Bítkọìnì: Sístẹ́mù Owó Ẹlẹktróníìkì Peer-to-Peer

látọwọ́ Satoshi Nakamoto 2008/10/31

Àkótán

Irú owó ẹlẹktróníkì tó jẹ́ peer-to-peer (ẹníkan sí ẹnìkejì) gidi yíó gba ìsanwó online láàyè láti wá tàárà látọ̀dọ̀ ẹníkan sí ọ̀dọ̀ ẹnìkejì lái gba ọ̀dọ̀ ilé-iṣẹ́ ìmójútó owó kankan kọjá. Ìtọwọ́bọ̀wé oníṇọ́mbà jẹ́ ìkan nínú àwọn ìṣojúùtú èyí, sùgbọ́n àwọn ànfàní rẹ̀ pàtàkì jùnù tí olùgbàjà bá pọndandan láti dínà ìnáwó-lẹ́ẹ̀mejì. A dá àbá ojúùtú fun isòrò ìnáwó-lẹ́ẹ̀mejì nípa lílo ẹ̀rọ- aṣẹṣẹ́pọ̀ peer-to-peer. Ẹ̀rọ ìṣẹṣẹ́pọ̀ ṣe àmì-ásìkò sí àwọn ìdúnadúrà nípa híha wọ́n sínú okùn ẹ̀rì-ìṣe-iṣẹ́ oníhíha tì kò dúró, èyì dá àkọsílẹ̀ tí kò le ṣe yí padà lái ṣe títún ṣe ẹ̀rí-ìṣe-iṣẹ́. Okùn tó gùn jùlọ dúró bí i ajẹ́ẹ̀rí bí ìṣẹ̀lẹ̀ tó ṣelẹ̀ ṣe tẹ̀lé ra wọn àti pé okùn náà wá látọ̀dọ̀ àgbajọ agbára CPU tọ́ tóbi jùlọ. Tó bá sá à ti jẹ́ pé ọ̀pọ̀ gbogbo agbára CPU wà lábẹ́ àwọn ojúpópó- ẹ̀rọiṣẹ́ tí wọn kò fọwọ́sọwọ́pọ̀ láti kọ lu ẹ̀rọ aṣẹṣẹ́pọ̀ náà, wọn yíò dá okùn tó gùn jùlọ, wọn yíò sì fi àwọn alátakò wọn sẹ́yìn. Ẹ̀rọ-aṣẹṣẹ́pọ̀ ọ̀hún gan kò sòro láti dá sílẹ̀. Àwọn ìkéde ún wáyé pẹ̀lú ìgbìyànjú ẹ̀rọ ìṣẹṣẹ́pọ̀ náà tó dára jùlọ, bẹ́ ẹ̀ sìni àwọn ojúpópó-ẹ̀rọiṣẹ́ le dara pọ̀ mọ́ tàbí yọ ara wọn kúrò láti inú ẹ̀rọ-aṣẹṣẹ́pọ̀ náà bọ́ bá ṣe wù wọ́n, tí wọn ó sì gba okún ẹ̀rí-ìṣe-iṣẹ́ tó gùn jùlọ gẹ́gẹ́ bíi ẹ̀rí ohun tó ti ṣẹlẹ̀ nígbà tí wọn kò sí níbẹ̀.

