan la xaqiijin, maxaa yeelay Node waliba wuxuu haystaa nuqul isaga u gaar ah, oo ka mid ah diiwaanka guud, sidaa darteed, halkaas is-maan-dhaaf kama dhacayo.

> *In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received.*
>
> *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.*

Satoshi wuxuu tusaale ahaan u soo qaatay hannaankii Mint-ga ku tiirsanaa (Mint-based Model), isagoo yidhi Mint-gu si uu uga hortago kharashgaraynta laban-laaban wuxuu haystaa diiwaan ay ku diiwaan gashan yihiin dhammaan lacag-dirisyadii dhacay, isagoo si fudud u go'aamin kara tii ugu horraysay ee la xaqiijiyay.

Sidaas si la mid ah, hadii aynu rabno inaynu ka hortagno kharashgaraynta laban-laaban, inagoon adeegsanaynin dhinac dhexe, sida Mint-ga, waa inaynu diiwaanka aynu ku diiwaan galinayno lacag-dirisyada ka dhignaa diiwaan furan oo shaacsan oo baahsan oo Public ah.

Tani waxay abuuraysaa baahi loo qabo hannaan is-afgarad, si aan la isku maan-dhaafin, oo aan loo helin diiwaan kala jaad ah, oo iska hor-imanaya.

TS, hadii uu **Node-ka B** arko Transaction-ka **X** ka hor **Y**, halka **Node-ka T** uu hor arko **Y** ka hor **X**, waxaa halkaa ka dhalanaysa is-maan-dhaaf weyn, oo keeni karta in labada Node ay kala aragti duwanaadaan, sidoo kalena kala go'aan noqdaan, tani waxay shabakadda ka dhigaysaa mid aan lagu wada hishiin karin, oo aan xaalad gaar ah ku hishiin karin, oo is-baraan-burin badan leh.

Sidaa darteed, si aysan tan u dhicin, Satoshi wuxuu yidhi waa in la helaa hannaan is-afgarad oo la isku raacsan yahay, oo midaynaya shabakadda, si loo helo diiwaan midaysan, oo quman. Waana halkaa halka ay ka timid "Consensus Mechanism".

> *The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.*
>
> *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.*

Dhanka kale Satoshi wuxuu leeyahay, loo-diraha ama qofka lacagta helaya waa in uu kalsooni ku qabaa in lacagta uu helay tahay lacag dhab ahaantii run ah, oo aan been-abuur ahayn, oo aan hore loo-laba kharashgarayn, maxaa yeelay waxaa si wada-jir ah u xaqiijiyay Nodes-yada shabakadda badankood, waxayna ahayd lacag-diristii ugu horraysay ee nooceeda ah.

> ***3. Timestamp Server (Blockchian)***
>
> *The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.*
>
> *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.*

Qeybtan 3-aad wuxuu Satoshi uga hadlayaa "Timestamp Server", oo maanta loo yaqaan Blockchain, isagoo yidhi, bar bilawga xalkeenu wuxuu ka bilaabmayaa Blockchain.

Wuxuuna Satoshi sharaxayaa sida ay Blockchain u shaqayso, isagoo leh: Blockchain waa diiwaan taariikhaysan, kaasoo xogta xidhmo-xidhmo u diiwaan galiya, xidhmadaasoo loo yaqaan "Block". Xidhmo kasta ama Block kasta waxay leedahay Hash, kaasoo ah summad iyada u gaar ah, si loogu aqoonsado, intaa kadibna si furan oo shaacsan loo baahinayo.

Sidoo kale wuxuu Satoshi sheegay in Timestamp, oo ah wakhtiga dhabta ah ee ay dhacdo dhacday, ay caddayn u tahay in goortii wax la Hash-garaynayay ay wakhti xaadirkaas jireen, isagoo hadalkiisa sii raaciyay, sida cadna wax lama Hash-garayn karo xog la'aan.

Waayo si aad Hash u hesho ama aad wax u Hash-garayso waa in ay marka hore jirtaa wax ama xog aad rabto inaad Hash-garayso, taasoo caddayn u ah in waxa la Hash-garaynayay ay wakhti xaadirkaas jireen.

Halkan wali waxaa jirta dhib kale, sidee lagu caddayn karaa goortii uu dhacay Hash-ku ama Timestamp-ka Hash-ka, maxaa yeelay Hash kaligii micno ma samaynayo, hadii aan la caddayn karin goortii la sameeyay.

Waa run, Hash la ma heleen, hadii aannuu jirin wax la Hash-garaynayo, taasoo cadayn u ah in goortii wax la Hash-garaynayay ay jirtay xogtu, hasa ahaatee yaa caddayn kara goortii ama wakhtigii wax la Hash-gareeyay?.

Hadii aad tidhaahdo Hash-kan waa caddaynta xogtan, oo aanad caddayn karin goortii la Hash-gareeyay, waxay caddayntaadu noqonaysaa mid kala dhantaalan, oo kala dhiman, mana noqonayso caddayn buuxda, oo ay shabakaddu ku qanci karto.

Si haddaba loo helo caddayn buuxda waa in si shaacsan loo baahiyaa goorta ama wakhtiga ama Timestamp-ka dhabta ah ee wax la Hash-gareeyay, si ay isku kaabaan, oo ay isku dhamaystiraan, sidaasna waxaa lagu heli karaa iyadoo diiwaanka xogta lagu diiwaan galinayo laga dhigo mid furan oo baahsan oo Public ah.

Sidaa darteed, ayuu Satoshi tusaale ahaan u soo qaatay wargaysyada iyo Usenet Post, oo ahaa adeeg fariimo, oo la sameeyay horraantii 1980-meeyadii, ka hor emails-yada, forums-yada, iyo social media-ha hadda jira.

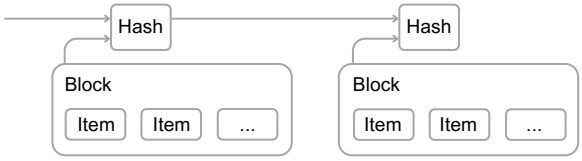
Wargaysyada uu Satoshi ka hadlayana waa kuwii jidhitaanka jidheed lahaa, ee la akhrisan jiray, ee subax waliba soo dhici jiray, kuwaasoo ay adkayd in markii wargays la daabaco oo la qaybiyo oo la faafiyo kadib, dib hadana wax looga bedelo ama la tirtiro gabi ahaanteed, wargaysyadaas oo lahaa wakhti ama Timestamp.

Dhanka kale, Usenet Post oo ahayd adeeg fariimo, oo waagii hore la isticmaali jiray, way adkayd in iyadana dib xogta looga bedelo, kadib markii la daabaco ama la baahiyo. Haddaba hadii wargaysyada ama Usenet Post lagu daabaco Hash, wuxuu Hash-kaas noqonayay mid wakhtiyaysan oo Timestamp leh, oo aan si fudud wax looga bedeli karin, taasoo caddayn buuxda ah.

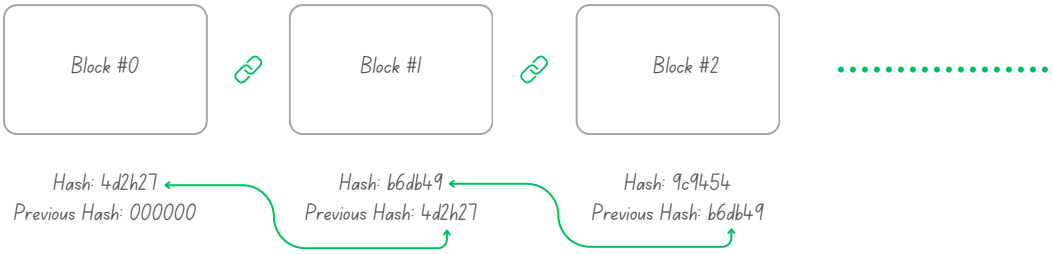
Wuxuuna Satoshi tusaaleyaashan u adeegsaday si uu fahamka dadka u soo dhaweeyo, maadaama ay labaduba ka siman yihiin wakhtiyaynta ama Timestamping-ka, iyadoo uu joornaalku ama warkaysgu soo bixi jiray isla maalinta la daabaco, isla mar ahaantaana la faafin jiray, sidaas oo kalena Usenet Post. Waana sababtaas sababta uu Satoshi u lahaa waa in la helo diiwaan shaacsan oo furan.

Wuxuuna sii raaciyay, Block kasta wuxuu la xidhiidhaa Hash-ka Block-gii ka horreeyay, halkaas oo uu ku samaysmi doono silsilad Block-yo ah, Block kasta wuxuu sii xoojinayaa runimadda Block-gii ka horreeyay, maadaama ay isku xidhiidhsan yihiin, waana halkaa halka ay ka timid "Blockchain".

Block kasta waxaa ku jira xidhmo xog ah, sida dhowr lacag-dirsyo ah, wuxuuna leeyahay Hash ama summad isaga u gaar ah, oo lagu aqoonsado, isla mar ahaantaana wuxuu la xidhiidhsan yahay Hash-ka ama summadda Block-gii ka horreeyay, sidaasina waxaa ku samaysmaya silsilad Block-yo ah oo midba midkii ka horreeyay ku xidhiidhsan yahay, sida halkan kaaga muuqata:



Aynu si kale u dhigno:



4. Proof of Work (Hab-sugid Shaqo)

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

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.

Qeybtan 4-aad, wuxuu Satoshi uga hadlayaa sidii loo hirgalin lahaa Blockchain ama hannaankii uu aragtida ahaan u soo sharaxay, waana qeybta ugu muhiimsan xaashidan, ama cilmi-baadhistan, waana in fiiro gaar ah loo yeeshaa.

Satoshi wuxuu hadalkiisa ku bilaabay, si loo hirgaliyo "Distributed Timestamp Server", oo aynu bedelkeeda odhanayno "Decentralized Blockchain", ku dhisan mabda'a qof-ka-qof waxaynu u baahanahay inaynu adeegsano wax la yidhaahdo "Proof-of-Work", oo aynu hore u soo nidhi waa hab-sugid shaqo, kaasoo la mid ah "Adam Back's Hashcash".

Hashcash: Wuxuu ahaa hab looga hortagayo Email-lada Spam-ka ah, ee aan la jeclaysan, ee inta badan ah xayaysiimo iyo Scam, ee sida tirada badan loo diro, waxaana hindisay Adam Back.

Qofka raba inuu Email diro waa inuu shaqo adag qabto, oo u baahan xalinta xisaabaad adag, ka hor inta uusan dirin, waana inuu helo Hash ka bilaabmaya tiro gaar ah oo ebero ah, tusaale ahaan Hash ka bilaabmaya 4 eber, sida 0000…, si uu u diro Email-ka.

Taasoo ka hortagaysa Email-lada Spam-ka ah ee tirada badan, isagoo oo uu qofku dirayay Email-ka iyo caddaynta shaqada uu qabtay. Ka qof ahaan way iska fududayd in la qabto shaqadaas, hasa yeeshee aad bay ugu adkayd kuwa raba inay Email-lo tiro badan diraan.

Sababta uu Satoshi "Hashcash" tusaalahaan ugu soo qaatay, waa inay ay ahayd tusaalaha ugu dhaw ee wakhtigaas jiray, waana markii ugu horraysay ee uu Satoshi mashruuc gaar ah magac-dhabo oo uu tusaale ahaan u soo qaato.

Haddaba Satoshi wuxuu yidhi, si aynu u helno hannaan si iskii ah u shaqaynaya oo peer-to-peer ah (P2P), waxaynu u baahanahay in soo-saarista Hash kasta loo maro shaqo adag (Proof of Work), bedelkii la adeegsan lahaa wargaysyada iyo Usenet Post.

Waayo wargaysyada iyo Usenet Post waa Centralized, oo aad u gaabis badan, oo aan madax-bannaanayn, Satoshi-na wuxuu rabaa hannaan madax-bannaan oo Decentralized ah, sidaa darteed buu u yidhi, bedelkii wargaysyada ama Usenet Post.

Proof of Work oo loo soo gaabiyo PoW waa hab-sugid shaqo, ama qaab-caddayn shaqo, in wax la caddeeyo oo la sugo iyadoo la qabanayo shaqo culus, oo lagu bixiyay tamar iyo wakhtiba, waana in la raadiyo oo la helo Hash ka bilaabmaya tiro ebero ah, si la mid ah Hashcash-kii Adam Back dhisay oo kale.

Sida aynu soo sheegnay Hash-ku waa sumad lagu aqoonsanayo xogta, oo leh qiimo iyo dherer go'an, kaasoo hadii wax yar laga bedelo xogtii, uu Hash-ku gabi ahaantii is-bedelayo. Waana natiijo ka dhalata markii xog la marsiiyo hab gaar ah, oo loo yaqaan "Hash Function", kaasoo ah habka ama nooca ama mishiinka bedelaya xogta.

Sida ay mishiinada cuntada ama sharaabka ridqa ama shiida ay u kala duwan yihiin, oo midba natiijo gaar ah uu ku siinayo, ayay sidoo kale hababka loo bedelo xogta ama qaababka la adeegsanayo in lagu bedelo xogta ay u kala duwan yihiin, hasa yeeshee xeer ahaan way siman yihiin, waana tan xeerka ay maraan:

- Data → Hash Function → Hash
- Xogta → Habka ama nooca la adeegsanayo si loo bedelo xogta → Natiijada Hash-ka

Bitcoin waxay adeegsataa hab ama Hash Function loo yaqaan SHA-256, oo laga soo gaabiyay "Secure Hash Algorithm", oo ah hab ama nooc ka mid ah noocyada Hashing-ka ama Hash Function-ka, kaasoo ilaa wakhti xaadirkan ah mid aad u amaan badan (1447H).

Sidaa darteed, iyadoo la adeegsanayo **SHA-256** oo ah jaad ka mid ah jaadyada Hashing-ka, waa in la baadi-goobaa oo la raadiyaa Hash ka bilaabmanaya tiro ebero ah.

Haddaba Satoshi wuxuu yidhi celceliska shaqo ee loo baahan yahay in la qabto si loo helo Hash ka bilaabmaya tiro ebero ah waxay ku jibbaaran tahay tirada eberada ee wakhti xaadirkaas shabakaddu rabto, taasoo marna kordhaysa, marna hoos u dhacaysa, hasa yeeshee inta badan kordhaysa uun.

Halkan wuxuu Satoshi ku leeyahay shaqada ama dadaalka looga baahan yahay inuu qabto kubmiyuutarkaagu ama qalabkaagu si uu u helo Hash ka bilaabmaya tiro ebero ah, waxay ku jibbaaran tahay inta eberaad ee ay shabakaddu markaas rabto.

Taas micnaheedu waa hadii ay shabakaddu rabto Hash ka bilaabmaya 1 eber isku-dayga la rabo waa 2, hadii 3 eberaad la rabo isku-daygu waa 8, hadii 5 eberaad la rabo isku-daygu waa 32 eber, hadii la rabo Hash ka bilaabmaya 20 eberaad, isku-dayga la rabo waa 1 milyan wax ka badan si loo helo Hash ka bilaabmaya 20 eber, sida halkan kaaga muuqata:

- 1 eber = celcelis 2 isku-day
- 2 eber = celcelis 4 isku-day
- 3 eber = celcelis 8 isku-day
- 4 eber = celcelis 16 isku-day
- 5 eber = celcelis 32 isku-day
- …
- …
- …
- 20 eber = celcelis 1,048,576 (in ka badan 1 milyan oo isku-day)
- 30 eber = celcelis 1,073,741,824 (in ka badan 1 bilyan oo isku-day)
- 40 eber = celcelis 1,099,511,627,776 (in ka badan 1 tirilyan oo isku-day)
- 50 eber = celcelis 1,125,899,906,842,624 (in ka badan 1 kuwantirilyan oo isku-day)

Bal u fiirso, si aad u hesho Hash ka bilaabmaya 50 eber waa inaad celcelis curiso ama Generate-garayso wax ka badan 1 kuwantirilyan oo Hash, hadda waa si aad kaliya u hesho Hash ka bilaabmaya 50 eber. Waana sababta uu Satoshi u lahaa: "*Exponential in the Number of Zero bits*".

Waana celcelis, ee ma ahan wax go'an oo aad ku khasban tahay inaad samayso, waayo waxaa suuragal ah inaad isku dayga koowaad ama labaad aad hesho Hash ka bilaambaya 50 eber, adigoonan ku khasbanayn inaad malaayiin iyo balaayiin jeer oo danbe isku daydo, hasa yeeshee waa wax aan ku dhawaad dhici karin, hadii uu nasiibku ku taageero mooyee.

Sababta celcelis loo yidhina waa in la ogaado heerka ama fursadda ama kanshada lagu heli karo Hash ka bilaabmaya tiro ebero ah.

- Hadii la rabo Hash 1 eber ka bilaabmaya, kanshada aad ku heli karto waa ½ ama 50%
- Hadii ay tahayna 2 eber, kanshadaadu waa ¼ ama 25%
- Hadii ay tahayna 3 eber, kanshadaadu waa ⅛ ama 12.5%
- Hadii kale se ay tahay 50 eberaad, kanshadaadu **1/(2^50)** ama qiyaastii **0.000000000088%**

Waana sababtaas sababta aysan ku dhawaad suuragal u ahayn in aad isku-dayada ugu horraysa ku hesho Hash ka bilaabmaya 50 eber, fursadda ama kanshada aad ku heli karto waa mid aad iyo aad iyo aad iyo aad iyo aad u adag, waana halkaa halka uu Satoshi lahaa waa in soo-saarista Hash kasta loo maraa shaqo adag. Waana halka ay ka magac baxday "Proof of Work".

Haatan oo ay goortu tahay 1447-kii, muxarram 30-keedii, abbaaro 8:11 habeeno, Block-gii ugu danbeeyay ee ay shabakaddu soo-saarto waa #907,153, Block-gan ayaa Hash-kiisu ka bilaabmayaa 81 eber, haa waa 81 eber, waana kan Hash-kiisa: "00000000000000000000004856b729177bc7d142e8ae42f92af37d7be71039acf4". Gacmahaaga ku soo hubi, adigoo booqanaya Blockchain-ka.

Halkna aynu mid baraarujinno, waxaa jira dhowr qaab oo tirooyinka loo muujiyo, kuwooda ugu caansanina waa:

- **BIN (Binary):** Waa qaab-tirin leh 2 sal
- **HEX (Hexadecimal):** Waa qaab-tirin leh 16 sal
- **DEC (Decimal):** Waa qaab-tirin leh 10 sal
- **OCT (Octal):** Waa qaab-tirin leh 8 sal
- …

Waxaana jira wax la yidhaahdo BIT ama Binary Digit, waa unuga ugu yar ee xog noqon kara, kaasoo ama 1 ka kooban ama 0, waa afka uu fahmo kumbiyuutarku, una rogi karo fal, tusaale, hadii aynu shibanaha "**S**", u soo bandhigno qaab-tirsiga Binary waa 01010011, kaasoo ka kooban 8 BIT ama sideed god.

Sidaa darteed, markii aynu leenahay waa Hash ka bilaabmaya 81 eber ama 50 eber, waxaynu ula jeednaa 81 eber oo bit ah, oo ka mid ah 256 bit.

Maxaa yeelay Hash Fanction-ka aynu adeegsanayno waa SHA-256, kaasoo ka kooban 256 bits.