Ìbẹ̀rẹ̀

Ọ̀rọ̀ ajé lórí Íntánẹ́ẹ̀tì gbọ́kàn lé àwọn ilé-iṣẹ́ ìmójútó owó gẹ́gẹ́ bí olùlàjà láti ṣe ìgbésẹ̀ àwọn ìsanwó ẹlẹktróníìkì. Bótilẹ̀ jẹ́ pé sístẹ́mù yìí unṣíṣẹ́ dáadáa fún ọ̀pọ̀ àwọn ìdúnádúnà, síbẹ̀ síbẹ̀ ó ní àwọn ìsòro tí àwọn ohun tó bá gbọ́kàn lé olùlàjà ní. Àwọn ìdúnádúrà tí kò ṣe é dá padà kò ṣe é ṣe rárá, nítorípé áwọn ilé-iṣẹ́ ìmújútó owó kò lé mọ́ ṣáì ṣe ìlàjà. Owó ìlàjà jẹ́ kí ìdúnádúnà náà ó gbówó lórí, èyí jẹ́ kí ìtóbi ìdúnádúnà tó ṣe é ṣe ó ní ye pàtó, èyí kò gba àwọn ìdúnádúnà kékèèké ní àáyè, bẹ́ ẹ̀ sìni àile ṣe ìsanwó aláìle-dápadà fún iṣẹ́ aláìle-dápadà fa ìgbówó lórí. Ìdúnádúrà tó ṣe é dápadà yíò jẹ́ kí àwọn olùlàjà ó pọ̀ si. Àwọn ọ̀tajà gbọ́dọ̀ sọ́ra fún àwọn oníìbárà wọn, wọ́n sì gbọdọ̀ mọ̀ wọ́n dáadáa ju bó ṣe yẹ lọ. Wọn kò le dínà jìbìtì. A le lo owó ọwọ́ fún ìdúnádúrà dínwó lái lo olùlàjà, sùgbọ́n lórí ìlà-ọ̀nà ẹ̀rọ-ìbánisọ̀rọ̀ kò sí ọ̀nà a ti ṣe ìdúnádúrà tàárà lái sí olúlàjà tó ṣe é gbọ́kàn lé.

Lati ṣè yí, a gbọ́dọ̀ dípò olùlàjà pẹ̀lú sístẹ́mù ìsanwó ẹlẹktróníìkì tó dá lórí ẹ̀rí ìkọbojúbojú (cryptography), kí àwọn tí wọn bá fẹ́ ó le ṣe ìdúnádúrà láàrin ara wọn tàárà lái lo olùlàjà kankan. Àwọn ìdúnádúrà tí ìṣirò wọn sòro láti dápadà yíò dá àbò bo àwọn àtàjà lọ́wọ́ jìbìtì, bẹ́ ẹ̀ sìni ọ̀nà ìmówódání kò ní sòro láti jẹ́ dídásílẹ̀ láti fi dá àbò bo àwọn arajà. Nínú àròkọ yì, a dá àbá ojúùtú sí ìsòro ìnáwó-lẹ́ẹ̀mejì nípa lílo ẹ̀rọ apèsè àmì-àsìkò peer-to-peer láti dá ẹ̀rí oníìṣirò àsìkò ìdásílẹ̀

àwọn ìdúnádúrà. Sístẹ́mù yí yíò ní àbò tó bá sá ti jẹ́ pé àwọn ojúpópó- ẹ̀rọisẹ́ olóòtọ́ọ́ darapò láti sàkóso àgbára CPU tó pọ̀ ju àwọn ojúpópó-ẹ̀rọisẹ́ tó fẹ́ kọ lùú lọ.

Àwọn ìdúnádúrà

A ṣe ìtumọ̀ owóníná ẹlẹktróníìkì gẹ́gẹ́ bí okùn kan àwọn ìtọwóbọ̀wé onínọ́mbà. Ẹni tó nií le fi ránṣẹ́ sí ẹlòmíràn nípá ṣíṣe ìtọwọ́bọ̀wé onínọ́mbà hìha ìdúnádúrà tó gbèyìn àti kọ́kọ́rọ́ ìgboro ẹni tókàn láti nií, tí wọn ó sì fi wọ́n kún ìṣetán owóníná náà. Ẹni tí wọ́n náwó náà fún le ṣe ìmúdájú àwọn ìtọwọ́bọ̀wé náà láti ṣe ìmúdájú gbogbo àwọn tó ti nií tẹ́lẹ̀.

Ó sòro fún ẹni tí wọ́n sanwó fún láti mọ̀ dájú dájú pé ẹni tó sanwó kò tí ì ná owó náà tẹ́lẹ̀, pé kò tí ì na ní ẹ̀ẹ̀mẹjì. A le borí ìsòro yìí pẹ̀lú olùlàjà tó ṣe é gbọ́kàn lé tí yíò ṣe àyèwó ìdúnádúnà fún ìnáwó-lẹ́ẹ̀mejì. Lẹ̀yìn ìdúnádúrà kọ̀ọ̀kan, á dá owó náà padà sí ibi tí a ti dáà, bẹ́ ẹ̀ sìni owó tí ilé-ìdá owó dá nìkan ní a mọ̀ dájú pé wọn kò tíì ná ní ẹ̀ẹ̀mẹjì. Ìsòro èyí ni pé gbogbo sístẹ́mù owó gbọ́kàn lé ilé-isẹ́ tó úndá owó, tórípé gbogbo ìdúnádúrà gbọ́dọ̀ gba ọ̀dọ̀ wọn kọjá bí i pé wọ́n jẹ́ bánkì.

A fẹ́ wá ọ̀nà tí ẹni wọ́n sanwó fún yíò fi mọ̀ pé àwọn tí owó náà gba ọwọ́ wọn wá tẹ́lẹ̀ kò tíì tọwọ́bọ̀wé àwọn ìnúnádúrà tẹ́lẹ̀. Láti ṣe èyí, ìdúnádúrà tó síwájú jùlọ nikan ni ó ṣe kókó, bí bẹ́ ẹ̀ẹ̀ a kò kọbi ara sí ìgbìyànjú láti ṣe ìnáwó ní ẹ̀ẹ̀mejì. Ọ̀nà kan soso a ti mọ̀ pé kò sí ìdúnádúrà ni tí a bá mọ gbogbo àwọn ìdúnádúrà. Nínú àpẹrẹ ilé-ìdá owó, ilé-ìdá owó mọ gbogbo ìdúnádúrá, bíi bẹ́ ẹ̀ẹ̀ wọn mọ eyí tó síwájú. Láti ṣe èyí lái sí olùlàjà tí a gbọ́kàn lé, àwọn ìdúnádúrà gbọ́dọ̀ jẹ́ hàn gbangba gbángbà sóde[1], a sì gbọdọ̀ wá sísẹ́tẹ́mù kan fún àwọn olùkópa yíò fẹnu kò sí lórí nípa bí àwọn ìdúnádúrà ṣe tẹ̀le ra wọn sí. Ẹni tí a sanwó fún gbọdọ̀ ní ẹ̀rí pé nígbà tí ìdúnádúrà kọ̀ọ̀kan wáyé, ọ̀pọ̀ àwọn ojúpópó-ẹ̀rọisẹ́ fẹnu kò si pé òhun ni ó síwájú.

Timestamp Server

Ojúùtú wa sí ìsòrò yìí bẹ̀rẹ̀ pẹ̀lú timestamp server (ẹ̀rọ-apèsè àmì-asìkò). Ẹ̀rọ-apèsè àmì- asìkò únsisẹ́ nípá mímú híha (hash) akójọ àwọn ohun tí a fẹ́ ṣe àmì asìkò sí, kí á sì tẹ híha wọ́n sí ta gbangban, bíi pé wọ́n jẹ́ ìwé-ìròyìn tàbí Usenet[2-5]. Àmì-asìkò fíhàn dájú pé dátà náà gbọ́dọ̀ ti wà ní àsìkò náà dájúdájú, nítoríẹ́ ló ṣe wá nínú híha. Amì-asìkò kọ̀ọ̀kan ní amí- àsìkò tó kọjá nínú híha rẹ̀, wọn ó wá dà bí okùn, gbogbo amì-àsìkò tó bá tẹ̀lé wọn ṣe ìmúdájú àwọn tó síwájú wọn.

Proof of Work (Ẹ̀rí-ìṣe-isẹ́)

Láti ṣe ẹ̀rọ apèsè àmì-asíkò tó dá lọ́rí peer-to-peer, a gbọ́dọ̀ lọ sístẹ́mù proof-of-work (ẹ̀ri-ìṣe- isẹ́) tó jọ Hashcash tí Adam Back dá sílẹ̀[6], dípò ìwé-ìròyìn tàbí ìfisórí Usenet. Ẹ̀rí-ìṣe-isẹ́ ni pé kí á wá iye nọ́mbà kan tó jẹ́ pé tí a bá ṣe híha rẹ̀, fún àpẹrẹ pẹ̀lú SHA-256, híha náà yíò bẹ̀rẹ̀ pẹ̀lú àwọn òdo. Isẹ́ ṣíṣe tó pọndandan yíò ga gan bí àwọn nọ́mba òdo tó pọndandan bá ṣe pọ̀ tó, ó sì ṣe é mọ̀

dájú nípa ṣíṣe híha kan soso.