Badanaa markii la muujinayo Hash SHA-256 waxaa loo muujiyaa qaab HEX ah, waayo hadii la is yidhaahdo si binary ah ha loo muujiyo, waxay noqonaysaa in 256-ka bit ama god ee uu ka kooban yahay in la wada muujiyo, taasoo kadeed u muuqata, sidatanna ayaa loo xisaabiyaa:

- Halkii Hash ee SHA-256 ah ee hadana HEX ah wuxuu ka kooban yahay 64 unug ama god
- Halkii god ama halkii unug ee HEX wuxuu u dhigmaa 4 bits oo binary ah
- Hadii aynu 64 ku dhufano 4 waxaa soo baxaysa 256 bit

Hadii aynu eegno Hash-keenii hore ee "0000000000000000000004856b729177bc7d142e8ae42f92af37d7be71039acf4", oo u dhigan qaab-tirsiga HEX (Hexadecimal), is nidhaahno u roga bits, waxaa noo soo baxaysa Hash ka kooban 256 bit ama god, kaasoo ka bilaabmaya 81 eber, sida halkan hoose ka muuqata:

"0000000000000000000000000000000000000000000000000000000000000000
0001001000010101101011011100101001000101110111101111000111110100010100001011101
0001010111001000010111110010010101011110011011111010111101111100111000100000011
10011010110011110100".

Sababtan awgeed, badanaa markii la joogo Hashing-ka, waxaa la adeegsadaa oo loo soo bandhigaa qaab-tirsiga HEX (Hexadecimal), maxaa yeelay wuxuu soo koobayaa xogtii badnayd, iyadoo halkii unug uu u dhigmo 4 unug oo bits ah, taasoo fududaynaysa akhriska iyo garashada jaadka uu yahay Hash-ku.

Sidaa darteed, hadii aad aragto Hash HEX ah, ha is odhan aaway ama meeye eberadii badnaa ee la sheegayay, maxaa yeelay god kasta oo HEX wuxuu u dhigmaa 4 god oo binary ah.

Dhanka kale, Satoshi isagoo hadalkiisa watta wuxuu yidhi: "*And Can be Verified by Executing a Single Hash*", si fudud ayaa loo xaqiijin karaa runimada Hash-ka, iyadoo kaliya la samaynayo hal hawlgal, ama hal Hash (Single Hash Operation). Sidee?

Sidii aynu hore u soo nidhi, Hash-ku waa sidii summad oo kale, kaasoo u taagan wixii la Hash-gareeyay.

Sidaa darteed, marba hadii aynu hayno xogtii la Hash-gareeyay, iyo Hash-ka laftiisa, si fudud baynu u xaqiijin karnaa, inagoo hal mar oo kaliya dib hadana xogtii u Hash-garaynayna.

Hadii Hash-ka noo soo baxa uu la mid yahay Hash-ka aynu hayno, markaa iyada ah Hash-ku wuu qumman yahay, hadii kale se waa Hash aan qumanayn, oo khaldan, sidaasina hal hawlgal oo kaliya ayaanu ku xaqiijinay runimadda Hash-ka.

TS:

- "CAWO ayaa 2 Bitcoin u dirtay CUDDOON" (Waa xogtii)
- "52262275fdd08faa…….4748b6b80b305d3b7" (Waa Hash-ka xogta, iyadoo la adeegsanayo SHA-256, adiga laftigaaguba soo hubi, oo xogtaas dib u Hash-garee adigoo adeegsanaya SHA-256, waxaa kuu soo baxaya isla natiijadan)

Hadii wax yar laga bedelo xogta, sida in laga dhigo 3 ama 2.5 Bitcoin, halkii ay ka ahayd 2 Bitcoin oo kaliya, ama la bedelo qaab qoraalka, iyadoo aan la bedelayn micnaha guud sida "**CAWO**" oo laga dhigo "**Cawo**" oo kale, ama "**Bitcoin**" oo laga dhigo "**bitcoin**", waxaa gabi ahaanba is bedelaya Hash-kii, xitaa hadii aysan micnaha guud is bedelin, waayo Hash-ku ma ogola wax faragalin ah haba yaraatee mar hadii uu samaysmo.

Hadda hadii qof uu rabo inuu hubiyo runimada Hash-ka, si fudud, xogtii ayuu mar labaad ku samaynayaa Hashing, isagoo sidaas ku ogaanaya runimada Hashing-ka, waana sababtaa sababta uu Satoshi u lahaa, si fudud ayaa loo xaqiijin karaa runimada Hashing-ka, iyadoo hal mar oo kaliya la samaynayo Hashing.

Hubintu ama xaqiijintu la mid ma ahan soo-saarista, waayo soo-saaristu iyada waxay u baahan tahay hawl iyo shaqo badan oo culus, oo joogto ah, si kaliya loo helo Hash ka bilaabmaya tiro ebero ah, halka Hubintu ama xaqiijintu iyada kaliya u baahan tahay hal hawlgal oo kaliya, maadaama la hayyo xogtii iyo Hash-kiiba.

> *For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.*
>
> *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.*

Halkan Satoshi si qoto dheer leh buu uga sii hadlayaa Proof of Work, isagoo markan ka hadlaya farsamooyinka hoose ee Proof of Work (Hab-sugid Shaqo), iyo sida ay iskula xidhiidhsan yihiin Block-yada.

Soo hore umaynaan odhan, waxaa loo baahan yahay in la qabto shaqo adag, taasoo ah in la helo Hash ka bilaabmaya tiro ebero ah, haddaba si loo helo Hash ka bilaabmaya tiro ebero ah, waxaa lagu khasban yahay in isku-dayo badan la sameeyo.

Waa wax aan suuragal ahayn, in isla xogtii marar badan la Hash-gareeyo, lana filo is-bedel, waayo si is-bedel loo helo, waa in marka hore ay wax is-bedelaan, hadii aanba waxa la Hash-garaynayo is-bedelin, Hash-ku marnaba isma bedelayo.

Halkan waydiinta sida iskeed u dhalanaysa ayaa ah: waa maxay waxa la bedelayo, si loo helo Hash-ka qumman ee ka bilaabmaya tirada eberada ah ee ay markaa shabakaddu u baahan tahay? Ma xogta lafteedaa la bedelayaa, oo la faragalinayaa?.

- Maya, xogta ma ahan waxa la faragalinayo, ee waa wax la yidhaahdo "Nonce".

"Nonce" Crypto-da markii la joogo waxaa loo yaqaanaa "Number Used Once", (Tiro Mar-qudha La Adeegsado), waa tiro lagu soo dabto ama lagu helo Hash-ka quman, ee ka bilaabmaya eberada ay shabbakaddu markaa iyada ah u baahan tahay, waa tiro si is-daba-joog ah loo kordhinayo ilaa iyo inta laga helayo Hash-kii ay shabakaddu u baahnayd.

Nonce waa tiro hal mar la adeegsanayo, waayo hadii 2 ama wax ka badan la adeegsado, waxba ma soo kordhayaan, Hash-kuna isma bedelayo, si uu haddaba Hash-ku isku bedelo, oo loo helo Hash qumman, waa in si joogto ah loo kordhiyaa Nonce-ga, ilaa laga helayo Hash-ka bartilmaameedka ah.

TS, aynu ka soo qaadno in ay shabakaddu wakhti xaadirkan rabto Hash ka bilaabmaya 20 eber, xogtuna tahay weedheenii hore ee "CAWO ayaa 2 Bitcoin u dirtay CUDDOON".

Isku-daygeena koowaad, Nonce-gu waa eber (0), hadii aan lagu guulaysan, oo aan la helin Hash-ka bartilmaameedka ah, waxaa la kordhinayaa Nonce-ka, waxaana laga dhigayaa 1, hadii aan wali lagu guulaysanna, waxaa laga dhigayaa 2, hadii kale 3, 4, 5, 6, 7, ….

Nonce-ku waa tiro marba marka ka danbaysa sii kordhaysa, si loogu dabto Hash-ka qumman, sida halkan hoose kaaga muuqataba:

- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 0
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 1
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 2
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 3
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 4
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 5
- …
- …
- …
- …
- …
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 10
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 11
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 12
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 13
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 14
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 15
- …
- …
- …
- …
- …
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 100,000
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 200,000
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 300,000
- CAWO ayaa 2 Bitcoin u dirtay CUDDOON + 498,368 = 000003f698ab190a4… ✓

Hadda kawaran, 498,368 isku-day ayaan samaynay, si aan u helno Hash kaliya ka bilaabmaya 20 eber, in kastuu 20 eber ahayn, ee uu yahay 22 eber hadii aynu bit ahaan u eegno.

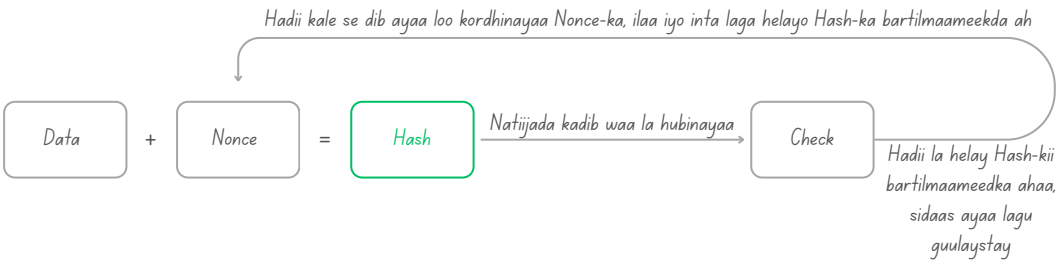
Waadna soo hubin kartaa, kaliya qaado xogtan oo raaci tirada Nonce-ka ah, adigoonan wax bannaan (Space) ah u dhaxaysiinayn, sidan oo kale "CAWO ayaa 2 Bitcoin u dirtay CUDDOON498368", waxaadna heli doontaa isla Hash-ka aynu helnay.

Halkan aynu qodob baraarujinno, Nonce-ka Bitcoin wuxuu leeyahay xad go'an, oo ugu badnaan ah 2,147,483,648 (2.1 bilyan), taasoo ka dhigan markii tiradaa la gaaro, hadii aan wali la helin Hash-kii bartilmaameedka ahaa, in lagu khasban yahay in xogta lafteeda la bedelo, oo lagu bedelo xog kale, ma ahan in isla xogta laf ahaanteed la bedelo, ee waa in xog kale lagu bedelo, sida hadii uu Block-gu ka koobnaa 1,200 oo lacag-diris, laga dhigo 1,300, ama 1,100, amaba lacag-dirisyada lafteeda la bedelo oo kuwo kale lagu bedelo, iyadoon si gaar ah loo faragashanaynin lacag-dirista, si hadana Nonce-ka dib eber loogu soo bilaabo, si loogu soo dabto Hash-ka bartilmaameedka ah.

Hadii aad rabto inaad si kali ah ama si Manually ah u soo-saarto Hash ka bilaabmaya tiro ebero ah, xogta dhamaadkeeda raaci eber, adigoo kordhinaya, ilaa aad ka gaadhayso bartilmaameedkaada, sidan oo kale ".....0".

Hadii kale se aad rabto in si otomaatig ah u hesho, booqo bog ama website, amaba meel aad Code-kan Python-ka ah ku hirgalin karto, adigoo adeegsanaya Code-kan halkan hoose kaaga muuqda, adigoo kaliya bedelaya xogta, iyo tirada eberada aad rabto inaad hesho:

```python
import hashlib

base_text = "CAWO ayaa 2 Bitcoin u dirtay CUDDOON" #Xogta

def find_nonce_with_5_zero_bits(text):
    nonce = 0
    while True:
        t = f"{text}{nonce}"
        h = hashlib.sha256(t.encode()).digest()
        h_bin = ''.join(f"{b:08b}" for b in h)
        if h_bin.startswith('00000000000000000000'): # Hash ka bilaabmaya 20 eber
            return nonce, h.hex(), h_bin
        nonce += 1

nonce, h_hex, h_bin = find_nonce_with_5_zero_bits(base_text)
print("Nonce:", nonce)
print("Hash (hex):", h_hex)
print("Hash (256-bit binary):", h_bin)
```



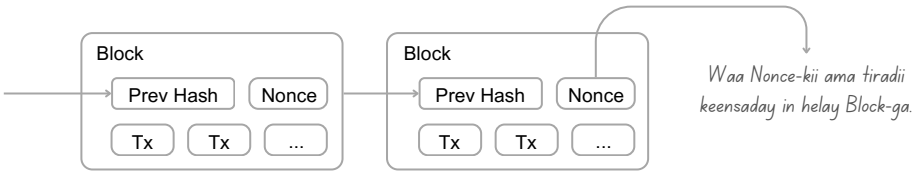
Shaqadan maanta waxaa loo yaqaanaa "**Mining**", qofka qabanayana waxaa loogu yeedhaa "Miner", ama "Qode", waana in la shaqeeyo, si loo helo Hash qumman oo ka bilaabmaya tirada eberada ee ay shabakaddu u baahan tahay, tiradaasoo marba marka ka danbaysa sii kordhaysa.

Waayo, waxaa jira wax kaloo la yidhaahdo "Difficulty Adjustment", kaasoo ah in ay shabakaddu dib isku cusboonaysiin samayso 2016 kastoo Block kadib, celcelis ahaan 2 todobaad kasta, halkaas oo ay shabakaddu isku dheelli-tirayso heerka adkida ee loo baahan yahay, iyo Miners-yada ku jira shabakadda.

Hadii ay Miners badan shabakadda ku soo biiraan, heerka adkida ayaa kordhaya, ama tirada eberada ee loo baahan yahay ayaa kordhaya, hadii ay yaraadaanna heerka adkida ayaa is dhimaya, si shabakaddu iskugu dheeli-tirnaato, oo halkii Block loogu ilaaliyo 10 daqiiqo.

Wuxuu kaloo Satoshi yidhi mar hadii uu samaysmo Block-gu, iyadoo la bixinayo tamar iyo wakhti badan, ama uu kumbiyuutarku bixinayo dadaal iyo tamar badan, si loo helo Hash-ka bartilmaameedka ah, lama awoodi doono in dib wax looga bedelo Block-gii, waayo waxaa lagu khasban yahay in hadana dib loo bixiyo dadaal iyo tamar la mid ah tii hore, si hadana mar labaad loogu guulaysto Hash-ka bartilmaameedka ah, maxaa yeelay Hash-kii hore wuu is-bedelay, kadib markii la bedelay xogta.

Intaas waxaa dheer, in Block kasta uu la xidhiidhsan yahay Block-gii ka horreeyay isaga, ama Hash-ka Block-gii ka horreeyay, taasoo ka dhigan in hadana lagu sii khasban yahay in Block-ga wax laga bedelay ma ahee, kuwa ka danbeeya oo dhan la bedelo, si ay shabakadu isku la jaanqaaddo, maxaa yeelay Block waliba midkii ka horeeyay ayuu ku xidhan yahay, sidii silsiladda, waana halkaa halka ay ka magac baxday "Chain", kadibna "Block**chian**", (Silsilad Block-yo Ah).



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.

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.

Halkan Satoshi wuxuu kaga hadlayaa dhib weyn oo bilawgii Internet-ka ka jiray, ilaa maantana taagan, waana marka uu qof kali ah awoodo inuu iska dhigo dhowr qof, ama boqolaal qof, si uu codad badan u yeesho, wuxuuna Satoshi rabaa inuu go'aamiyo cidda loo aqoonsanayo cod-bixiyayaasha ama go'aan-dajjiyayaasha aqlabiyadda ah, (Majority Decision Making), marka la doonayo in si Online ah afti-uruuruin ama codayn loo sameeyo.

Hadii aad maanta rabto inaad doorasho ka qeyb gasho, way adag tahay inaad dhowr qof iska dhigto, adigoo dhowr aqoonsi samaysanaya, amaba siyaabo kale ku samaynaya, sidaasina aad ku yeelato dhowr cod.

Hase ahaatee hadii isla doorashadaas laga dhigo mid Online ah, aad iyo aad bay u fudud tahay in aad dhowr qof iska dhigto, adigoo helaya dhowr IP address-yo aan mararka qaar dhammaad lahayn, si aad u yeelato dhowr cod, waana sababtaas sababta ay ilaa haatan u adag tahay in si Online ah doorasho loo qabto.

Hadii la yidhaahdo, halkii IP address wuxuu u dhigmaa hal cod, waxaa si fudud loo heli karaa IP address-yo badan oo badan oo badan, sidaasina waxaa lagu yeelanayaa codod badan oo badan oo badan.

Sidaa darteed, si aysan tan u dhicin Satoshi wuxuu yidhi xalku waa hal CPU, hal cod, bedelkii laga dhigi lahaa hal IP address, hal cod.

Maanta bedelkii CPU waxaa inta badan la adeegsadaa ASIC, iyo mararka qaar GPU, sidaa darteed, waxaynu bedelkii CPU adeegsanaynaa ASIC, sida aynu hore u soo dhinina ASIC waa qalab loogu talagalay Hashing-ka iyo Proof of Working-ka, ahna qalab aad uga wax tar badan CPUs-ka iyo GPUs-ka.

Satoshi si dhab ah uma xallinin dhibkan, kaliya si xeeladaysan buu u yareeyay, oo uu u dhimay, hasa yeeshee dhibku wali wuu taagan yahay, waxaana mar labaad la awoodaa in la helo ASIC dheeraad ah, sidaasina lagu helo codod dheeraad ah, waana waxa loo yaqaan "Sybil Attack".

Sybil Attack: Waa jaad ka mid ah weerarada Internet-ka ka dhaca. Crypto markii la joogo waa in la samaysto aqoonsiyo iyo nodes-yo badan, si loo helo codod badan. Ciddii awood u leh inay hesho awood badan, waxay awood u leedahay inay yeelato codod badan, hasa ahaatee wali way xaddidan yihiin, oo ma la awoodi karo codod aad iyo aad u tiro badan, si la mid ah IP address-yada:

- **10,000 IP** address xogaa way iska yar fudud tahay in la helo
- **10,000 ASIC** ama awood kubiyuutareed oo badan oo shaqaynaya 24/7, aad iyo aad iyo aad bay u adag tahay in la helo, waxayna u baahan tahay lacag badan si loo helo, iyo tamar badan si loo kiciyo.

Satoshi ma uusan cidhib-tirin dhibkan, ee wuu yareeyay, wuxuuna ka dhigay mid kharash badan u baahan, oo aan si fudud lagu samayn karin.

Qofkii raba inuu dhowr qof iska dhigo wuxuu ku khasban yahay inuu dhowr qalab ama dhowr kumbiyuutar helo, ama awood badan isku keeno, taasoo aad u kharash badan.

Marka uu Satoshi leeyahay Hal ASIC waa hal cod, micnaheedu ma ahan in halkii qalab ee CPU, GPU ama ASIC ah uu leeyahay hal codbixin, ee waa in codkiisu ku miisaaman yahay awoodda qalabadiisa oo dhan.

TS, qofka haysta 1 ASIC ama 3 ASIC, la mid ma ahan, oo iskuma cod miisaamna qofka haysta 30 ASIC, maxaa yeelay wuu ka awood badan yahay, cod-bixintuna waa awoodda uu Node-ku leeyahay, markii la isku geeyo qalabadiisa oo dhan.

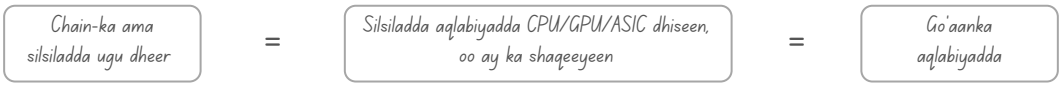
Satoshi si uu fahamka dadka u soo dhaweeyo darteed ayuu u yidhi Hal CPU/GPU/ASIC wuxuu u dhigmaa hal codbixin, hasa yeeshee halkii codbixin waa isku-geynta awoodda halkii Node.

Wuxuu kaloo Satoshi yidhi, go’aan-qaadashada aqlabiyadda waxay u taagan tahay silsiladda ugu dheer, taasoo lagu bixiyay tamar (ASIC) badan.

Go’aanka (Decision) la jeedo waa go’aaminta waxa qumman iyo waxa aan qummanayn, sida lacag-diristan ma qumman tahay mise ma qummana.

Halka aqlabiyaddu (Majority) tahay sidii la is kugu raacay go’aanka, sida in lacag-diristan ay qumman tahay waxaa isku raacday aqlabiyadda shabakadda, oo macnaheedu tahay Nodes-yada ugu badan ee shabakadda ku jira, kuwaasoo ah cidda go’aamisa wax kasta oo shabakadda ka dhex socda, sida lacag-diristii qummanayd, iyo ciddii xaqqa u lahayd, iwm.

Silsiladda ugu dheer waa silsiladda aqlabiyadda CPU/GPU/ASIC dhiseen, oo ay ka shaqeeyeen, sidaa darteedna waa tan aqlabiyadda go’aan-qaadashada leh, oo ay shabakaddu mar waliba qaadanayso, socodsiinaysana.



Marka uu Satoshi leeyahay: "*The majority decision is represented by the longest chain...*", macnaheedu ma ahan silsiladda ama Blockchian-ka ugu dheer tiro ahaan, ee waa Blockchain-ka ama silsiladda shaqada ugu badan lagu bixiyay, waana tan la isku raacsan yahay.

Maxaa yeelay hadii ay tiro ahaan noqon lahayd, si fudud baa lagu soo saari lahaa Block-yo badan, sidaasina waxaa ku samaysmi lahayd silsilad ka dheer silsiladda tamarta badan lagu bixiyay.

Haddaba markii ay silsilad gaar ah noqoto tan ugu dheer, macnaheedu waa in ay silsiladdaas tahay tan tamarta iyo wakhtiga ugu badan lagu bixiyay, lagana shaqeeyay (PoW).

Hadii Nodes-yada daacadda ahi (Honest Nodes), oo ah kuwa raaca xeerarka dagsan, ee aan is-daba-marinta iyo been-abuurka wadin, yihiin aqlabiyadda shabakadda, oo ay gacanta ku hayyaan awoodda shabakadda inteeda badan, shabakadda ayaa sii dhisi doonto silsiladda ama Blockchain-ka ugu dheer, ee tamarta ugu badan lagu bixiyay, waxayna had iyo jeer si joogto ah uga dheereen doontaa silsilad kasta oo been-abuur ah oo ka soo garab-baxda silsiladda daacadda ah.

Tani waxay keenaysaa in silsiladda ugu dheer ee leh wax-qabadka ugu badan (Longest Chain With Most Work) noqoto tan loo aqooonsan yahay inay mar kasta tahay tan qumman, waayo waxaa lagu bixiyay aqlabiyadda awoodda shabakadda.

Go’aanka aqlabiyadda ama go’aanka ay shabakaddu ku heshiiso waa kan ay dhiseen Nodes-yada daacadda ah, kuwaas oo ay ku bixiyeen, isla mar ahaantaana galiyeen wakhtigooda, tamartooda, iyo processors-kooda (CPU/GPU/ASIC).

To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

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.

Halkan Satoshi wuxuu tilmaamayaa sida ay u adag tahay in xog hore loo diiwaan galiyay, dib wax looga bedelo, isagoo yidhi hadii la damco in Block hore loo diiwaan galiyay, dib wax looga bedelo, cidda isku dayaysa inay bedesho, oo uu Satoshi ugu yeedhayo "Attacker" (Weeraryahan), waxay ku khasban tahay inay dib u samayso shaqadii Proof of Work-ga ahaa, ee la raadinayay ebereda badan, intaas uun ma ahee, inay sidoo kale dib hadana u bedesho Block-yadii ka danbeeyay Block-ga wax laga bedelayay, oo hadana dib shaqo kale loo galo, si loola tartamo Nodes-yada daacadda ah.

Maxaa yeelay sida aynu hore u soo nidhi Block-kasta wuxuu la xidhiidhsan yahay Block-gii ka horreeyay, hadii mid ka mid ah la bedelo, waxaa lagu khasban yahay in dib hadana loo wada bedelo Block-yadii ka danbeeyay oo dhan, si ay mar kale silsiladdu iskula xidhiidho.

Satoshi wuxuu Nodes-yada aan daacadda ahayni u adeegsanayaa ama uu ugu yeedhayaa weeraryahan, ama Attacker, maadaama uu weerar ku yahay shabakadda.

Haddaba hadii uu weeraryahan isku dayo in uu wax ka bedelo tusaale ahaan Block-ga 10-aad, haatanna ay shabakaddu marayso Block-16-aad, wuxuu weeraryahankaas ku khasban yahay inuu Block-ga 10-aad dib uga shaqeeyo, oo uu raadiyo Hash ka bilaabmaya tiradii eberada ahaa ee la rabay, kadib hadii uu ku guulaysto uu hadana Block-ga 11-aad dib uga shaqeeyo, kadibna uu u sii guuro 12-aad, ilaa iyo inta uu ka gaadhayo silsiladda daacadda ah.

Silsiladdaas oo aan markeedii horeba sii sugaynin, maxaa yeelay inta uu ka shaqeynayo Block-ga 10-aad, shabakaddu iyaduna way sii shaqaynaysaa, waxaana ku soo biiraya tiro cusub oo Block-yo ah.

Waana sababtaas sababta uu Satoshi u lahaa, wakhti kadib, waxaynu arkaynaa in ay si tartiib-tartiib ah u soo yaraanayso suurtagalnimada uu weeraryahanku ku gaadhi karo silsiladda daacadda ah, maxaa yeelay lama tartami karo Nodes-yada shabakadda ku jira oo dhan, isagoo ah hal qof ama tiro koox ah.

Mar allaale markii Block cusub lagu soo biiriyo shabakadda waxaa si weyn hoos ugu dhacaysa awoodii uu weeraryahanku lahaa, mana awoodi doono in uu xittaa u dhawaado silsiladda daacadda ah, waayo inta uu hal Block ka shaqaynayo, silsiladda waxaa ku soo biiraya tiro Block-yo ah oo cusub, sidaa darteed marnaba suuragal ma ahan in xog ama Block la diiwaan galiyay dib wax looga bedelo, maxaa yeelay Nodes-yada daacadda ah iyo kuwa aan daacadda ahayn isku tallaabo ma noqon karaan.

Waana sababta ay ganacsatada qaar ama ururada qaar u yidhaahdaan lacag-diristaadu waa inay ka soo wareegtaa "6 Confirmations" oo micnaheedu yahay 6 xaqiijimood, oo loola jeedo in Block-ga ay lacag-diristaadu ku jirto, ay ka soo wareegto 5 Block oo danbe, si ay lacagtaas u noqoto lacag aan suuragal ahayn in dib loo-la noqdo ama wax laga bedelo.

TS, Hadii Block-ga ay lacag-diristaadu ku jirto tahay Block-ga #100, waxaad u baahan tahay 5 Block oo danbe oo cusub, oo aan ahayn Block-ga ay lacag-diristaadu ku jirto, si ay lacag-diristaadu u noqoto mid aad iyo aad iyo aad u adag in wax laga bedelo (Irreversible Almost), sida:

- Block #100 → 1 Confirmations (suurtagalnimadu way jirtaa)
- Block #101 → 2 Confirmations (suurtagalnimadu way sii yaraanaysaa)
- Block #102 → 3 Confirmations (suurtagalnimadu way sii yaraanaysaa oo ay sii adkaanaysaa)
- Block #103 → 4 Confirmations (suurtagalnimadu aad iyo aad bay u sii adkaanaysaa)
- …
- Block #105 → 6 Confirmations (waxay noqonaysaa mid aanba suuragal ahayn, kanshaduna waa 0.000…1%)

Halkan mid aynu baraarujino, suurtagalnimadu macnaheedu ma ahan in ay dhacayso, ee waa in ay dhici karto, xittaa hadii ay fursadeedu ama kanshadeedu ka yar tahay 0.0000000000000…..1%, marba hadii ay jirto jaanis ama fursad, ama kansho uu ku dhici karo, waxaasi waxaa lagu tilmaamayaa suuragal, haba iska yaraadee.

Sidaa darteed, marka aynu leenahay suurtagalnimadu way jirtaa, macnaheedu waa in ay jirto kansho, haba iska yaraatee, gaar ahaan wakhtigan (1447H), kanshadu waxay ku dhawdahay suuragal li'i (Impossible) in xittaa isla Block-ga koowaad ama Block-ga ay lacag-diristaadu ku jirto la bedelo, iyadoon la sugin Block-yo danbe.

> *To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.*
>
> *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.*

Halkan Satoshi wuxuu uga hadlayaa qaabkii shabakadda la iskugu dheelli-tiri lahaa, si aysan shabakaddu marna u adkaan, marna u fududaan, isagoo yidhi heerka adkida oo uu ula jeedo tirada eberaad ee ay shabakaddu rabto, waxay ku xidhan tahay ama lagu go'aamiyaa xawaaraha lagu helayo halkii Block.

Satoshi wuu ogaa in ay tignoolajiyaddu hormari doonto, oo la soo-saari doono qalabo aad iyo aad u awood badan sida ASIC oo kale, kuwaasoo ilbiriqsiyo gudahood ku awooda inay ku helaan Hash ka bilaabmaya tiro go'an oo ebero ah.

Sidaa darteed, si aysan shabakaddu u fududaan markii la helo qalabo aad u awood badan, sidoo kalena aysan u adkaan markii ay Nodes-yo qaar ah go'aansadaan inay shabakadda ka baxaan, wuxuu Satoshi dajiiyay xeer maanta loo yaqaan "Difficulty Adjustment", oo aynu hore wax uga nidhi.

Difficulty Adjustment: Waa in ay shabakaddu dib isku cusboonaysiin samayso 2016 kastoo Block kadib, celcelis ahaan 2 todobaad kasta, halkaas oo ay shabakaddu isku dheelli-tirayso heerka adkida ama fududaanta ee loo baahan yahay.

Wuxuuna Satoshi yidhi heerka adkida ama tirada eberada ee la rabo in la helo, waxay ku xidhan tahay ama waxaa go'aamiya xawaaraha lagu helayo halkii Block.

Hadii si dhakhso badan lagu helo, waxaa kordhaya heerka adkida, ama waxaa kordhaya tirada eberada ee loo baahan yahay in la helo.

Hadii kale se oo ay Nodes-yo qaar go'aansadaan inay shabakadda si ku-meel-gaar ah uga baxaan, taasoo sababaysa gaabis, waxaa is-dhimaya heerka adkida, ama tirada eberada ee loo baahan yahay ayaa is-dhimaysa oo yaraanaysa.

Haddaba waa maxay waxa looga qiyaas qaadanayo, oo loo odhanayo shabakaddu markan way gaabinaysaa, ama way dheereenaysaa?

Waa xeerka kale ee uu Satoshi u dajiiyay Block-ga, isagoo halkii Block celcelis ahaan ka dhigay in uu qaato 10 daqiiqo.

Hadii 10 daqiiqo wax ka badan lagu soo saaro Block-gii, waxaa is-dhimaya heerka adkida, hadii 10 daqiiqo wax ka yar lagu soo saarana, waxaa kordhaya heerka adkida.

Hadii ay Nodes-yo badan shabakadda ku soo biiraan, amaba ay tignoolajiyaddu hormarto, oo la helo qalabo aad u xawaare sarreeya, heerka adkida ayaa kordhaya, ama tirada eberada ee loo baahan yahay ayaa kordhaya, hadii ay yaraadaanna heerka adkida ayaa is-dhimaya, si shabakaddu iskugu dheeli-tirnaato, oo halkii Block celcelis ahaan loogu ilaaliyo 10 daqiiqo.

- Hadii ay ka dhakhso battaan **10 daqiiqo/Block** → Difficulty ama heerka adkida ayaa kordhaya
- Hadii ay ka gaabiyaan **10 daqiiqo/Block** → Difficulty ama heerka adkida ayaa is-dhimaya, oo hoos u dhacaya

Wuxuuna is-bedelku ama is-cusboonaysiintu dhacdaa 2016 kastoo Block kadib, celcelis ahaan 2 todobaad kasta, ama 14 maalmood.

Waana sababtaas sababta uu Satoshi u yidhi waxaa heerka adkida lagu go'aaminayaa celcelis si joogto ah isu-bed-bedelaya (Moving Average), oo ah Nodes-yada marna shabakada ku soo biiraya, marna ka baxaya, taasoo ujeedkeedu yahay in lagu helo celcelis tiro go'an oo Blocks-yo ah saacadii (Target Average), oo ah in sacaddii la helo 6 Block, maadaama uu halkii Block celcelis ahaan qaato 10 daqiiqo.

Aynu sii kala saarno, Satoshi wuxuu xusay laba Avrage ama labo celcelis:

- **Moving Average:** Waa celcelis si joogto ah isu bed-bedelaya, kaasoo ku xidhan Nodes-yada shabakada ku jira, iyo qalabada la adeegsanayo, oo is-bed-bedela, marna kordhaya marna is-dhimaya
- **Target Average:** Waa celcelis la doonayo in halkii Block lagu ilaaliyo 10 daqiiqo, 1-kii saacna 6 Block

5. Network (Shabakadda)

The steps to run the network are as follows:

1. *New transactions are broadcast to all nodes.*
2. *Each node collects new transactions into a block.*
3. *Each node works on finding a difficult proof-of-work for its block.*
4. *When a node finds a proof-of-work, it broadcasts the block to all nodes.*
5. *Nodes accept the block only if all transactions in it are valid and not already spent.*
6. *Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*

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.*

Qeybtan 5-aad wuxuu Satoshi uga hadlayaa sida ay shabakaddu u shaqayso tallaabo-tallaabo, iyo sida ay si iskeed ah isu maamusho, iyadoon loo baahnayn maamul dhexe, isagoo ku bilaabay tallaabooyinkan 6-da ah:

1. Tallaabada koowaad, lacag-diris kasta oo cusub oo la sameeyo waxaa loo dirayaa dhammaan Nodes-yada shabkadda ku jira.

2. Tallaabada labaad, wuxuu Node kasta bilaabayaa inuu si gaar ah u uruuriyo lacag-dirsyada cusub, kuna uruuriyo Block cusub

3. Tallaabada saddexaad, wuxuu Nodes kasta bilaabayaa inuu ka shaqeeyo Block-gii uu lacag-dirisydii cusbaa ku uruursaday, isagoo raadinaya Hash ka bilaabmaya tiro ebero ah, oo ay markaa shabakaddu rabto

4. Tallaabada afaraad, Markii mid ka mid ah Nodes-yada uu helo Hash-kii bartilmaameedka ahaa, waxaa Block-gaas loo dirayaa Nodes-yadii kale oo dhan, si loo ogaysiiyo in la heley Block heblaayo

5. Tallaabada shanaad, waxaa la hubinayaa Block-gii in uu buuxiyay shuruudihii, in lacag-dirisyada ku jira ay yihiin kuwo qumman oo aan hore meelo kale loogu laba kharashgarayn, oo aan Double Spending la samaynin, kadibna hadii ay wax waliba qumman yihiin Block-gaas waa la ansixinayaa, silsiladii ama Blockchain-kii baana lagu soo biirinayaa.

6. Tallaabada lixaad, kadib markii la ansixiyay Block-ga, Nodes waliba wuxuu hadana dib u guda bilaabayaa shaqo cusub, isagoo raadinaya Hash-ka Block-ga xiga, isla mar ahaantaana adeegsanaya Hash-ka ama summadda Block-gii la ansixiyay, sidaas ayayna ku samaysantaa silsiladda.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proo-fof-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

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 loo qaato. Xaaladan ayaa la jabin doonaa markii hab-sugidda shaqo lagu helo laanta ugu dheer, oo ay hal laan noqoto, waxayna Nodes-yada kale ee ka shaqaynayay laanta kale u soo guuri doonaan laanta ama silsilada ugu dheer.

Halkan Satoshu wuxuu uga hadlayaa sida ay shabakaddu xaaladaha qaar ee soo darriya uga baxdo, sida xaaladda loo yaqaan "Temporary Fork", kala qeybsani ku-meel-gaar ah, ama laan ku-meel-gaar ah.

Wuxuuna hadalkiisa ku bilaabay, Nodes-yadu waxay mar waliba silsiladda ugu dheer u tixgaliyaan, una aqoonsadaan inay tahay tan ugu qumman, waxayna ku dadaalaan sidii ay uga sii shaqayn lahaayeen, una sii ballaadhin lahaayeen, ugana dhigi lahaayeen tan mar waliba ugu dheer, tamarta ugu badanna lagu bixiyay.

Haddaba hadii ay laba Node si kadis ah mar qudha u wada helaan Hash-kii bartilmaameedka ahaa, dabeetana mar qudha u soo wada saaraan laba Block oo kala duwan, oo ay labaduba qumman yihiin, una dhamaystiran yihiin shuruudihii, silsiladdu ama Blockchain-ku si ku-meel-gaar ah bay u qeybsami doontaa, waxayna yeelan doontaa laan cusub oo ku-meel-gaar ah, oo loo yaqaan "**Temporary Fork**".

Nodes-yaduna waxay u qeybsami doonaan laba qeybood, **Node B** oo hor arkaya **Block B**, iyo **Node T** oo hor arkaya **Block T**.

Satoshi wuxuu yidhi xaaladan oo kale markii lala kulmo, oo ay yar tahay inay dhacdo, ayaa labada qeybood ee Nodes-ku mid waliba si gaar ah uga shaqayn doonaa Block-ga uu hor arkay, ama uu hor helay, iyadoo silsiladda laanteeda kale uu mid waliba si ku-meel-gaar ah u kaydinayo, si hadii ay mustaqbalka u noqoto tan ugu dheer loogu guuro, sidaas ayayna labada silsiladood isku barbar soconayaan.

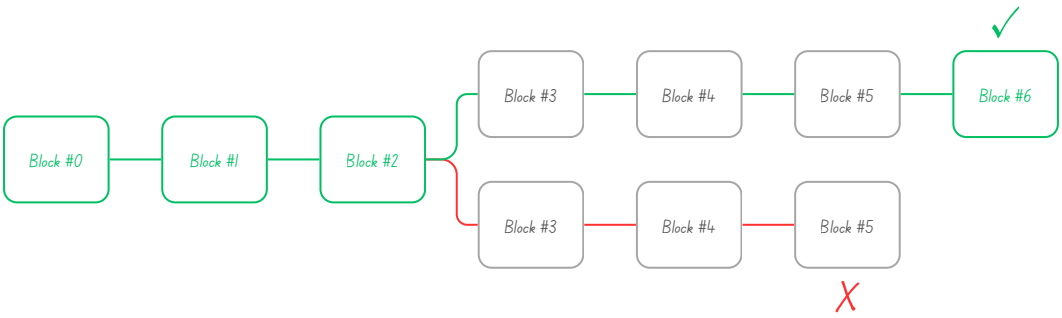
Ilaa uu midkood hor helo Block cusub oo dheeri ah, oo ay sidaa ku noqoto tan ugu dheer, markaasna Nodes-yadii kale ee silsiladda laanteeda kale ka shaqaynayay waxay u soo wareegi doonaan silsiladdan ugu dheer.

TS, laba Node ayaa hor helay Block #101, shabakaddu si ku-meel-gaar ah bay u qeybsamaysaa:

- **Node B**, waxay hor arkeen nuqul ka mid ah **Block #101**
- **Node T**, waxay hor arkeen nuqulkii kale ee **Block #101**

Qolo waliba si gaar ah bay uga shaqaynayaan nuqulkii ay hor heleen.