Fún ẹrọ-aṣeṣẹpọ àmì-àsìkò wa, a lo ẹrí-ìṣe-iṣẹ nípa ṣíṣe ìgbéga iye nonce nínú àkójọ náà títí tí a ó fi rí iye kan tí yíò fún híha àkójọ náà ní iye nọmbà òdo tó yẹ. Lẹyìn tí agbára CPU bá tí fi ṣiṣẹ tán láti ṣe ẹrí-ìṣe-iṣẹ, àkójọ náà kò le ṣe é dápadà lái tún iṣẹ náà ṣe. Nítorípé àwọn àkójọ tó ún bọ lẹyìn jẹ síso mọ lẹyìn, iṣẹ tí yíò gbà láti ṣe ìdápadà àkójọ náà yíò pọndandan láti ṣe túntúnṣe gbogbo àwọn àkójọ tó tẹle.

Ẹrí-iṣẹ-ṣiṣe náà tún ṣe ojúùtú ìsòro wíwá ásojú ogolọgọ nínú ìpinu ṣíṣe. Tí ogunlọgọ bá dá lórí àdírẹẹsì IP kan-ìbò kan, ẹnikẹni ló le fi tipátipá gba agbára nípa fífún ara rẹ ní IP tó pọ. Ẹrí-iṣẹ-ṣiṣe dà bi CPU kan-ìbò kan. Ìpinu ogunlọgọ jẹ sísojú pẹlú okùn tógùnjùlọ, tó ní agbára ẹrí-iṣẹ-ṣíṣe tógajùlọ lórí rẹ. Tí ogunlọgọ agbára CPU bá wà lábẹ àwọn ojúpópó-ẹrọiṣẹ tó jẹ asọòótọ, okùn tó jẹ òótọ yíò pọ kíákíá, yíò sì ṣíṣẹ kíákíá ju okùn tó hún bá figa gbága lọ. Láti le ṣe àtúnṣe àkójọ tótipẹ kan, onípìbìtì kan gbọdọ le ṣe àtúnṣe ẹrí-iṣẹ-ṣíṣe fún àkójọ náà àti fún gbogbo àwọn àkójọ tó tẹle, ati pé kó tún le sáré ba, kó sì sáré síwájú iṣẹ àwọn ẹrọiṣẹ- ojúpópó asọòótó. Á fihàn níwájú nínú àyọkà yí pé agbára onípìbìtì láti sáre bá wọn yíò dín sí bí àwọn àkójọ tuntun bá ṣe ún jẹ fífi kún.

Láti ba ṣe ìdógba ìṣáre ìrinṣẹ àti ìfẹ láti ní ẹrọiṣẹ-ojúpópó fún ìgbà pípẹ, ìsòro ẹrí-iṣẹ-ṣíṣe jẹ wíwá pẹlú nọmbà ìpín-àrin tí kò dúró sójúkan tí yíò dá lórí iye nọmbà ìpín-àrin fún àwọn àkójọ tó wà láàrin wákàtí kan. Tí wọn (àkójọ) bá ún jẹ dídá sílẹ kíàkíá, ìsòro yíò pọ si.

Ẹrọ-aṣeṣẹpọ

Àwọn ìgbésẹ wọnyí ni a fi dá ẹrọ-áṣeṣẹpọ sílẹ:

1. Àwọn ìdúnádúrà jẹ fífi kéde sí gbogbo àwọn ẹrọiṣẹ-ojúpópó.
2. Ẹrọiṣẹ-ojúpópó kọọkan ṣe àkójọ àwọn ìdúnádúrà tuntun sínú búlọkù kan.
3. Ẹrọiṣẹ-ojúpópó kọọkan bẹrẹ iṣẹ láti wá ẹrí-iṣẹ-ṣíṣé tósòro fún búlọkù rẹ.
4. Tí ẹrọiṣẹ-ojúpópó kan bá ti rí ẹrí-iṣẹ-ṣíṣe, yíò ṣe ìkéde búlọkù náà sí gbogbo àwọn ẹrọiṣẹojúpópó tó kù.
5. Àwọn ẹrọiṣẹ-ojúpópó yíò gba búlọkù náà nìkan tí gbogbo àwọn ìdúnádúrà inú rẹ bá jẹ èyí tó bójúmu, tí wọn kò sì tíì jẹ èyi tí wọn ti ná.
6. Àwọn ẹrọiṣẹ-ojúpópó fihàn pé àwọn gba búlọkù yìí nípá bí bẹrẹ iṣẹ lórí dídá búlọkù tọkàn nínú okún náá, pẹlú lílo híhá búlọkù tí wọn gbà gẹgẹ bí híhá tó gbẹyìn.