Haddaba hadii ay hadana mar labaad wada helaan Block #102, silsiladdu wali si ku meel gaar ah bay u qeybsanaan doontaa, hadii ay hadana mar saddexaad dhacdo in ay wada helaan Block xiga ee ah #103, sidii si le'eg, ilaa uu midkood hor helo Block cusub, ka hor kan kale, oo ay sidaas ku noqoto hal silsilad, dabeetana loo guuro, oo ay sidaas mar labaad ku noqoto sillsiladda ugu dheer.



New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

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 silsiladu wax ka maqan yihiin ayuu codsanayaa.

Halkan Satoshi wuxuu uga hadlayaa sida ay shabakaddu u tahay mid dulqaad u leh xaaladaha qaar (Fault Tolerant), ee aan laga baaqsan karin, iyo sida ay uga soo kabsanayso, maadaama ay wax waliba yihiin Decentralized, isla mar ahaantaana ku salaysan yihiin qof-ka-qof (P2P), isagoo hadalkiisa ku bilaabay, laguma khasbana in ay lacag-diris kasta oo cusub gaadho dhammaan Nodes-yada shabakadda ku jira, si loo xaqiijiyo, ee kaliya waxaa ku filan in ay gaadho tiro Nodes-yo ah.

TS, hadii uu qof lacag diro, lacagtaasna ay arki waayaan Nodes-yada qaar, wax dhibaato ah ma lahan, waayo shabakaddu waa mid baahsan, oo aan hal ama dhowr Node kaliya ku xidhnayn, hadii ay kaliya arkaan dhowr Node ugu danbayntii lacag-diristaas waxay noqon doontaa mid la xaqiijiyo, oo lagu soo daro silsiladda, ama Blockchain-ka, khasabna ma ahan mar waliba in ay lacagtaas gaadho dhammaan Nodes-yada shabakadda ku jira.

Dhanka kale, hadii uu Node arki waayo Block gaar ah, iyadna wax dhibaato ah ma lahan, markii uu ogaado in ay nuqulkiisa ka maqan yihiin Block gaar ah, si fudud ayuu shabakadda uga codsanayaa dhamaystirka silsiladdiisa.

TS, Node B, waxaa ka maqan #102, hasa yeeshee wali ma oga inay wax ka maqan yihiin, markii uu helay Block #104, ayuu ogaaday in ay silsiladiisu ka maqan tahay Block #103, si fudud wuxuu shabakadda ka codsanayaa Block #103, wuxuuna ku biirinayaa silsiladiisa, sidaasina wuxuu ku haystaa nuqul dhamaystiran. Waana sababtaas sababta uu Satoshi u leeyahay shabakaddu waa mid dulqaad u leh xaaladaha qaar, sida xogaha maqan oo kale.

6. Incentive (Dhiirigalinta)

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

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.

Qeybtan 6-aad wuxuu Satoshi kaga hadlayaa abaalmarinta uu helayo Node-ku markii uu shaqo qabto kadib, wuxuuna u adeegsanayaa ereyga dhiirigalin ama Incentive. Marka ay Nodes-yadu si daacadanimo leh u shaqeeyaan, una ilaaliyaan shabakadda, waxay badelkeeda helayaan abaalmarin, taasoo ku dhiirigalinaysa inay shaqadooda sii wadaan, si loo helo hannaan is-maamul, oo madax-bannaan.

Wuxuuna hadalkiisa ku bilaabay, sida xeerku yahay Transaction-ka ugu horreeya ee Block kasta waa mid gaar ah, oo maanta loo yaqaan "Coinbase Transaction", waana Transaction-ka dhaliya ama soo-saara lacagta cusub, taasoo lagu abaalmarinayo qofkii soo saaray Block ee helay Hash-kii bartilmaameedka ahaa, qofkaasoo maanta loo yaqaan "Miner".

Block kasta oo cusub oo la soo-saaro waxaa la-la soo saaraa ama la dhasha tiro lacag ah oo go'an oo cusub, taasoo abaalmarin u ah Miner-kii ama qofkii soo saaray ee heley Hash-ka Block-ga, waxaana lacagtaas cusub maanta loo yaqaanaa "Block Reward", Abaalgudka Block-ga. Lacagtaas Transaction-ka soo saarana waxaa loo yaqaanaa "Coinbase Transaction".

Coinbase Transaction: Waa Transaction-ka ugu horreeya ee block kasta, waana mid ay abuuraan Miners-ku, kaas oo ay ku dalbanayaan abaalgudka iyo Fee-ga ama khidmadda xawaaladihii ku jiray Block-ga, waana Transaction-ka sida dhabta ah u abuura Bitcoin cusub, kaasoo aan lahayn wax Input ah, kaliya waa Output, maxaa yeelay Transaction-kaas ma ahan mid uu qof soo diray, ee waa mid la curiyay, waana sababtaas sababta ka dhigaysa mid gaar ah.

Block Reward-kan ama abaalgudkan waxay dhiirigalin u tahay Nodes-yada Miners-ka ah, ee shaqadii adkayd qabanaya (PoW), si ay u sii wattaan shaqadooda, una sii taageeraan shabakadda, maadaama ay shabakaddu abaalmarinayso.

Sidoo kale Block Reward-ku waa qaab ay lacagta cusubi u timaado suuqa, looguna soo daayo bulshada dhexdeeda, si ay isu-waydaarsadaan, maadaama aysan jirin bangi dhexe ama hay'ad dhexe oo lacagta suuqa keenta, oo fidisa.

Halkan Satoshi wuxuu qaabkan Block Reward-ka ah barbardhigay tusaalahan, wuxuuna yidhi sida ay macdan qodoyaasha dahabka soo saara u adeegsadaan agabka dahabka lagu soo-saaro, si ay dahab cusub u soo saaraan, suuqana ugu soo biiriyaan, ayay Bitcoin qodoyaashooda u adeegsadaan CPU/GPU/ASIC iyo koronto, si ay Bitcoin cusub u soo saaraan, suuqana ugu soo biiriyaan.

Tusaalahan uu Satoshi soo qaatay waxay si weyn uga turjumaysaa aragtida Bitcoin, Bitcoin-na ma ahan wax si dheel-dheel ah ama meel madhan looga helayo, ee waa sida dahabka oo kale, waa in bedelkeeda wax la kharashgareeyaa oo la bixiyaa tamar iyo koronto, si loo helo.

Sidaa darteed, helitaanka Bitcoin ma ahan wax iska fudud, oo gujin ama Click kaliya ku samaysmaya, ee waa mid u baahan shaqo adag, oo marba marka ka danbaysa sii adkaanaysa, waana mid ka mid ah sababaha keensanaysa in ay si joogto ah qiimaheedu u sare kaco, sida dahabka oo kale.

Block Reward-ku dhanna waa lacag curin cusub, dhanna waa abaalmarin lagu abaalmarinayo Miner-kii ama qofkii helay Block-ga, dhanna waa qaab lacagta suuqa loogu keenayo, sida dahabka oo kale.

> *The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.*
>
> *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.*

Satoshi wuxuu yidhi intaas uun ma ahee, waxaa sidoo kale Miner-ka lagu abaalmarinayaa khidmadaha ama Fees-ka la socda lacag-dirisyada, Fee-gaasoo ah lacag ka dheeri ah lacagta la dirayo, ama la rabo in la helo.

TS, hadii lacagta la adeegsanayo oo ah Input-kii yahay 0.5 Bitcoin, halka lacagta la dirayo ama la bixinayo oo ah Output-kii yahay 0.49 Bitcoin, waxaa 0.01 Bitcoin ee soo hadhay laga dhigayaa khidmad, waxaana lagu biirinayaa abaalmarintii uu Block-ga, ama Block Reward-ka, Block-gaasoo markii horeba ka koobnaa tiro lacag-dirisyo ah.

Sidaa darteed, qofka Miner-ka ah kaliya abaalmarin ahaan uma helayo lacag cusub, ee sidoo kale wuxuu abaalmarin ahaan u helayaa khidmadaha ku jira lacag-dirisyada Block-giisa ku jira, ee uu xalliyay, ama uu soo saaray, taasoo dhiirigalin u ah Miner-ka.

Haddaba markii la gaadho tiro go'an oo uu Satoshi ula jeedo, markii la soo saaro dhammaan tiradii Bitcoin loo qoondeeyay, waxay dhiirigalintu ama abaalmarintu noqonaysaa oo ay u wareegaysaa kaliya khidmadaha ama Fees-yada lacag-dirisyada, waayo ma jirto lacag danbe oo cusub oo la soo saari karo, sidaasina Bitcoin waxay ku noqonaysaa hannaan-lacageed oo ka madax-bannaan sicir-barar.

Haatan Miner-ku wuxuu leeyahay laba ilood oo dakhli ah, Bitcoin cusub iyo Fee-ga lacag-dirisyada, hasa yeeshee markii la gaaro tiro go'an oo ah 21 milyan oo Bitcoin ah, ama markii la soo saaro dhammaan tiradii loo qoondeeyay Bitcoin, wuxuu yeelanayaa hal il oo kaliya, waana Fee-ga lacag-dirisyada.

Abaalmarinta ayaa si tartiib tartiib ah isku dhimaysa, isla mar ahaantaana u wareegaysa khidmadaha ama Fees-ka lacag-dirisyada, qaabkan ayaa mustaqbalka Bitcoin ka dhigaysa mid sii shaqayn doonta oo aan joogsan doonin markii la soo saaro dhammaan Bitcoin-tii la qoondeeyay oo ah 21 milyan.

Wakhti xaadirkan Block Reward-ku waa 3.125 Bitcoin oo cusub, taasi micnaheedu waa in Block kasta oo la soo saaro celcelis ahaan 10 daqiiqo, lala curiyo 3.125 Bitcoin oo cusub oo abaalmarin ama Reward ah, Reward-kaasoo bilawgeedii hore ka bilaabmay 50 Bitcoin.

Waxaa jira wax la yidhaahdo "Halving", kaasoo ah in abaalgudka la kala badho 210,000 kastoo Block kadib, ilaa ay ugu danbayntii noqoto eber, dabeetana loo guuro Fees-ka.

Ciddii rabta faahfaahin aad u xeel dheer oo la xidhiidha arinkan, waxaannu talo ahaan u soo jeedinaynaa, inay PDF-kan akhrisato↗, si ay si qoto dheer leh u fahamto sabab ayay Bitcoin u tahay 21 milyan, iyo siday ku noqotay, iyo run ahaantii ma 21 milyan oo dhab ah baa, mise?

> *The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.*
>
> *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.*

Halkan Satoshi wuxuu leeyahay, abaalmarintu waxay keensanaysaa in ay Nodes-yadu daacadnimadoodu ku sii taagnaadaan, maxaa yeelay waxay si joogto ah u helayaan abaalmarin, taasoo ku dhiirigalinaysa inay si daacadnimo leh u shaqeeyaan.

Hadii qof damac badan oo uu Satoshi ku tilmaamayo weeraryahan damac badan ama Greedy Attacker, doonayo in uu tusaale ahaan lacag laba kharashgareeyo oo uu sameeyo Double Spending, wuxuu u baahan yahay inuu awood badan isku keeno, si uu u fuliyo weerarkiisa. Haddaba hadii weeraryahankaasi awoodo in uu isku keeno awood ka badan awoodda kuwa daacadda ah, oo ay taasi u suurtagasho, waxaa u furan laba doorasho midkood:

1. Inuu awooddiisa u adeegsado siyaabo khaldan, sida in uu lacag laba kharashgareeyo, isla mar ahaantaana uu u wiiqo hannaanka.
2. Inuu awooddiisa u adeegsado si uu dakhli badan uga sameeyo, isagoo soo saaraya Bitcoin cusub oo ka badan isku darka Nodes-yada daacadda ah intii ay soo saari jireen, oo uu sidaasi awoodiisa uga faa'idaysto.

Wuxuuna Satoshi si dadban ugu doorayaa doorashada labaad, isagoo leh, waa in uu weeraryahanku ogaadaa in raacista xeerarka ay ka faa'ido badan tahay ku ciyaaristeeda, isagoo qofku helayo dakhli joogto ah oo ka badan isku darka dakhligii ay heli jireen Nodes-yda daacadda ah, maadaama uu ka awood badan yahay.

Intaas waxaa dheer, hadii uu weeraryahanku siyaabo khaldan u adeegsado awooddiisa, sida in uu Double Spending sameeyo oo kale, waxaa hoos u dhacaysa kalsoonidii lagu qabay Bitcoin, waxayna noqonaysaa mid Centralized ah, oo uu qof ama qolo gaar ah maamusho, dabeetana way qiimo beelaysaa, sidaasina waxaa la qiimo beelaysa hantidiisii.

Sidaa dateed, hadii uu weeraryahan weeraro shabakadda, wuxuu si toos ah u dhaawacayaa hantidiisii, waxayna noqonaysaa mid aan lagu kalsoonayn, sidaasina wuxuu noqonayaa qof laba goorbaba khasaaray, waana sababtaas sababta uu Satoshu u yidhi "*Than to Undermine The System And The Validity of His Own Wealth*".

Hadalka Satoshi oo kooban, hadii uu qof awoodo in uu uruuriyo awood badan, waxaa u furan laba doorasho, in uu raaco xeerarka, iyo in uu ku ciyaaro, waana in uu se ogaadaa in raacista xeerarka ay ka faa'ido badan tahay ku ciyaaristeeda, intaas waxaa dheer, hadii uu doorto tallaabada khaldan waxaa burburaysa kalsoonidii dadka, sidaasina waxay hantidiisu noqonaysaa mid qiimo la'aan ah.

7. Reclaiming Disk Space (Badbaadinta Qeyb Ka Mid Ah Kaydka)

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

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.

Qeybtan 7-aad wuxuu Satoshi kaga hadlayaa sidii loo yarayn lahaa qaadka diiwaanka, si uusan u buuxinin kumbiyuutarka, oo qeyb kaydka ka mid ah loo badbaadiyo (Disk Storage Optimization), oo aysan keydku noqon dhibaato weyn oo hortaagan Bitcoin.

Wuxuu hadalkiisa ku bilaabay marka Transaction-ka ugu danbeeya ee lacagta lagu aaso ama la galiyo Block ku filan, Transaction-yadii hore waa la tirtiri karaa, si kaydka kumbiyuutarka loo badbaadiyo.

Block-ga uu Transaction-ku jiro markii ay ka soo wareegto tiro Blocks-yo ah, tusaale ahaan 5 Block oo danbe, oo ay sidaas ku noqoto 6 Confirmations, wuxuu Transaction-kaas noqonayaa mid aad iyo aad ay u adag tahay in lala noqdo ama wax laga bedelo, waxaana Transaction-kaas loogu yeedhaa Transaction la aasay, ama Transaction Buried ah, waayo meel hoose ayuu ku jiraa, waana sababtaas sababta uu Satoshu u yidhi markii Transaction-ka ugu danbeeya ee lacagta lagu aaso tiro Block-yo ku filan, ama "Enough Blocks", waa la tirtiri karaa ama la qarin karaa Transactions-yadii hore, si kaydka kumbiyuutarka qeyb ka mid ah loo badbaadiyo.

Sida aynu hore qeybta 2-aad ee Transaction-ka ku soo nidhi, lacag-diristu ama Transaction-ku waa wareejinta milkiyadda, iyadoo la adeegsanayo saxiixa qofka, sidaa darteedna Bitcoin waa silsilad saxiixyo ah, oo is-daba-taxan oo xidhiidhsan, taasoo muujinaysa sidii loo kala dhaxlay lacagta, laga bilaabo milkiilihii ugu horreeyay ee dhaliyay lacagta, iyo dhowrkii gacmood ee ay soo martay, iyo milkiilaha u danbeeya.

Haddaba markii uu Satoshi leeyahay Transaction-kii ugu danbeeyay ee Coin-ka ama lacagta, micnaheedu ma ahan Transaction-kii u danbeeyay ee shabakadda, ee waa gacantii u danbaysay, ama waa milkiilihii u danbeeyay ee ay lacagtu u soo wareegtay.

TS, inagoo magacyo adeegsanayna, si uu fahamku u soo dhawaado, XAASHI waa Node (ama Miner) ka mid ah shabakadda, wuxuu helay Hash-kii bartilmaameedka ahaa, isagoo shaqeeyay oo bixiyay tamar iyo wakhtiba, sidaasina wuxuu ku abuuray Block, shabakadduna waxay ku abaalmarisay 1 Bitcoin, XAASHI 1-kii Bitcoin gaadhi buu ku iibsaday, isagoo ka iibsaday XIRSI, XIRSI isla 1-kii Bitcoin wuxuu u diray XOOSH, oo waa-hore 1 Bitcoin amaahiyay, ama daymiyay, XOOSH hadana isla 1-kii Bitcoin wuxuu u diray XAREED, oo ahaa saaxiibkii.

Lacagtii uu XAASHI dhaliayay waxay u kala gooshtay dhowr qof ilaa ay ku danbaysay XAREED.

Sidaa darteed hadalka Satoshi ee "*Once The Latest Transaction in a Coin is Buried Under Enough Blocks, The Spent Transactions Before it Can be Discarded to Save Disk Space*", micnaheedu waa marka wareejinta u danbaysa la xaqiijiyo ee XAREED, oo ay ka soo wareegto tiro danbe oo Block-yo, lacag-dirisyadii hore sida XOOSH, XIRSI, iyo XAASHI, waa la tirtiri karaa, si keydka kumbiyuutarka qeyb ka mid ah loo badbaadiyo, maxaa yeelay kuwii hore waa la kharashgareeyay, waxaynuna haynaa wareejintii u danbaysay ee XAREED.

Halkan tirtiridda laga hadlayo ma ahan in lacag-dirista gabi ahaanteed la tirtirayo, ee waa in la soo yaraynayo, oo kaliya laga soo qaadanayo raadka lacag-dirisyadii hore, ujeedkuna waa in qaadka kumbiyuutarka qeyb ka mid ah la bedbaadiyo, maxaa yeelay hadii aynu nidhaahno xogta waa inaynu siday tahay u diiwaan galinaa, waxay culays ku noqonaysaa Nodes-yada aan haysan qalab qaad weyn leh.

Si haddaba tan loo sameeyo, iyadoon lacag-dirista gabi ahaanteed la tirtiraynin, waxaa la adeegsanayaa wax la yidhaahdo "Merkle Tree" (Geedka Merkle).

Merkle Tree: Waa qaab-dhisme xogeed, oo koobaya ama cabburinaya xogo badan ama lacag-dirisyo badan, iyadoo xogihii la Hash-garaynayo, dabeetana la isku gaynayo, ilaa laga helayo hal Hash ama hal summad oo u wada taagan dhammaan xogihii ama lacag-dirisyadii oo idil, Hash-kaasoo loo yaqaan Merkle Root, oo ah xididka Merkle.

Bedelkii la kaydin lahaa dhammaan lacag-dirisyadii ku jiray Block-ga oo isku dhan, waxaa la kaydinayaa sumadihii ama Hash-yadii, sidaasina waxaa lagu badbaadinayaa qeyb ka mid ah qaadka kumbiyuutarka.

Si kale hadii aynu u dhigno, halkii aynu kaydin lahayn 1,000 Transaction, waxaynu kaydinaynaa 1,000 Hash oo u taagan 1,000 Transaction, dabeeto 1,000-kii Hash ayaa hadana la isku celcelinayaa, oo laba-laba la isku Hash garaynayaa, ilaa hal Hash laga helayo, kaasoo loo yaqaan xididka geedka Merkle ama Merkle Root.

Geedka Merkle wuxuu ka kooban yahay:

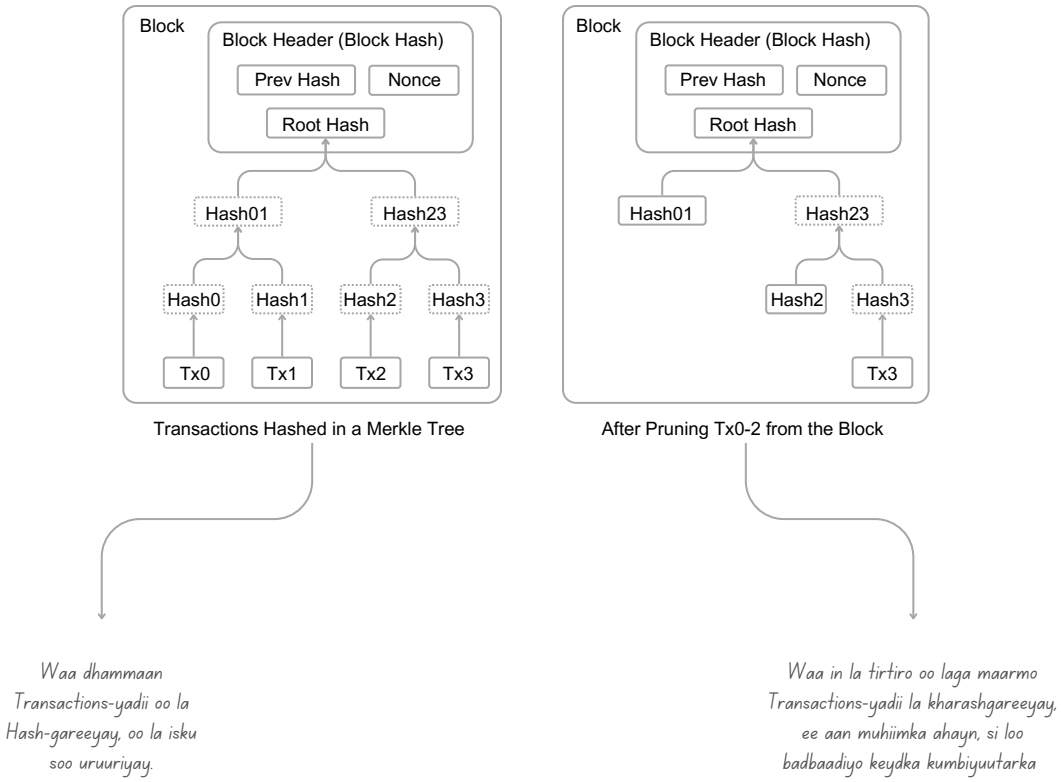
- **Merkle Leaves (Caleemaha Geedka):** oo ah Transaction-yadii oo la Hash-gareeyay
- **Merkle Branch (Laamaha Geedka):** oo ah isku Hash-garaynta Hash-yadii Transactions-yada, kaasoo heerar kala leh
- **Merkle Root (Xididka Geedka):** oo ah Hash-kii kama danbaysta ahaa ee koobsanayay dhammaan Hash-yadii hore

Haddaba Satoshi wuxuu yidhi markii uu Block-gu duugoobo, oo uu Old noqdo, oo sidoo kale lacagtii ku jirtay dhammaanteed la kharash gareeyo, waa laga maarmi karaa in laamihii dhexe la sii kaydiyo, waxaana kaliya lagu kaaftoomi karaa xididka geedka, maxaa yeelay wax dan oo looga sii baahan yahay ma jirto.

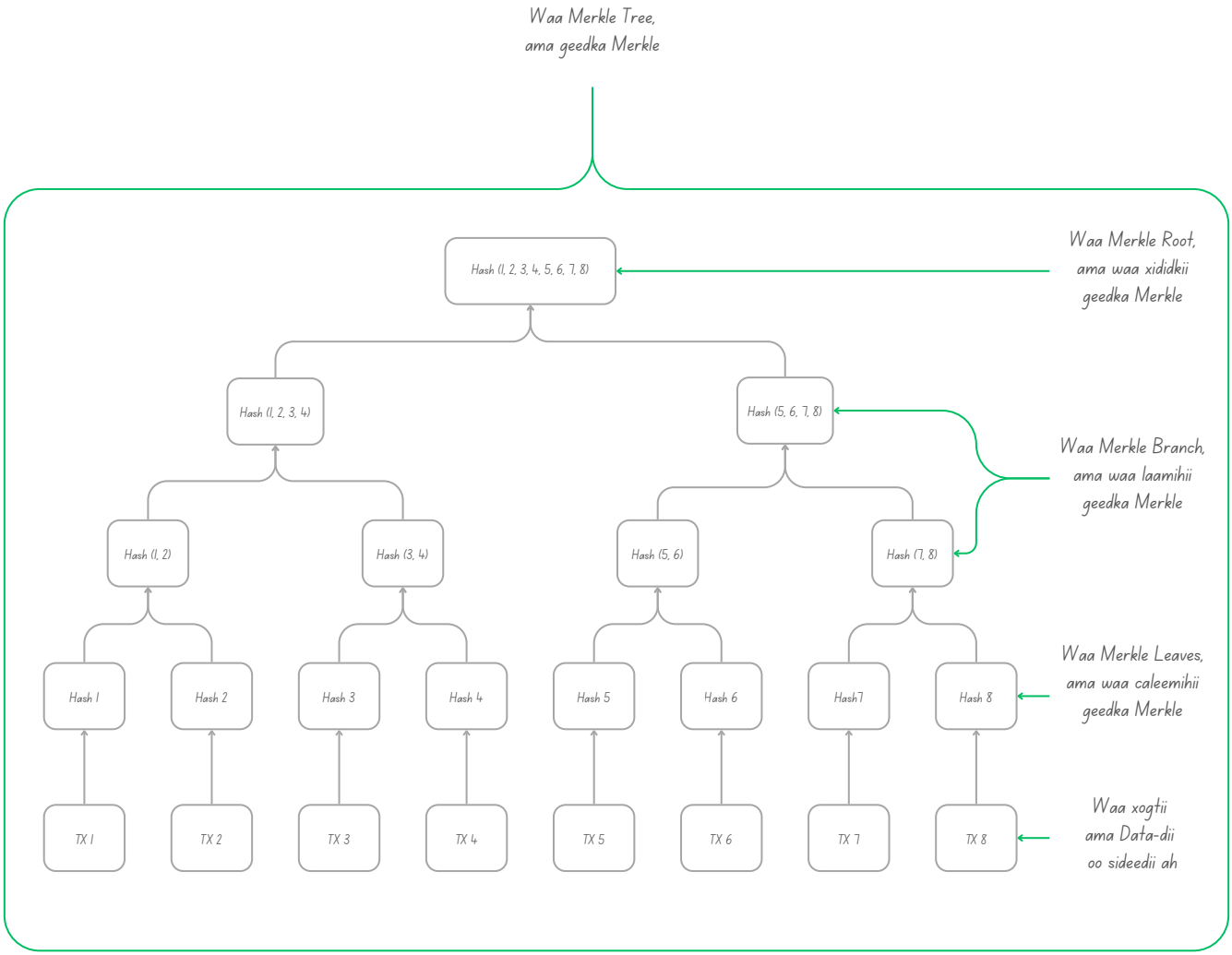
Bedelkii la kaydin lahaa caleemaha geedka, laamaha geedka iyo xididka geedka, waxaa la kaydinayaa oo kaliya xididka geedka, iyo 1 ama 2 laan oo ka mid ah laamaha geedka oo astaan u ah in geedkan wax laga gooyay, caleemaha geedka uma baahna in iyada la kaydiyo.

Halkan aynu mid baraarujinno, waxaa jira dhowr jaad oo Node-yo ah, waxaana ugu waa-weyn labadan:

- **Full Node:** Waa Node si buuxda u hayya diiwaanka Blockchain-ka oo dhan
- **Light Node:** Waa Node fudud, oo aan ku khasbanayn in uu diiwaanka dhan hayyo, isagoo ku kalsoon Full Node-ka, wuxuu kaliya kaydiyaa Merkle Root-ka iyo qaar ka mid ah Hash-yada aan lagama maarmaanka ahayn, waana kan uu Satoshi ka hadlayay, si uu qeyb ka mid ah qaadka kumbiyuutarkiisa u badbaadsado



Aynu si kale u dhigno qaab-samayska geedka Merkle:



Sida halkan ka muuqata, ugu horrayn waxaa si kali-kali ah loo Hash-garaynayaa Transactions-yadii, kadibna laba-labaa la isku Hash-garaynayaa, ilaa ugu danbayntii 1 Hash oo kaliya laga dhigayo, kaasoo u taagan dhammaan Transactions-yadii ku jiray Block-ga, Hash-kaasoo loo yaqaan Merkle Root, soomaali ahaanna ku noqonaysa xididka geedka Merkle.

*A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.*

*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).*

Halkan Satoshi xisaab ahaan ayuu u muujinayaa , wuxuuna yidhi, hadii Block Header-ka ama Madaxa Block-ga, uusan wax Transaction ah xanbaaarsanayn, oo uu madhan yahay, wuxuu ku dhawaad qaadkiisa ama culayskiisu noqonayaa 80 bytes, Block Header-kaasoo ka kooban:

- Previous Hash → (32 Bytes)
- Merkle Root → (32 Bytes)
- Version → (4 Bytes)
- Timestamp → (4 Bytes)
- Nonce → (4 Bytes)
- Difficulty → (4 Bytes)

Haddaba hadii aynu ka soo qaadno in celcelis 10-kii daqiiqaba la curiyo hal Block, markaa iyada ah 1-kii saac waa 6 Block, 24-kii saacna waa 144 Block, 365 maalmoodna oo ah hal sano waa 52,560 Block sanadkii, hadii aynu isku dhufanana waxaa noo soo baxaysa 4.2 Megabytes (MB) sanadkii, taasoo ah wax aad iyo aad u yar.

80 bytes × 6 Blocks saacaddii × 24 saacadood × 365 maalmood = 4.2 Megabytes (MB) sanadkii

4.2 MB sanadkii oo dhan waa qaad ama culays aad iyo aad u yar, markii loo bar bardhigo keydka ama qaadka kumbiyuutarka, sidaa darteed, hadii uu Node-ku kaliya kaydinayo madaxyada Block-ga, oo uusan kaydinaynin dhammaan Transaction-yadii hore, wuxuu si fudud ku badbaadsanayaa qeyb weyn oo ka mid ah qaadka kumbiyuutarkiisa.

Wuxuuna Satoshi sii raaciyay kumbiyuutarada maanta (2008) suuqa yaala, waa kuwo qaadka RAM-koodu, oo ah keyd ama qaad ku-meel-gaar ah yahay 2GB, sidaa darteedna ay ku filan tahay inay si ku-meel-gaar ah u kaydiyaan madaxyada Block-ga (Block Headers), iyadoo la tixgalinayo in ay tignoolajiyaddu sii hormari doonto, oo la soo saari doono kaydad aad u qaad weyn, markii la eego xeerka Moore.

Xeerka Moore ama Moore's Low wuxuu dhigayaa in tirada Transistor-rada ku jira Chip-ka ama Processors-ka kumbiyuutarada laban-laabmaan qiyaastii 18 bilood kasta, taasoo keensanaysa in ay si joogto ah u kordhaan qaadka kombiyuutarrada, waana sababta uu Satoshi xeerkan halkan ugu xusay, si uu u muujiyo in aan laga welwelin kaydinta.

8. Simplified Payment Verification (Fududaynta Xaqiijinta Lacag-bixinada)

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.

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-ka 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.

Qeybtan 8-aad waxay si weyn ula xidhiidhaa qeybtii hore ee 7-aad, wuxuuna Satoshi kaga hadlayaa qaabkii lagu xaqiijin lahaa runimada lacag-dirista, iyadoo aan lagu khasbanayn in diiwaanka ama Blockchain-ka oo dhan la hayyo, isagoo hadalkiisa ku bilaabay, waa suurtagal in la xaqiijiyo lacag-bixinnada iyada oo aan loo baahnayn Node dhamaytiran, ama Full Node, kaasoo ah Node diiwaanka Blockchain-ka oo dhan kaydiya oo hayya, teeda ugu yar iyo teeda ugu weynba.

Halkan xaqiijinta ama hubinta laga hadlayo ma ahan xaqiijinta lacag-diris cusub, ee waa hubinta runimada lacag-diris hore loo xaqiijiyay, ama lacag-diris la sugayay in la xaqiijiyo, oo la rabo in la hubsado in la xaqiijiyay.

Wuxuuna Satoshi yidhi, adeegsadaha caadiga ah, ee adeegsanaya Bitcoin, si uu lacag diris u hubiyo, oo uu u ogaado in la xaqiijiyay iyo in kale, ama in ay jirtaba, kuma khasbana in uu haysta diiwaanka oo dhan, ee kaliya wuxuu u baahan yahay inuu helo nuqul ka mid ah Madaxyada Block-ga (Block Header), oo ah qeyb ka mid ah Block-ga, kaasoo qiyaastii qaadkiisu yahay 80 Bytes, kana kooban: Previous Hash, Version, Merkle Root, Timestamp, Nonce, iyo Difficulty, sidii aynu ku soo marnay qeybta 7-aad. Iyo wuxuu sidoo kale u baahan yahay Merkle Branch, oo ah qeyb ka mid ah laamaha geedka Merkle.

Si haddaba loo helo Block Header-ka iyo Merkle Branch-ka, wuxuu qofku ama user-ku ka dalbanayaa Nodes-yada dhamayskatiran (Full Node), kuwaas oo hayya silsiladda ugu dheer ee tamarta ugu badan lagu bixiyay, taasoo loo aqoonsan yahay inay tahay tan ugu qumman, dabeetana wuxuu sidaas ku helayaa laantii ama Branch-gii xidhiidhinaysay lacagta iyo xididka geedka, sidaasina wuxuu ku xaqiijinayaa runimada Transaction-ka.

Hadii aynu dib u milicsano geedka Merkle, waa:

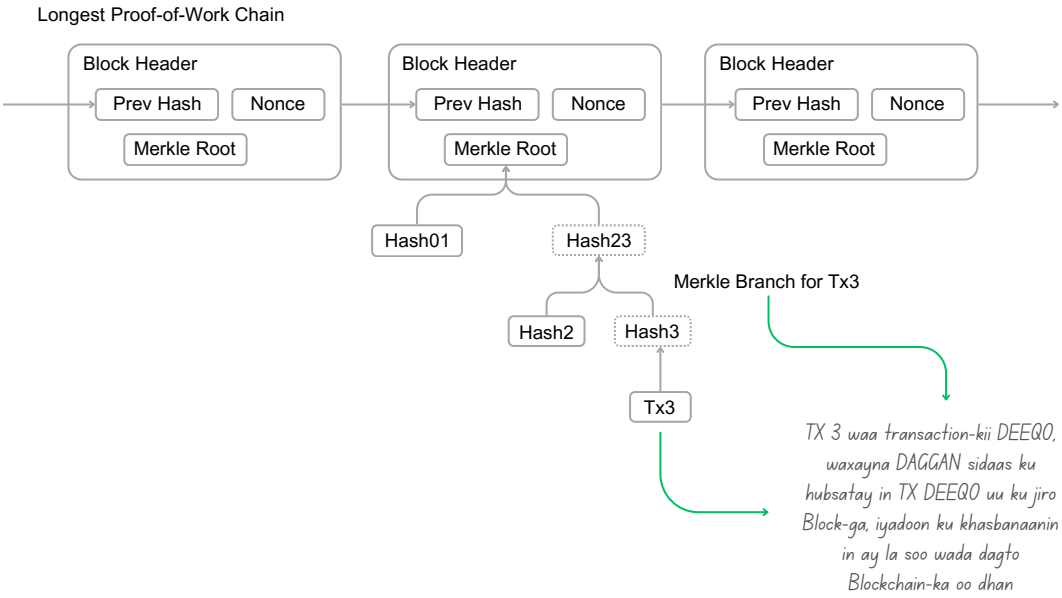
- **Merkle Tree:** Waa geedkii
- **Merkle Root:** Waa xididkii geedka, ahna qeybta ugu sarraysa geedka, ee isku xidhaysay dhammaan qeybihii hoose
- **Merkle Branch:** Waa laamihii geedka, ahna Hash-yadii la sii Hash-garaynayay, oo la isa sii galgalinayay
- **Merkle Leaves:** Waa caleemihii geedka, ahna lacag-dirisyadii ama Transaction-yadii oo la Hash-gareeyay

Hadii aynu si kale u dhigno, si runimada lacag-diris loo hubiyo, waxaa loo baahan yahay 2 waxyaabood, Block Header-kii ay lacag-diristu ku jirtay iyo Merkle Branch-kii ama laantii xidhiidhinaysay lacag-dirista iyo xididka geedka ama Merkle Root, taasoo muujinaysa in ay lacag-diristu ku jirto Block-ga, taasoo noo caddaynaysay runimadeeda.

TS, DEEQO waxay 1 Bitcoin u dirtay DAGGAN, Transaction-kii DEEQO waa la xaqiijiyay, oo waxaa lagu soo daray shabbakadda, hasa ahaatee DAGGAN waxay rabtaa inay hubsato oo ay xaqiijiso in run ahaantii DEEQO 1 Bitcoin u soo dirtay, iyadoon rabin inay soo wada dagsato Blockchain-ka oo dhan, si ay u hubsato. Haddaba waxay Full Nodes-yada ka codsanaysaa nuqul diiwaanka ka mid ah oo fudud oo ka kooban Block Header iyo Merkle Branch-kii isku xidhayay lacag-dirista DEEQO iyo xididka geedka, markii ay aragto in Transaction-ka DEEQO ay ku jirto Block-ga, waxay DAGGAN sidaas ku hubsatay in run ahaantii DEEQO 1 Bitcoin u soo dirtay.

Habkan waxaa la yidhaahdaa "Simplified Payment Verification", oo loo soo gaabiyo SPV, waa in si fudud lagu xaqiijiyo runimada lacag-diris, iyadoon lagu khasbanayn in diiwaanka oo dhan la soo dagsado, si wax loo hubsado, haatanna in si shakhsiyan SPV loo sameeyo looma baahna, si loo hubsado runimada lacag, waxaana maanta shaqadaas si toos ah, oo otomaatig ah u qabta Wallets-yada, sidaa darteed, ma jirto baahi loo qabo in tallaabooyinkaas oo dhan la raaco si loo hubsado Transaction-ka.

Wuxuu kaloo Satoshi raaciyay, adeegsaduhu ama User-ka adeegsanaya Bitcoin, isagu laf ahaantiisa uma hubin karo runimada lacag-dirista, waayo ma haysto diiwaan dhamaystiran, sida diiwanka uu haysto Full Node-ka oo kale, hasa yeeshee wuxuu heli karaa Block Header-kii ay lacag-diristu ku jirtay iyo Merkle Branch-kii isku xidhaysay lacag-dirista iyo Block-ga, sidaasina wuxuu ku ogaanayaa meeshii ay lacag-diristu kaga jirtay silsiladda, silsiladdaasoo ay ka shaqeeyaan Nodes-yada shabakadda, wixii danbe ee Block-yo ah ee ay shabakaddu soo saari doontana waxay sii xojindoonaan runimadii lacag-dirista.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network.

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.

Halkan Satoshi wuxuu leeyahay habkan SPV-ga ah wuxuu ku tiirsan yahay aqlabiyadda shabakadda, hadii aqlabiydda shabkaddu yihiin ama ay gacanta ku hayyaan Nodes-yo daacad ah, oo aan been-abuur iyo taag-taag ka shaqaynaynin, habka SPV-ga ah waa la isku hallayn karaa, waana lagu tiirsanaan karaa, hadii se awoodda shabakada inteeda badan ay u gacan-gasho Nodes-yo aan daacad ahayn, habka SPV-ga la iskuma hallayn karo, waayo waxay u nugul yihiin wax ka bedel iyo been-abuur, waxaana la abuuri karaa silsilad dheer oo been-abuur ah, User-kuna ama adeegsadaha caadiga ahna ma hubin karo, waayo ma hayysto diiwaanka oo dhamaystiran.