Àwọn ẹrọiṣẹ-ojúpópó gba okùn tógùnjùlọ gẹgẹbí èyì tó tọ, wọn yíò sì tẹ síwájú iṣẹ láti fàágùn si. Tí àwọn ẹrọiṣẹ-ojúpópó méjì bá ṣe ìkéde irú búlọkù ọtọọtọ tó kàn tó yàtọ sí ra wọn lẹẹkan náà, àwọn ẹrọiṣẹ-ojúpópó mìrán le gba ìkan tàbí òmíràn lákọọkọ. Tó bá jẹ báyìí, wọn yíò bẹrẹ iṣẹ lórí èyí tí wọn kọkọ gbà, sùgbọn wọn yíò fi èkejì pamọ bóyá ó le gùn si. Nìgbà tí wọn bá rí ẹrí-iṣẹ-ṣíṣe tókàn ní wọn yíò tó mọ búlọkù wo lógùn; àwọn ẹrọiṣẹ-ojúpópó tó ún ṣiṣẹ lórí èkejì yíò yí ra wọn sí orí èyí tó gún jù.

Àwọn ìkéde ìdúnádúrà tuntun kò pọndandan kí wọn ó dé ọ̀dọ̀ gbogbo àwọn ẹ̀rọiṣẹ́-ojúpópó. Tí wọ́n báà ti dé ọ̀dọ̀ àwọn ọ̀pọ̀lọpọ̀ ẹ̀rọiṣẹ́-ojúpópó, wọn yíò bọ́ sínú búlọ́kù kan nígbà tó bá yá. Bákannáà àwọn ìránṣẹ́ tí kò jásí rere kò ní ipa lórí àwọn ìkéde búlọ́kù rárá. Tí ẹ̀rọiṣẹ́- ojúpópó kan kò bá gba búlọ́kù kan, yíò tọrọ rẹ̀ nígbàtí ó bá gba búlọ́kù tó kàn, tó bá ti ríi pé òhun ti fò ó tẹ́lẹ̀.

Ìwúrí

Gẹ́gẹ́ bíi ìṣe, ìdúnádúrà àkọ́kọ́ nínú búlọ́kù kan jẹ́ ìdúnádúrà pàtàkì tó bẹ̀rẹ̀ owọ́níná tuntun kan látọwọ́ olúdásílẹ̀ búlọ́kù òòhún. Èyí wà bíi ìwúrí fún àwọn ẹ̀rọiṣẹ́-ojúpópó láti fẹ̀yìn ti ẹ̀rọ- aṣẹṣẹ́pọ̀ náà, àti láti pèsè ọ̀nà láti ṣe ìpínjáde àwọn owóníná sínú káràbátà, nígbà tó jẹ́ pé kò sí aláse gbangba tó gbé wọn jáde. Bí owóníná sè ún jẹ́ fífikún lái yàtọ̀ jọ bí àwọn tó ún wa wúrà ṣe ún lo àlúmọ́nì láti fi wúrà kún káràbátà. Nínú tí wa yìí, àsìkọ̀ CPU àti iná wáyà ni à ún lò. Lẹ̀yìn ìgbà tí iye àwọn owóníná pàtó kan bá ti wọ inú káràbátà tán, ìwúrí le jẹ́ ilẹ́wó owó ìdúnádúrà níkàn pátápátá tí kò sì ní lẹ́wó rárá.

Ìwúrí tún le jẹ́ pẹ̀lú ìlẹ́wó owó ìdúnádúrà. Tí iye tó bá ìdúnádúrà jáde bá dín ju iye tó bá a wọlé lọ, ìyàtọ̀ ni ilẹ́wó owó ìdúnádúrà tí a fi kún gẹ́gẹ́ bí iye ìwúrí búlọ́kù náà tó ní ìdúnádúrà náà nínú.