Full Nodes-yadu iyaga way awoodaan inay kala saaraan runta iyo beenta, wayna hubin karaan lacag-dirisyada runta ah iyo tan beenta ahba, maadaama ay hayyaan diiwaanka oo dhamaystiran, hasa yeeshee kuwa aan haynin diiwaanka oo dhammaystiran, ee adeegsanaya habka fudud ee SPV, waxay u nugul yihiin khiyaamo, waxaana si fudud loo tusi karaa silsilad been-abuur ah oo ka dheer tan daacadda ah, waxayna sidaas ugu malayn karaan inay tahay silsilad qumman, sidaasina waxaa lagu khiyaami karaa adeegsadayaasha adeegsanaya habkan ah SPV-ga.

Waana khatar sii jiri doonta ilaa iyo inta uu weeraryahanku ama Nodes-yada aan daacaddda ahayni gacanta ku hayyaan awoodda shabakadda inteeda badan.

One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

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.

Si loo yareeyo halista soo food-saari karta qofka adeegsanaya habkan SPV-ga, ee aan awoodin in uu la soo dago diiwaanka oo dhammaystiran, Satoshi wuxuu soo jeediyay hab ama qaab ama istaraatiijiyad difaac.

Wuxuuna Satoshi yidhi, waa in Software-ka ama qalabka adeegsanaya SPV-ga uu helo digniino (Alert), markii ay Nodes-yada daacadda ahi la kulmaan waxyaabo khaldan, sida Block khaldan oo silsiladda lagu soo daray oo kale, oo ay dabeetana si degdeg ah ula soo dagaan qeybtii ama Block-yadii laga shakisnaa, si ay u hubiyaan, oo ay u xaqiijiyaan wixii khaldanaa ee jiray.

Istaraatiijiyaddan waxay adeegsadayaasha SPV-ga u ogolaanaysaa inay durbadiiba ka war helaan digniinada ay soo gudbiyaan Nodes-yada daacadda ah, ee ka dhanka ah amniga shabakadda.

Dhanka kale, Satoshi wuxuu fariin u dirayaa ganacsatada sida joogtada ah u helaya lacag-bixino, ee Bitcoin u adeegsada sidii lacag-helid oo kale, isagoo leh, hadii aad tihiin ganacsato, isla mar ahaantaana aad si joogto ah u heshiin lacag, waxaad u baahan tihiin, ama kama maarmayso in aad Full Node idiin gaar ah samaysatiin, halkii aad kaliya ku tiirsanaan lahaydeen SPV, si aad u heshaan amni dheeraad ah, madax-bannaanni buuxda, iyo niyad-sami joogto ah, maxaa yeelay markan cid danbe uma daba fadhidid, halka SPV-gu daba fadhiyo Full Node-ka.

9. Combining and Splitting Value (Isku-darka Iyo Kala Reebidda Lacagta)

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.

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).

Qeybtan 9-aad, wuxuu Satoshi kaga hadlayaa sida loo maareeyo lacagaha markii la rabo in la diro, haday noqon lahayd in la isku qaado oo la isku geeyo (Combine), ama in qeyb-qeyb loo diro (Split), isagoo hadalkiisa ku bilaabay, waa suuragal in lacag kasta siday ahayd loo maareeyo (centi by centi), hase ahaatee waxay taasi soo kordhin lahayd dhib iyo culays weyn, gaar ahaan hadii la doonayo in qaddar yar la diro.

Sababtaas awgeedna, waxaynu u baahannahay hannaan awood u leh in uu lacagta isku qaado markii la rabo, sidoo kalena kala qeyb-qeybiya markii la rabo, iyadoo la adeegsanayo Input iyo Output.

- **Input:** Waa galitaan, waana tilmaanta sheegaysa halka ay lacagtu ka timid
- **Output:** Waa bixitaan, waana tilmaan sheegaysa halka ay lacagtu ku soccoto, ama loo dirayo

Bitcoin ma ahan sidii koonto bangi oo kale, ama Account Balance-yada caadiga ah oo kale, bedelkii aad ka haysan lahayd hal koonto oo ay lacagtaadu kugu jirto, waxaad haysataa dhowr koontooyino kala duwan, kuwaasoo loo yaqaan "UTXO", oo laga soo gaabiyay "Unspent Transaction Output".

UTXO: Waa lacagaha aan wali la kharashgarayn, ee Unspent-ga ah, ee diyaarka u ah in mustaqbalka danbe la kharashgareeyo, si kooban waa lacagta kugu jirta Wallet-kaaga, ee aan ilaa haaatan la kharashgarayn.

TS, hadii ay Wallet-kaagu ku jiraan 2 Bitcoin, oo aad ku heshay siyaabo kala duwan, sida:

- 0.1 BTC ka heshay HOODO
- 0.4 BTC ka heshay HANI
- 0.2 BTC ka heshay HABBOON
- 0.2 BTC ka heshay HIBAAQ
- 1.1 BTC ka heshay HINDA

Waxaad haysataa 5 UTXO oo aan wali la kharashgarayn, oo isku geyntoodu tahay 2 Bitcoin, mid walibana waxay u taagan tahay lacag gaar ah, oo gooni ah.

Haddaba hadii aad rabto inaad dirto 0.5 BTC, Bitcoin ma odhanayso qofkan diraha (Sender) ah, noo eega hadhaagiisa, oo dabeetana hadii ay ku jirto ka jara hadhaagiisa 2 BTC - 0.5 BTC, oo ka dhiga 1.5 BTC, sidii bangiyada oo kale.

Taa bedelkeeda, waxay Bitcoin isku qaadaysaa oo ay isku gaynaysaa laba ka mid ah UTXO-yadaada, sida 0.1 BTC ee HOODO + 0.4 BTC ee HANI, waxayna u adeegsanaysaa Input ahaan, halka uu Output-ku yahay 0.5 BTC.

Inaad 1 Bitcoin haysataa micnaheedu ma ahan in ay hal meel ka wada yimaadeen, waxay noqon karaan 20 UTXO, ama 50 amaba ka badan, sidaa si la mid ahna waxay noqon karaan hal 1 UTXO.

Lacag-diris kasta ama Transaction kasta ugu yaraan wuxuu leeyahay hal Input iyo hal Output (marar badanna dhowr Input), markii aad rabto inaad lacag dirto, Bitcoin waxay Input ahaan u adeegsanaysaa UTXO-yadaada.

TS kale, IDIL waxay haysataa 4 UTXO, oo kala ah 0.2 BTC + 0.4 BTC + 0.3 BTC + 0.2 BTC = 1.1 BTC, waxayna rabtaa inay 1 Bitcoin u dirto ILWAAD.

Haddaba Transaction-kii IDIL wuxuu ka kooban yahay:

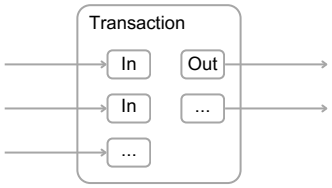
Inputs:
- 0.2 BTC
- 0.4 BTC
- 0.3 BTC
- 0.2 BTC = (Wadarta: 1.1 BTC)

Outputs:
- 1.0 BTC → ILWAAD
- 0.1 BTC → Baaqigii ama hadhaagii IDIL, oo dib loogu soo celinayo (oo dib u noqonaysa UTXO cusub)

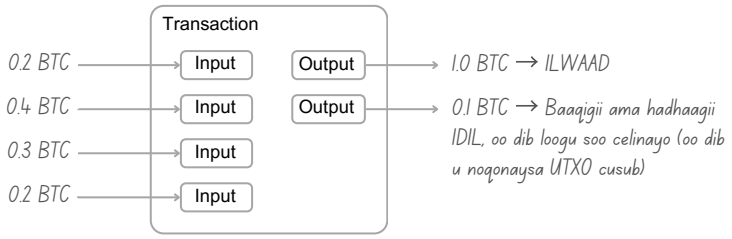
Wuxuu kaloo Satoshi yidhi, haddii aad leedahay hal UTXO oo weyn oo ku filan lacagta aad rabto inaad dirto, waxaad adeegsan doontaa halkaa Input oo kaliya, sida in aad leedahay hal UTXO, oo ah 1 BTC, oo aad rabto inaad dirto 0.6 BTC, waxaad adeegsanaysaa halkaa Input oo kaliya, oo ka kooban hal UTXO oo ah 1 BTC.

Hadiise aanad haysan hal UTXO oo weyn oo dabooli kara lacagta aad rabto inaad dirto, markaa iyada ah waxaad adeegsan doontaa dhowr Input, oo ka kooban dhowr UTXO yar-yar, oo la isku geeyay, si aad u gaarto wadarta aad rabto inaad dirto, sidii aynu tusaalaha hore ku soo aragnay.

Dhanka kale, wuxuu Satoshi yidhi, badanaa lacag-dirisyadu waxay yeelan doonaan 2 Output, oo kala ah Output ku socda qofkii lacagta loo dirayay, iyo Output lacag-celin ah, oo dib ugu soo noqonaysaa dirihii, ama qofkii lacagta dirayay, waa se hadii ay jirto lacag baaqi ah.



Aynu tusaalaheenii danbe ee IDIL ku dhaqan-galinno:



> *It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.*
>
> *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.*

Halkan Satoshi wuxuu leeyahay, waa in la ogaadaa markii lacagta la rabo in la diro ay ku xidhan tahay ama ay leedahay Inputs-yo badan, kuwaasoo iyaguna leh Inputso-yo kale, kuwaas oo iyaguna sidoo kale laga yaabo inay leeyihiin Inputs-yo kale… aysan wax dhibaato ah lahayn, sidoo kalena aan loo baahnayn tixraac dhammaystiran.

Xaaladan waxaa loo yaqaanaa "Fan-out", waana markii uu unug ku xidhiidhsan yahay unug kale, unugaasoo unugo kale oo badan ku sii xidhiidhsan, kuwaasoo iyaguna kuwo kale ku sii xidhiidhsan.

TS, Trsancation B wuxuu leeyahay Input ka timid Transaction W, X, T, K, D, iyo F, sidaa darteedna Transaction-ka B wuxuu la xidhiidhsan yahay Transactions-ka kala ah W, X, T, K, D, iyo F.

Markaa Satoshi wuxuu leeyahay looma baahna, oo laguma khasbana in la helo diiwaan dhamaystiran, si loo sameeyo daba-gal, oo loo ogaado ciddii hore u haysatay lacagta, iyo ciddii ka horraysay, iyo ciddii ka sii horraysayba, si loo xaqiijiyo runimadeeda.

Waayo UTXO ayaa muujinaya in ay lacagtaas aan wali hore loo adeegsan, UTXO-guna wuxuu u taagan yahay "Unspent Transaction Output", lacago aan wali la kharash garayn.

10. Privacy (Qarsoodida)

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

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.

Qeybtan 10-aad, wuxuu Satoshi kaga hadlayaa qarsoonaanta, ama dadnaanta. Sidii loo noqon lahaa summadlaawayaal, loona ilaalin lahaa qarsoonida adeegsadayaasha Bitcoin.

Satoshi wuxuu qirsan yahay in ay bangiyadu leeyihiin heer ama xaddi go'an oo qarsoodi ah, hasa yeeshee aan ahayn qarsoonaan 100% ah, waayo bangigu waa dhexeeye, wuxuu u dhaxeeyaa 2 dhinac, wuxuuna hayyaa dhammaan xogtooda, haday noqon lahayd cidda wax diraysa, cidda u diraysa, qaddarka la dirayo, goorta la dirayo, iwm, hasa yeeshee si shaacsan looma baahiyo xogtaas, waxaa kaliya og 2-da dhinac iyo bangiga, oo dhaxeeye ah, waana sabata uu Satoshi u lahaa bangiyadu waxay leeyihiin heer qarsoodi ah.

Bitcoin la mid ma ahan bangiyada. Ma jirto cid dhexe oo lagu kalsoon yahay, oo xogta diiwaan galisa, misna ilaalisa. Taas bedelkeeda xogtu waa mid shaacsan oo furan, oo ay cid kasta arki karto wixii la is-dhaafsaday.

Hasa yeeshee, taasi waxay ka hor-imanaysaa qarsoonaanta ama Privacy-ga. Hadiiba ay suuragal tahay in la arki karo wax kasta, maxay tahay qarsoodida hadhay?. Sidaa darteed, buu Satoshi u yidhi, qaabkii bangiyada halkan suuragal kama aha, waayo Bitcoin waa mid daah-furan, oo dhammaan lacag-dirisyada iyo is-dhaafsiyada ka dhigaysa mid shaacsan oo baahsan, si loo xaqiijiyo.

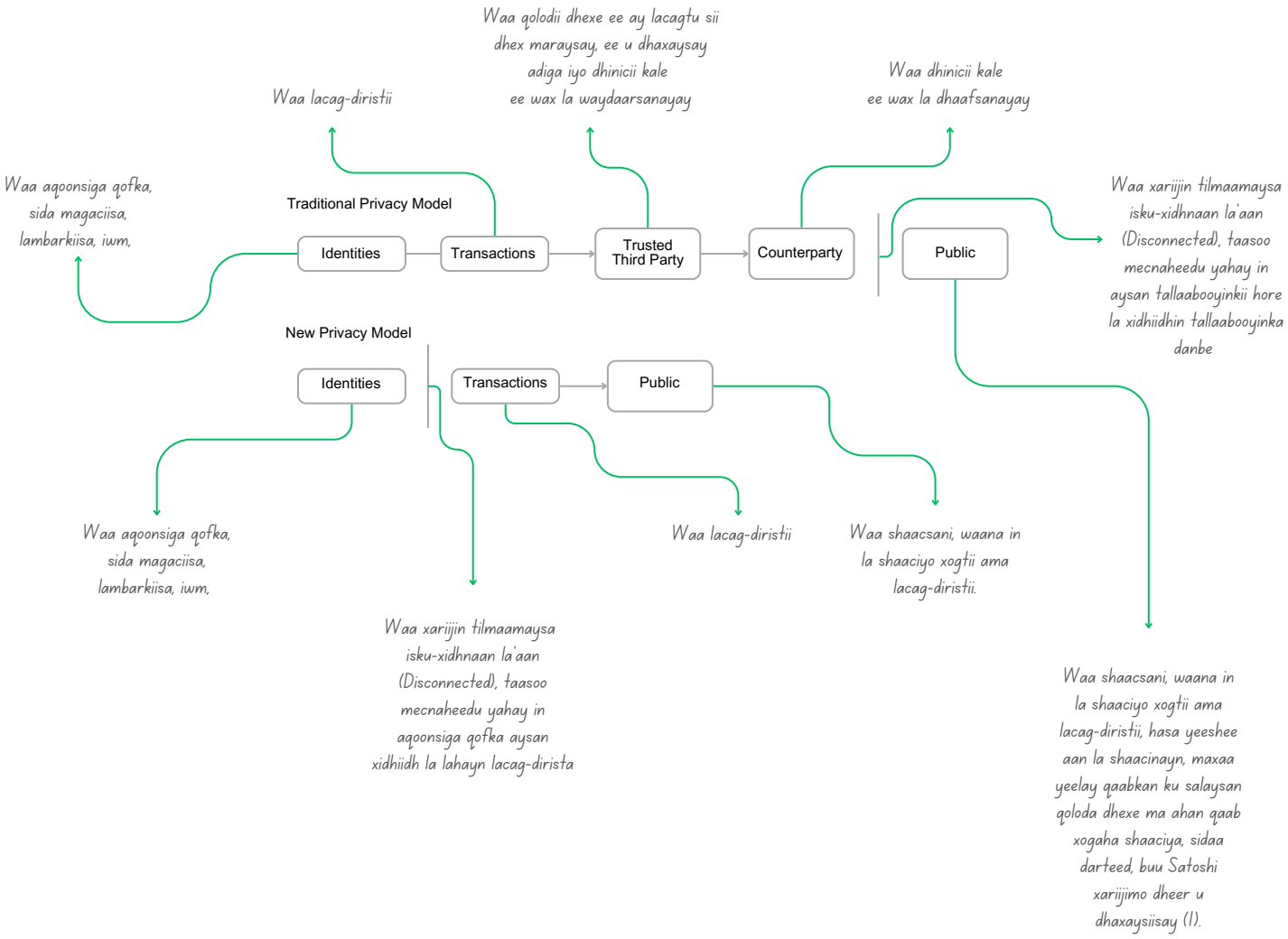
Haddaba waa maxay xalku?

Xalka Satoshi baa soo jeediyay, wuxuuna yidhi waa suuragal in la helo Privacy ama qarsoonaanta, iyadoo la jarayo xidhiidhkii u dhaxeeyay lacagta iyo qofkii diray.

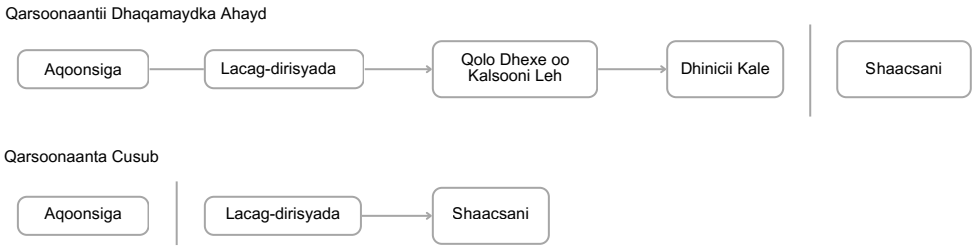
Halkan wuxuu leeyahay Satoshi, in kastoo aan xogta si 100% loo qarin karin, sida wakhtiga ay dhacday, qaddarka la diray, cinwaanka diray iyo kan loo dirayba, hadana waxaa la qarin karaa aqoonsigii diraha iyo loo-diraha, iyadoo furayaasha guud ama Public Keys-ka laga dhigayo kuwo summad ama magac laawayaal ah.

Dadkuna kaliya waxay arkayaan cinwaan wax diray, iyo cinwaan wax loo diray, hasa yeeshee lama garan doono oo lama aqoonsan doono qofka leh cinwaanka, sidaasina waxaa la jabiyay xidhiidhkii u dhaxeeyay lacagtii la diray, iyo aqoonsiga qofkii diray.

Wuxuuna Satoshi la meel dhigay, oo uu barbardhigay, sida ay suuqyada saamiyaduhu u shaqeeyaan, isagoo yidhi, suuqyada saamiyaduhu waxay kaliya shaaciyaan qaddarkii ama tiradii saami ee la kala iibsaday iyo wakhtigii la kala iibsaday, iyo qiimihii lagu kala iibsaday, iyagoon shaacin cidda ama aqoonsiga qofka iibsaday, sida magaciisa ama lambarkiisa, iwm.



Aynu soomaaliyeeno:



> *As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.*
>
> *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.*

Halkan wuxuu Satoshi kaga hadlayaa sidii kor loogu qaadi lahaa heerka qarsoonaanta, isagoo talo soo-jeedin ku bilaabay, oo yidhi, si amni sare oo dheeraad ah loo helo waa in si joogto ah loo bed-bedelaa furayaasha, Transaction kastana loo adeegsadaa furayaal cusub, si aan loo helin wax raad ah haba yaraatee oo tilmaamaya ama isku xidhaya aqoonsiga qofka iyo cinwaanka.

Wuxuuna sii raaciyay, aqoonsiga waxyaabaha qaar waa lama huraan, waana wax aan laga baaqsan karin, sida Transaction-kii lahaa dhowr Input, taasoo si aan ku talagal ahayn lagu ogaanayo in uu hal qof lahaa, maadaama uu ku yaalo hal saxiix, iyadoon wali la ogaan aqoonsigiisa dhabta ah.

Waxayna khatartu imanaysaa markii mid ka mid ah cinwaanadiisa la ogaado, oo la aqoonsado milkiilihii lahaa, sidaasina waxaa si fudud lagu ogaanayaa dhammaan cinwaanadii iyo Transactions-yadii la xidhiidhay.

11. Calculations (Xisaabinta)

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

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.

Qeybtan 11-aad, sidoo kale waa qeyb muhiimadeeda leh, wuxuu Satoshi si xisaabaysan kaga hadlayaa suurtagalnimada lagu soo weerari karo Bitcoin, iyo kanshada ama fursada ama jaaniska uu haysto qofka raba inuu isku dayo inuu shabakadda weeraro, isla mar ahaantaana lagu abuuro silsilad ama Chain ka dheer tan daacadda ah (Honest Chain).

Wuxuuna Satoshi xisaab ahaan u muujinayaa sida ay Bitcoin u adag tahay in la soo weeraro, iyo sida ay is kaga caabinayso is-bedel kasta oo aan qorshaysnayn.

Wuxuuna hadalkiisa ku bilaabay, xittaa hadii uu weeraryahanku ku guulaysto inuu shabakadda weeraro, oo uu dabeetana soo saaro silsilad ka dheer tan daacadda ah, taasi micnaheedu kama dhigno inuu wax kasta samayn karo, sida in lacag cusub meel aan jrin laga abuuro oo kale, ama lacago ay dad leeyihiin in loo dhaco, oo la qaato oo kale, waayo Nodes-yadu marnaba ma aqbali doonaan waxyaabo sidan oo kale ah, mana ansixin doonaan Block ay ku jiraan waxyaabo sidan u khaldan oo kale.

Weeraryahanku wuxuu kaliya isku dayi karaa inuu wax ka bedelo mid ama dhowr ka mid ah Transactions-yadii hore ee uu dhawaan kharashgareeyay, si uu dib ula soo laabto, oo uu u sameeyo Double Spending.

Halkan Satoshu wuxuu tilmaamayaa in si kasta uu weeraryahanku ku awoodo inuu gacanta ku dhigo awoodda shabakadda inteeda badan, waana waxa maanta loo yaqaan "51% Attack", wali wuu xaddidan yahay, mana awoodi doono waxyaabo badan.

Halista ugu weyn ee uu weeraryahanku gaysan karo waa in uu isku dayo in uu dib u soo ceshto lacagihii uu dhawaan kharashgareeyay, hasa yeeshee ma awoodo in lacag aan jirin abuuro, ama uu lacagaha dadka qaato.

Waayo lacagtu waxay u baahan tahay saxiiix, saxiixa qofkana lama heli karo Private Key la'aan, sidaa darteedna lama qaadan karo, oo lama xadi karo lacagaha dadka.

Waana kaliya lacagaha uu dhawaan kharash gareeyay, ma ahan lacagihii todobaadyo, bilo ama sanado ka hor uu kharashgareeyay, iyo xitaa kuwii uu maalmo ka hor kharashgareeyay, waayo si uu wax u bedelo wuxuu ku khasban yahay inuu bedelo dhammaan wixii ka danbeeyay oo dhan, sidaa darteed, hadii ay lacag-diristu ka soo wareegtay tiro Blocks-yo badan, ma la awoodi doono in wax laga bedelo, waayo kanshada ama fursadda wax lagu bedelayo waa mid aad iyo aad u hoosaysa, waana sababta loo yidhaahdo ha la sugo 6 Confirmations, taas oo micnaheedo yahay, Block-ga ay lacag-diristu ku jirto in ay ka soo wareegto 5 Block oo danbe, oo ay sidaas iskula noqdaan 6 Block, si ay u korodho heerka adkida wax ka bedelka, taasoo loo yaqaan "Block Finality".

> *The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.*
>
> *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.*

Halkan wuxuu Satoshi sheegayaa in hadii uu qof rabo in uu wax bedelo, uu ku khasban yahay in uu soo saaro silsilad ka dheer tan daacadda ah, oo uu dabeetana kula tartamo Nodes-yada daacadda ah, wuxuuna Satoshi doonayaa in uu xisaab ahaan (Probabilistic) u cabbiro suurtogalnimada uu weeraryahanku ku guuleysan karo tartanka.

Wuxuuna hadalkiisa ku bilaabay, tartanka u dhaxeeya silsiladda daacadda ah iyo tan uu weeraryahanku abuuray waxaa lagu tilmaami karaa sidii socod laba-geesood ah, ama "Binomial Random Walk".

Binomial: Waa erey xisaabeed (Maths), waana xaalad leh laba natiijo midkood, guul ama guuldarro, sidii shlinkii cirka loo tuurayay oo kale, ugu danbayntii laba dhinac mid kood uunbuu u dhacayaa, taasoo ka kala dhigan guul iyo guuldarrao.

Marka uu Satoshi leeyahay "Binomial Random Walk", wuxuu ula jeedaa socod iska nasiiib ah (Randomly), oo laba-geesood ah. Tani micnaheedu waa in ay tallaabo kasta ay leedahay suurtogalnimo go'an. Cidda ama qofka tallaabada hor leh qaada ayaa mar kasta ah hogaanka tartanka.

Wuxuuna Satoshi yidhi, guuushu waxay timaadaa ama tahay marka ay silsiladda daacadda ah tallaabada hor qaado, oo ay hor hesho Block cusub, ka hor silsiladda weeraryahanka, taasoo tartanka ku hogaaminaysa +1.

Dhanka kale, guuldarradu waxay timaadaa ama tahay markii ay silsiladda weeraryahanku hor qaado tallaabada, oo ay hor hesho Block cusub, ka hor tan daacadda ah, taasoo abuuraysa gaabis dhan -1.

"**-1**", micnaheedu waa in silsiladda daacadda ah 1 Block ka danbayso tartanka, TS:

- **+1:** macnaheedu waa in silsiladda "**Daacadda**" ah hogaanka hayso
- **0:** macnaheedu waa in ay labada silsiladoodba barbaro yihiin
- **-1:** macnaheedu waa in silsiladda "**Weeraryahanka**" ah hogaanka hayyo, taasoo hadaynu si kale u dhigno ka dhigan in silsiladda daacdda ah shabakadda ka danbayso 1 Block.

TS, kale:

- Wareega 1-aad
  - Honest Chain (Silisiladda Daacadda ah): 10 Block
  - Attacker Chain (Silsiladda Weeraryahanka): 10 Block
  - Tartanku waa 0

- Wareega 2-aad
  - Honest Chain: 11 Block (Silsiladda daacada ah ayaa hogaaminaysa tartanka)
  - Attacker Chain: 10 Block
  - Tartanku waa +1

- Wareega 3-aaad
  - Honest Chain: 12 Block (Wali silsiladda daacada ah ayaa hogaaminaysa)
  - Attacker Chain: 10 Block
  - Tartanku waa +2

- Wareega 4-aad
  - Honest Chain: 12 Block
  - Attacker Chain: 11 Block (Markan silsiladda weeraryahanka ayaa hor heshay Block-ga)
  - Tartanku waa +1

- Wareega 5-aad
  - Honest Chain: 12 Block
  - Attacker Chain: 12 Block (Hadana markan silsiladda weeraryahanka ayaa hor heshay Block-ga, taasoo tartanka ka dhigtay barbaro)
  - Tartanku waa 0

- Wareega 6-aad
  - Honest Chain: 12 Block
  - Attacker Chain: 13 Block (Markan silsiladda weeraryahanka ayaa hogaaminaysa tartanka)
  - Tartanku waa -1

- Wareega 7-aad
  - Honest Chain: 12 Block
  - Attacker Chain: 14 Block (Hadana mar kale ayay silsiladda weeraryahanka hogaaminaysaa tartanka)
  - Tartanku waa -2

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

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

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

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

Halkan Satoshi wuxuu xisaab ahaan u muujinayaa kanshada uu haysto weeraryahanku, si uu u soo gaaro silsiladda daacadda ah, isagoo ku tilmaamay xaalad la mid ah "Gambler's Ruin".

Wuxuuna yidhi suurtagalnimada ama kanshada uu haysto weeraryahanku, si uu u soo gaaro, ama uu ula qabsado silsiladda daacadda ah, ama uu u yimaado barbardhaca, waxay la mid tahay, sidii adigoo khamaar ciyaaraya oo kale, oo haysta lacag iyo isku day aan dhamaad lahayn, oo ku jira khasaare xoogan, hasa yeeshee ku rajjo weyn inuu guulaysto, oo dib uga soo kabsado khasaaraha, xaaladaasoo loo yaqaan "Gambler's Ruin".

Waana aragti ama male aan inta badan dhicin, waayo badanka markii uu qof khasaare ku jiro, wuu joojiyaa khamaarka, ee ma sii wado, mararka qaar waa suuragal in la isku dayo in khasaaraha laga soo kabsado, hasa yeeshee waa wax aan inta badan dhicin.

Tusaalaha Satoshi oo kooban, Hadii aad haysato lacag aan dhamaad lahayn, sidoo kalena aad haysato isku day aan dhamaad lahayn, in intee le’eg bay kugu qaadan lahayd inaad barbardhicii ama meeshii ay lacagtaadu ku ekeed gaadho, hadii aad khasaaro ku jirto?

Si haddaba loo helo suurtagalnimadii ama Probability-gii uu weeraryahanku ku gaadhi karo silsiladda daacadda ah waxaa lagu helaa iyadoo la raacayo xeerarkan:

- **p =** waxay u taagan tahay kanshada ama suurtagalnimada uu Node-ka daacadda ahi u leeyahay in uu hor helo Block-ka xiga (ama hadaynu si kale u dhigno, waa awoodda ama Hash Power-ka ay leeyihiin Nodes-yada daacadda ah)
- **q =** waxay u taagan tahay kanshada ama suurtagalnimada uu weeraryahanku u leeyahay in uu hor helo Block-ka xiga (ama hadaynu si kale u dhigno, waa awoodda ama Hash Power-ka ay leeyihiin weeraryahannada)
- **q^z =** waxay u taagan tahay kanshada ama suurtagalnimada uu weeraryahanku ku gaadhi karo ama uu ku dhaafi karo silsiladda daacadda ah
- **z =** waxay u taagan tahay tirada Block-yada uu weeraryahanku ka danbeeyo silsiladda daacadda ah

Haddii uu weeraryahanku leeyahay awood xisaabeed oo ka badan ama le'eg tan kuwa daacadda ah ay leeyihiin, sida **50%** wixii ka sarreeya, markaa iyada ah **q** oo u taagan weeraryahanka waxay la mid tahay ama ka badan tahay **p** oo u taagan Nodes-yada daacadda ah (**$q \geq p$**), sidaa darteedna **q^z** oo ah suurtagalnimada uu weeraryahanku ku soo gaadhi karo ama uu ku dhaafi karo silsiladda daacadda ah waxay la mid tahay **= 1** (**$q^z = 1$**), taasoo ka dhigan inay tahay **100%**. Waxaana jirta halis uu weeraryahanku ku fulin karo waxyaabo sharci darro ah.

Hadii se uu weeraryahanku leeyahay awood xisaabeed oo ka yar kuwa daacadda ah, sida **50%** wixii ka hooseeya, markaa iyada ah **q** waxay ka yar tahay **p** (**$q < p$**), waxaana loo baahan yahy in la go'aamiyo awooddiisa, iyo tirada **z** ama tirada Blocks-yada ee uu ka danbeeyo.

TS, hadii uu weeraryahanku leeyahay awood **30%** ah, tirada **z**, oo ah tirada Blocks-yada ee uu ka danbeeyo silsiladda daacadda ah ay tahay **3**, markaa iyada ah **q** oo u taagan weeraryahanka waxay la mid tahay **0.3**, maadaama uu haysto awood dhan **30%**, halka **p** oo u taagan Nodes-yada daacadda ah ay la mid tahay **0.7**, oo ah **70%-ka** kale ee soo hadhay **(q=0.3/p=0.7)^z**, waxaynuna intaa ku jibbaaraynaa **3** oo ah **z** Block **(q=0.3/p=0.7)^3**, sidaa darteedna **q^z** oo ah suurtagalnimada uu weeraryahanku ku soo gaadhi karo ama uu ku dhaafi karo silsiladda daacadda ah waxay la mid tahay **= 0.078 ($q^z = 0.078$)**, taasoo ka dhigan inay tahay **7.8%**.

Hadii aynu si kale u dhigno, inagoo raacayna xeerkan "**$q^z = (q/p)^z$**":

- **q** = 0.3 (30%) awoodda uu weeraryahanku leeyahay
- **p** = 0.7 (70%) awooda ay leeyihiin Nodes-yada daacadda ah
- **z** = 3 tirada uu weeraryahanku ka danbeeyo silsiladda daacadda ah
- **q^z** = 0.078 = 7.8%

Tani waxay ka dhigan tahay hadii weerayahan haysta awood dhan **30%**, isla mar ahaantaana uu silsiladda daacadda ah ka danbeeyo **3** Block ay suurtagalnimadiisu ama kanshadiisu tahay **7.8%**.

Hadii se uu ka danbeeyo **6** Block, (**z = 6**), sidoo kale ay awoodiisu tahay **30%**, suurtagalnimadiisu waa mid aad iyo aad u hoosaysa, waana ku dhawaad **($q^z = 0.0055$)**, taasoo ka dhigan inay tahay **0.55%**, waana sababta uu Satoshi u lahaa, Block kasto oo cusub oo soo biira, wuxuu adkeenayaa wax ka bedelka Block-yadii hore.

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

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.

Halkan Satoshi wuxuu yidhi, hadii Nodes-yada daacadda ah (**p**) ay ka awood badan yihiin kuwa weeraryahanada ah (**p > q**), kanshada uu weeraryahanku ku gaari karo silsiladda daacadda ah, si uu "Double Spending" u sameeyo, waxay isku dhimaysaa si aad u dhakhso badan oo xawli ah (Exponentially), mar kasta oo ay tiro cusub oo Block-yo ah silsiladda ku soo biiraan, Tusaale, hadii uu weeraryahanku ka danbeeyo 3 block = ~7.8%, 6 block = ~0.55%, 10 block = ~0.016% iwm, isagoo waliba haysta awood dhan **30%**. Wakhti xaadirkan aad iyo aad iyo aad bay u adag tahay in la helo awood intaa le'eg.

Hadii uu weeraryahanku nasiib u yeelan waayo inuu goor hore bilaabo, kanshadiisu waxay marba marka ka danbaysa si aan la malaysan karin isku dhimaysaa, mar kastuu sii danbeeyo.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

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.

Halkan wuxuu Satoshi kaga hadlayaa sidii kor loogu qaadi lahaa kalsoonida lagu qabo lacag-dirisyada la helayo, isla mar ahaantaana loo yarayn lahaa halista ku aadan lacag la diray in dib loola noqdo, isagoo hadalkiisa ku bilaabay waa maxay muddada ay tahay in la sugo, si si buuxdo loogu kalsoonaado lacagta, si aan dib loola noqon.

Wuxuuna yidhi, aynu ka soo qaadno in qofka lacagta diraya uu yahay weeraryahan, isla mar ahaantaana uu awooday in uu gacanta ku dhigo awoodda shabakadda inteeda badan, wuxuuna rabaa lacag uu dhawaan diray in uu la noqdo, mar allaale markii uu silsilad been-abuur ah, oo ka dheer tan daacadda ah dhiso, waxaa durbadiiba la ogaysiinayaa loo-dirihii ama qofkii lacagta loo dirayay, isagoo ogaanaya in lacagtii laga saaray silsiladdii.

Wuxuuna Satoshi yidhi "*But the Sender Hopes it Will be Too Late*", diruhu ama qofka lacagta diraya wuxuu jeclaan lahaa in goor danbe la ogaado, kadib markii uu badeecadii helo, ama adeegii, oo uusan loo-diruhu waxba ka qaban karin.

Sababtan awgeedna, wuxuu Satoshi soo jeedinayaa, in markii lacagta la helo kadib, la sugo wakhti, tusaale ahaan in la sugo 6 Confirmations, oo macnaheedu yahay in la sugo ilaa iyo inta ay ka soo wareegayaan 5 Block oo danbe, amaba ka badan, gaar ahaan lacag-dirisyada waa-weyn, si loogu niyad-samaado in aan lala noqon karin, ama ugu yaraan la faragashan karin. Mar alaale markii ay tiro badan oo Blocks-yo ah ka soo wareegaan, waa mar kasta oo ay lacagtaas adag tahay in dib loola noqdo.

> *The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.*
>
> *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.*

Halkan wuxuu Satoshi soo jeedinayaa talo ama xeelad hoos u dhigaysa in uu weeraryahanku lacagta dib ula noqdo, isagoo hadalkiisa ku bilaabay, waa in qofka loo-diraha ah ama qofka lacagta loo dirayo uu adeegsadaa furayaal cusub ama Address-yo cusub, mar kasta oo lacag loo dirayo, si uu weeraryahanka u dib dhigo.

Ujeedka Satoshi waa in aan weeraryahanka la siin fursad uu goor hore ku diyaariyo silsilad been-abuur ah, waayo diruhu wuxuu mar waliba ku khasban yahay in uu helo cinwaanka ama furayaasha loo-diraha ka hor inta aan wax loo dirin, taasoo weerarka dib u dhac weyn u horseedaysa, weerarkana ka dhigaysa mid aan hore loo sii qorshayn karin, maadaama loo baahan yahay Address-ka loo-diraha.

Satoshi wuxuu halkan tilmaamayaa in ay jirto halis ah in diraha aan daacadda ahayn, uu si qarsoodi ah u dhiso silsilad kale oo ay ku jirto Version ama nuqul been ah oo Transaction-kiisa ah, hadii uu hore u ogaa halka loo dirayo lacagta, isagoo ku rajjo weyn in ay mar uun silsiladdiisa dhaafi doonto tan daacadda ah.

Hadii uu loo-diruhu adeegsado furayaal cusub (Fresh Public Key), waxa uu meesha ka saarayaa suurtagalnimadii ahayd in uu diruhu goor hore sii diyaarsado silsilad been-abuur ah, sababtoo ah lama fulin karo lacag-dirista, maxaa yeelay wali lama go'aamin halka loo dirayo.

Hadii se uu diruhu (Sender) hore u sii ogaa furaha guud ama Address-ka lacagta lagu dirayo, wuxuu goor hore bilaabi karaa inuu si qarsoodi ah uga shaqeeyo silsilad been-abuur ah, taasoo xanbaarsan lacag-diristii la-la noqonayay, kadibna uu kula tartamo silsiladda daacadda ah, hadii uu ka hormaro tan daacadda ah, si lama filaan ah buu u soo bandhigayaa, taasoo keensanaysa in ay shabakaddu aqbasho, maxaa yeelay shuruudihii bay buuxisay, sidaasina weeraryahanku wuxuu ku sameeyay "Double Spending".