Ìwúrí le jẹ́ kí àwọn ẹ̀rọiṣẹ́-ojúpópó kó jẹ́ aṣọ̀ótọ́. Tí olójúkòkòrò oníjìbìtì kan bá ṣe àgbájọ agbára CPU tó pọ̀ ju ti àwọn ẹ̀rọiṣẹ́-ojúpópó olóòótọ́ lọ, ó gbọ́dọ̀ mú bọ́yá òhun yíò lòó láti fi ṣe jìbìtì nípa jíjí owó ara rẹ̀ lọ́wọ́ ara rẹ̀, tàbí láti lòó láti fi dá owóníná tuntun. Yíò ri pé èrè wà fún òhun tí ó bá tẹ̀lé òfin, òfin tó jẹ́ pé ó gbàa láyè láti ní ọ̀pọ̀ owóníná tuntun ju àwọn tó kù lọ, ju pé kó wá fẹ́ ba sístẹ́mù òhún jẹ́ lọ àti ìdí owó ara rẹ̀.

Ìdásí Ààyè fún Ìkópamọ́

Lẹ́yìn tí ìdúnádúrà tó gbẹ̀yìn nínú owóníná kan bá ti rìn jìnnà nínú àwọn búlọ́kù tó pọ̀ tó, àwọn ìdúnádúnà tí a ti sanwó wọn le jẹ́ píparẹ́ láti ṣe ìdásí ààyè dískì. Láti ṣe èyí lái gẹ́ híha búlọ́kù náà, a lo ọ̀nà igi Merkle[7][2][5] láti fi ha àwọn ìdúnádúrà náà, lọ́nà tó jẹ́ pé gbòngbò rẹ̀ níkan ni yíò wà nínú híha búlọ́kù náà. Àwọn búlọ́kù tótipẹ́ le jẹ́ fífúnpọ̀ nípa gíge àwọn ẹ̀ka igi náà. Àwọn híha tó wà nínú kò pọndandan ká fi wọ́n pamọ́.

Àkọlé búlọ́kù tí kò ní ìdúnádúrà kankan nínú yíò jẹ́ bíi 80 bytes. Tí a bá sọ pé àwọn búlọ́kù únjáde láàrin ìṣẹ́jú 10, 80 bytes * 6 * 24 * 365 = 4.2MB lọ́dún. Pẹ̀lú àwọn ṣístẹ́mù kòmpútà tí wọ́n ní RAM 2GB nínú ní ọdún 2008, Òfin Moore sọ pé yíò tó 1.2GB lọ́dún, ààyè ìkópamọ́ kò ní jẹ́ ohun tósòro tí a bá tiẹ̀ sọ pé a fẹ́ fi àwọn àkọlé búlọ́kù pámọ́ sínú ààyè ìrántí kọ̀mpútà.

Ìmúdájú Ìsanwó Tíkòsòro

Ó ṣe é ṣe láti ṣe ìmúdájú àwọn ìsanwó lái ní ẹ̀rọiṣẹ́-ojúpópó aṣẹṣẹ́pọ̀ tó kún rẹ́rẹ́. Oníṣe kàn ní láti fi àwòkọ àwọn àkọlé búlọ́kù ẹ̀rí-iṣẹ́-ṣíṣe tógùnjùlọ pamọ́, ó le gbà wọ́n tó bá tọrọ wọn nínú àwọn

ẹ̀rọ-áṣeṣẹ́pọ̀ ojúpópó títí tó fi ní ìdálójú pé ó ti rí okùn tógùnjùlọ, tó sì gba ẹ̀ka igi Merkle tó so ìdúnádúrà náà mọ́ búlọ́kù tó ní àmì-àsìkò rẹ̀ nínú. Kò lè rí ìdúnádúrà náà gan fún rarẹ̀, sùgbón nítorípé ó tí ní sísopọ̀ mọ́ ibì kan lórí okùn, ó lé ríi pé ẹ̀rọ-áṣeṣẹ́pọ̀ ojúpópó kan tí gbàá, àti pé àwọn búlọ́kù tó tẹ̀le náà tún fi dáwalójú pé ẹ̀rọ-ìṣeṣẹ́pọ̀ ti gbàá.