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

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

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:

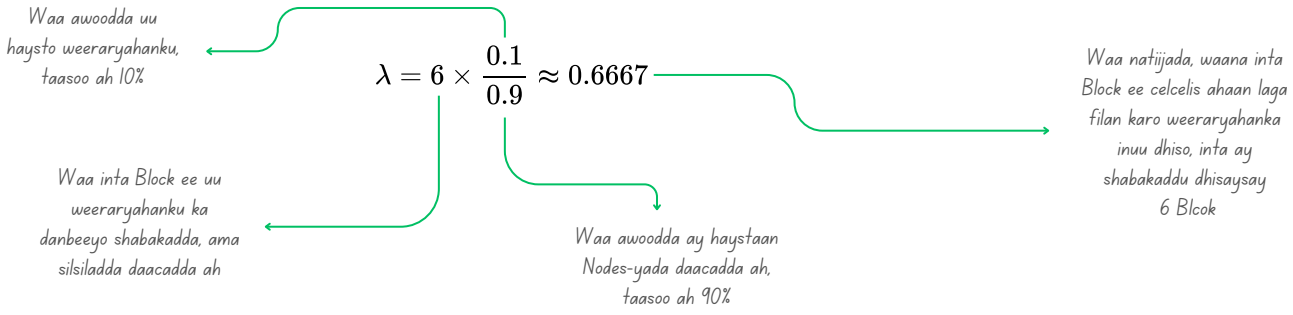
Dhanka kale, wuxuu Satoshi yidhi waa in loo-diruhu (Receiver) sugaa tiro Blocks-yo ah oo danbe (6 Confirmations ama ka badan, hadii ay lacagtu aad u badan tahay), si uu si niyadsami leh ugu kalsoonaado lacagta, isla mar ahaantaana uu u garawsado in aan la-la noqon karin, kadibna uu bixiyo badeecaddii ama adeegii uu dhaafsanayay.

Loo-diruhu ma oga tallaabada dhabta ah ee uu marayo weeraryahanku, maxaa yeelay si qarsoodi ah buu u dhisayaa silsiladdiisa, sidaa darteed, waxaynu adeegsanaynaa xeer xisaabeedka loo yaqaan "Poisson Distribution", si aynu u ogaan heerka uu weeraryahanku marayo, xeerkaasoo ah:

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

- **λ =** (lambda) waa celceliska tirada Blocks-yada uu weeraryahanku filan karo inuu dhiso intii ay shabakadda daacadda ahi dhisaysay z blocks.
- **z =** waa tirada Blocks-yada ee ay shabakadda daacadda ah dhistay, tan iyo markii Transaction-ka la geliyay Block-ga.
- **q =** waa suurtagalnimada ama kanshada uu weeraryahanku ku heli karo Block xiga (ama hadaynu si kale u dhigno, waa awoodda ama Hash Power-ka ay leeyihiin weeraryahanada).
- **p =** waa suurtagalnimada ama kanshada uu Node daacad ahi ku heli karo Block xiga (ama hadaynu si kale u dhigno, waa awoodda ama Hash Power-ka ay leeyihiin Nodes-yada daacadda ah).

Hadii uu weeraryahanku rabo in uu la noqdo lacag uu diray, lacagtaasoo ku jirta Block **#100**, hasa yeeshee ay ka soo wareegeen **6** Block oo danbe, oo ay haatan shabakaddu marayso Block-ga **#106**, markaa **z** oo u taagan tirada Blocks-yada ka danbaysay lacag-dirista waa **6** (**z = 6**), haddaba hadii uu weeraryahanku haysto awood dhan **10%**, kuwa daacadda ahina ay haystaa **90%-ka** kale ee soo hadhay, markaa iyada ah waxaa noo soo baxaysa: **≈ 0.6667**.



Hadii aynu si kale u dhigno, inagoo raacayna xeerkan "**λ = z × (q/p)**":

- **q = 0.1** awoodda uu weeraryahanku leeyahay
- **p = 0.9** awooda ay leeyihiin Nodes-yada daacadda ah
- **z = 6** tirada uu weeraryahanku ka danbeeyo silsiladda daacadda ah
- **λ = 0.6667** Block, oo ah tirada laga filanayo in uu weeraryahanku dhiso, intii ay shabakaddu dhisaysay 6 Block

Tani waxay ka dhigan tahay in weeraryahanka celcelis ahaan laga filan karo inuu dhiso ku dhawaad **0.66 Block**, intii ay shabakaddu dhisaysay **6 Block**, taasoo noo muujinaysa heerka ama hormarka uu samayn karo weeraryahanku.

> *To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:*
>
> $$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$
>
> *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:*
>
> $$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & hadii\ k \le z \\ 1 & hadii\ k > z \end{cases}$$

Kadib markii aynu ogaanay celceliska laga filan karo weeraryahanku inuu dhiso ku dhawaad 0.66 Block, intii ay shabakaddu dhisaysay 6 Block, Satoshi wuxuu leeyahay waa maxay suurtagalnimada uu wali weeraryahanku haysto, si uu uga daba imaado silsiladda daacadda ah?

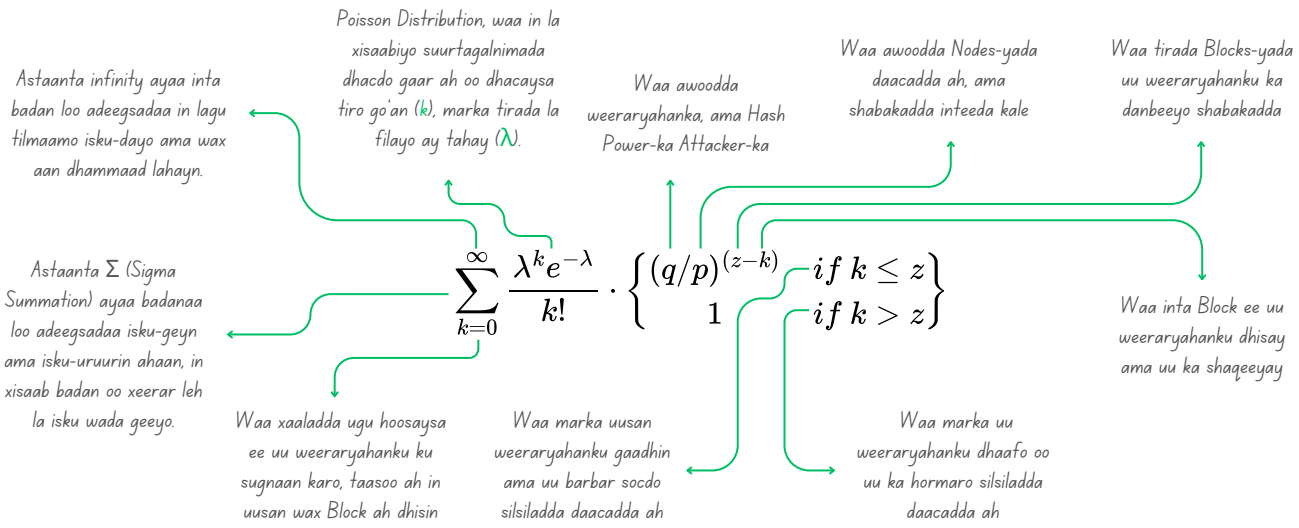
Halkan Satoshi wuxuu leeyahay, ma garan karno inta Block ee uu weeraryahanku dhisay, waayo si qarsoodi ah buu u dhisayaa, hasa yeeshee kaliya waxaynu ogaan karnaa suurtagalnimada uu ku dhisi karo, markii loo barbardhigo inta ay shabakaddu dhistay.

Sidaa darteed, si aynu haddaba u ogaano suurtagalnimada ama kanshada uu wali haysto weerarayahanku, waxaynu tallaabo kasta ama korordh kasta ee uu awoodi karo inuu qaado ka eegaynaa laba dhinac:

1. Celceliska Block ee uu dhisi karo weeraryahanku, inta ay shabakaddu dhisaysay **z** Block, taasoo lagu helo "**λ = z × (q/p)**"
2. Inta ay le'eg tahay kanshada ama suurtagalnimada uu haysto weeraryahanku, si uu u soo gaadho silsiladda daacadda ah, meel kasta uu markaas joogo, ama uu kaga danbeeyo silsiladda

Isku-darka labadaas, waxaynu ku helaynaa halista guud ee uu weeraryahanku wali leeyahay, sida xeerka ku cad.

Tani waa mid ka mid ah xeerarka (Formula) ugu qotoda dheer leh ee uu Satoshi Nakamoto ku soo bandhigay xaashidan cad, ama cilmi-baadhistan.



TS, hadii uu weeraryahanku rabo inuu dib ula soo noqdo lacag uu kharashgareeyay, taasoo ku jirta Block-ga #100, hasa yeeshee ay shabakaddu sii marayso Block-ga #106, markaa iyada ah waa:

- Haddii uusan weeraryahanku wali wax dhisin 0 Block (k = 0) → wuxuu silsiladda ka danbeeyaa 6 → suurtagalnimadu waa (q/p)^6
- Haddii uu dhisay 1 Block (k = 1) → wuxuu ka danbeeyaa 5 → suurtagalnimadu waa (q/p)^5
- Haddii uu dhisay 2 Block (k = 2) → wuxuu ka danbeeyaa 4 → suurtagalnimadu waa (q/p)^4
- Haddii uu dhisay 3 Block (k = 3) → wuxuu ka danbeeyaa 3 → suurtagalnimadu waa (q/p)^3
- Haddii uu dhisay 4 Block (k = 4) → wuxuu ka danbeeyaa 2 → suurtagalnimadu waa (q/p)^2
- Haddii uu dhisay 5 Block (k = 5) → wuxuu ka danbeeyaa 1 → suurtagalnimadu waa (q/p)^1
- Haddii uu dhisay 6 Block (k = 6) → labada silsiladood way is barbarsocdaan → suurtagalnimadu waa (q/p)^0
- Haddii uu weeraryahanku gaadho 7 Block → wuu dhaafay silsiladdii daacadda ahayd

Tusaalahan waxaynu u soo qaadanay si aynu fahamka u soo dhawayno, hasa yeeshee waa tusaale ama male runta ka fog, oo aan xaqiiq ahayn, waayo inta uu weerayahanku waxaas oo Block dhisayay, shabakaddu iyadu maxay qabanaysay, oo ay u sii sugaysay?.

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

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

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

Halkan waa isla xeerkii hore ama Formula-dii hore oo la soo koobay, si looga baaqsado suurtagalnimada yar-yar ee aan dhammaadka lahayn, maadaama ay tii hore xisaabinaysay dhammaan suurtagalnimadii, yar iyo weynba, isagoo Satoshi dib-u-qaabayn ku sameeyay.

Converting to C code...

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

Halkanna waa iyadoo Code-ahaan loo rogay, gaar ahaan loo rogay af-ka C, waxaynu inagana ku daraynaa nuqul kale oo Python ah.

```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;
}
```

Waa dhowr tijaabo, (Mult-Test), oo lagu helayo kanshada uu weeraryahanku leeyahay, hadii uu haysto awood intaas le'eg, iyadoo wax laga bedeli karo, awoodiisa, waxnana lagu kordhin karo

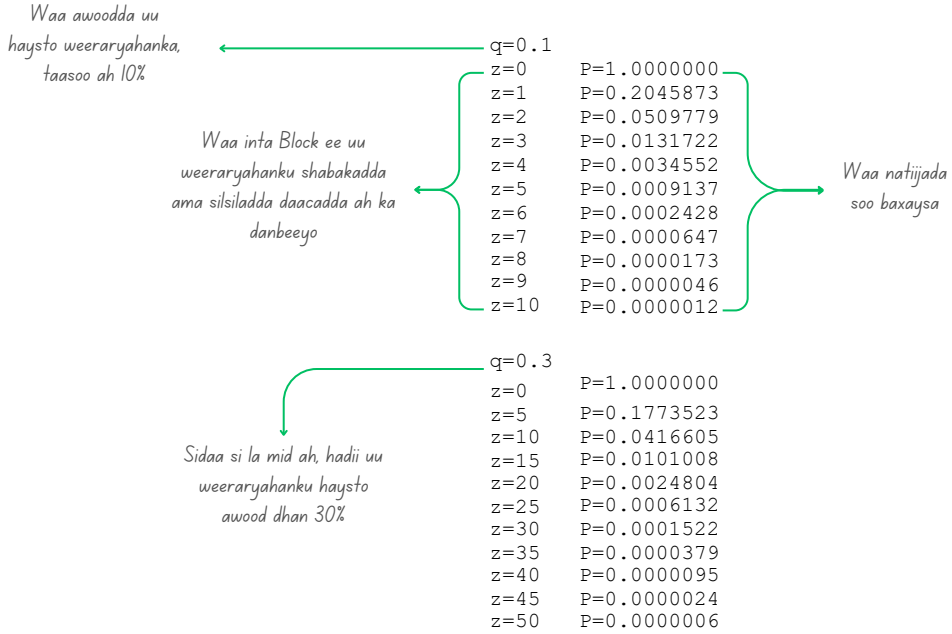
Waa inta Block ee uu weeraryahanku shabakadda ama silsiladda daacadda ah ka danbeeyo, iyadoo la kordhin karo, lana dhimi karo, si loo helo natiijooyin kala duwan

```python
from math import pow, exp

def attacker_success_probability(q: float, z: int) -> float:
    p = 1.0 - q
    lam = z * (q / p)
    total = 1.0

    for k in range(z + 1):
        poisson = exp(-lam)
        for i in range(1, k + 1):
            poisson *= lam / i
        total -= poisson * (1 - pow(q / p, z - k))

    return total

# Tijaabooyin kala duwan
q = [0.1, 0.2, 0.3, 0.4, 0.5, 0.6]
z = 5  # Confirmations

for q in q:
    prob = attacker_success_probability(q, z)
    print(f"q = {q:.1f}, z = {z} → kanshada weeraryahanka = {prob:.7f}")
```

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

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

Halkanna waxaa ah natiijooyinka qaar, oo tusinaya sida ay kanshadu u yaraanayso, mar kasta oo ay tiro Blocks-yo ah oo danbe soo kordhaan, taasoo muujnaysa heerka adkida wax ka bedelka shabakadda, gaar ahaan markii tiro Blocks-yo ah, ama z Blocks-yo ka soo wareegaan.

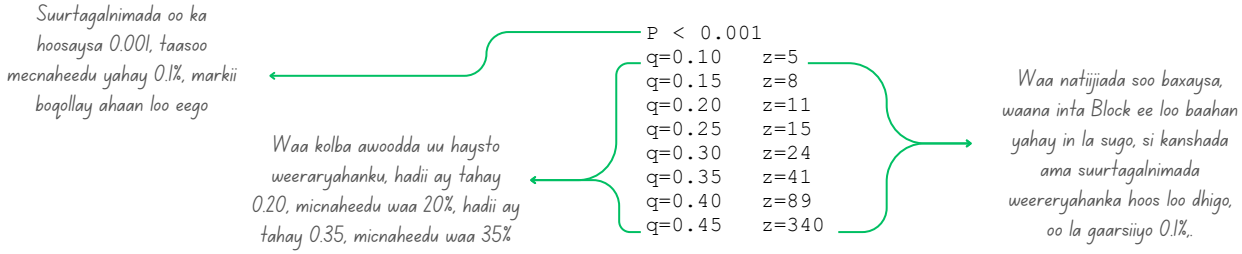


Solving for P less than 0.1%...

Suurtagalnimada ama kanshada P oo ka hoosaysa 0.1%...

Halkan Satoshi wuxuu soo bandhigayaa tusaalooyin keensanaysa in ay kanshadu ama suurtagalnimadu hoos uga yaraato **0.1%**. Hadii uu weeraryahanku leeyahay awood dhan **10%**, taasoo ah **q = 0.10**, markaa iyada ah waxaa loo baahan yahay kaliya in la sugo **5 Block** oo danbe, si ay lacagtaas u noqoto mid aan lala noqon karin, waxnana laga bedeli karin, kanshada la noqoshadeeduna noqoto **0.1%**.

Hasa yeeshee, hadii uu weeraryahanku haysto awood dhan **45%**, taasoo ah **q = 0.45**, si ay lacagtaas u noqoto wax ay adag tahay in lala noqdo, oo ay ku biirto **0.1%**, waxaa loo baahan yahay in la sugo **340 Block** oo danbe, ama **340 Confirmations**.



12. Conclusion (Gabagabada)

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

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.

Qeybtan 12-aad, wuxuu Satoshi ku soo gunaanadayaa aragtida Bitcoin, isagoo yidhi waxaan soo jeediyay hannaan lacageed oo dhamaystiran, oo danabaysa, oo suuragalinaya in qof dunida dacalkeeda jooga uu lacag u diro qof kale oo jooga dunida dacalkeeda kale, oo aan ku tiirsanayn kalsooni, taasoo meesha ka saaraysa baahidii loo qabay qolo saddexaad, oo go'aamo ka gaarta waxyaabaha shabakadda ka dhex socda.

Xalkeenu wuxuu ka bilawday saxiixyada dhijitaalka ah, oo caddaynayay lahaanshiyaha lacagta, hasa yeeshee waa xal kala dhantaalan, oo aan buuxin, si uu haddaba xalka u dhammaystirmo wuxuu Satoshi mar labaad soo jeediyay hannaan ama shabakad qof-ka-qof ah, iyadoo la adeegsanayo hab-sugid shaqo.

Tani waxay suuragal ka dhigaysaa in la helo silsilad ama Blockchain aan si fudud wax looga bedeli karin, la faragashan karin, lala noqon karin, la tirtiri karin xisaab ahaan, hadii cidda gacanta ku haysa badidoodu yihiin daacad.

Hannaankan wuxuu si weyn u beddelay aragtida dhaqaalaha, kaasoo suuragalinaya in qof uu lacag si toos ah ugu diro qof kale, iyada oo aan loo baahnayn marin dhexe, ogolaanshiyo, tallaabooyin dheeri ah, bangi, iwm, kaliya labada qof ee wax is waydaarsanaya (P2P).

Hannaanku waa mid aan u baahnayn qaab-dhismeed ama sal adag, si uu u shaqeeyo, wuxuu kaliya u baahan yahay is abaabul yar oo fudud, qof kasta oo shabakadda ka tirsan si madax-bannaan buu u hawlgalaa, si gaar ahna buu uga shaqeeyaa waxyaabaha qumman, halka uu iska idha-tiro waxyaabaha aan qummanayn. Natiijaduna waxay noqotay in si dabiici ah loo helo hannaan kala saara runta iyo beenta, daacadnimada iyo khiyaamada, iyadoo aan loo baahnayn garsoore dhexe.

Qof kasta wuxuu si toos ah ugu biiri karaa shabakadda goorta uu doono, sidaa si la eg, wuu ka bixi karaa, isla mar ahaantaana wuu ku soo laaban karaa shuruud iyo ogolaanshiyo la’aan, isagoo kaliya aqbalaya wixii wax-qabad ee hore ee ay shabakaddu qabatay, taasoo caddayn ama marag u ah wixii dhacay intii la maqnaa.

Sidoo kale waa la codayn karaa, loona codayn karaa wixii quman, sida ansixinta Blocks-yda iyo Transaction-yada qumman iyo wixii aan qummanayn sida Blocks-yadii iyo Transaction-yadii aan qummanayn, iyadoo la iska indha tirayo, waxaana codka lagu miisaamayaa awoodda xisaabeed ee qalabka la adeegsanayo (CPU/GPU/ASIC).

Intaa kadib wuxuu Satoshi yidhi, hadii loo baahdo in xeer cusub la soo saaro ama xeer hore u jiray la sii hormariyo, amaba wax kaloo dan guud ah waa lagu dhaqan-galin karaa Bitcoin, dabcan hadii ay aqlabiyaddu ogolaato in uu dan guud yahay, ama dan u yahay Bitcoin, oo si wada jir ah la iskugu raaco (Consensus Mechanism).

BItcoin waa hannaan isku dhan, oo caddayn iyo hufnaan ku dhisan, kaasoo awood u leh inuu la tacaalo waxyaabaha cusub ee ku soo darriya, ee aan loo meel dayin, waa hannaan u babac dhigmi kara qalalaasaha, musuq-maasuqa, is-bedelada aan loo meel dayin, iyo xittaa weerarada qorshaysan, waa hannaan aan ku tiirsanayn wax kalsooni ah haba yaraatee, waa hannaan 100% madax-bannaan.

References (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.