Nípa bẹ́ ẹ̀, ìmúdájú náà ṣe é gbọ́kànlé tó bá sá ti jẹ́ pé àwọn ẹ̀rọiṣẹ́-ojúpópó olóòtọ́ ló úndarí ẹ̀rọ-ìṣéṣẹ́pọ̀ náà, sùgbọ́n yíò kúdíẹ̀ káàtó tí ẹ̀rọ-ìṣéṣẹ́pọ̀ náà bá bọ́ṣọ́wọ́ oníjìbìtì. Bótitìlẹ́pé àwọn ẹ̀rọiṣẹ́-ojúpópó lé ṣe ìmúdájú àwọn ìdúnádúrà fún ra wọn, ọ̀nà tíkòsòro yìí le ṣe é túje tí oníjìbìtì kan bá dá ìdúnádúrà èké nígbàtí ẹ̀rọ-ìṣéṣẹ́pọ̀ bá bọ́ sọ́wọ́ rẹ̀. Ònà kan tí a fi le dínà èyí ní kí á gba ìkìlọ̀ látọ̀dọ̀ àwọn ẹ̀rọiṣẹ́-ojúpópó nígbàti wọ́n bá rí búlọ́kù tí kò bójúmu, èyí yíò fàá kí kọ̀mpútà kó daunlóòdù gbogbo búlọ́kù lẹ́ẹ̀kúnrẹ́rẹ́ àtí àwọn ìdúnádúrà tó ní ìkìlọ̀ láti fi dájú pé kò bójúmu. Àwọn onítajà tí wọ́n úngba ìsanwó nígbàkígbà yẹ́ kí wọn ó ní àwọn ẹ̀rọiṣẹ́-ojúpópó tókúnrẹ́rẹ́ fún àbò ara wọn àti láti ṣe ìmúdájú kíákíá.

Ìsopọ̀ àti Ìyàsọ́tọ̀ Iye

Bótilẹ̀jẹ́pé ó ṣe é ṣe láti ṣe ìgbéṣe owóníná kọ̀ọ̀kan fúnra ara wọn, yíò ti pọ̀jù láti ṣe ìdúnádúrà ọ̀tọ̀ọ̀tọ̀ fún eépìnnì kọ̀ọ̀kan nínú ìfiránṣẹ́. Kí á le baà ṣe ìyàsọ́tọ̀ àtí ìsopọ̀ àwọn iye, àwọn ìdúnádúrà ní ọ̀pọ̀lọpọ̀ ìkówọlé àtí ìkójáde. Déédéé ìkówọlé kan soso látínú ìdúnádúrà gbàngbà tẹ́lẹ̀ kan tàbí ọ̀pọ̀ ìkówọlé tó dá áwọn ìdúnádúrà kékèké papọ̀, àti ó pọ̀ jú, ìkójáde méjì: ìkan fún ìsanwó, àtí èkejì tí yíò dá owó tóṣẹ́kù, to bá wà, padà sí ẹni tó fi ránṣẹ́.

A gbọ́dọ̀ ṣe àkíyésí pé iye àwọn ìkówọlé tọ́ bá ìkójáde wá, níbití ìdúnádúrà kan dá lé àwọn ọ̀pọ̀ ìdúnádúrà, àti àwọn ọ̀pọ̀ ìdúnádúrà náà tún dálé àwọn míràn, kò jẹ́ ìsòro ní hà hín rara. Kò sí ìdí láti wá ìtàn ìdúnádúrà ẹyọkan soso tó dáwá fún rara rẹ̀.

Ìdáni

Àpẹrẹ bí bánkì ṣe únṣiṣẹ́ ní ìpele ìdáni nípa dídènà sí mì mọ àwọn wo ní wọ́n únṣe káràbátà. Nítorípé ó pọndandan láti polongo gbogbo ìdúnádúrà síta a kò le lo irú ọ̀nà ìdáni yìí, síbẹ̀ a sì le ní ìdáni tí a bá dìnà ìmò ní ibòmíràn: nípa jíjẹ́ kí àwọn kọ́kọ́rọ́ ìgboro jẹ́ aláìlórúkọ. Gbogbo aye ló le ríi pé ẹnìkan únfi iye owó kán ránṣẹ́ sí ẹlòmíràn, sùgbọ́n láì sí ìmọ̀ kankan tó so ìdúnádúrà náà mọ́ ẹnìkankan. Èyì jọ bí irú ìmọ̀ tí àwọn ilé-iṣẹ́ pásípàrọ̀ únfi síta, níbi tí àsìkò àti ìtóbi pásípàrọ̀, èyun "tape", jẹ́ pípolpngo síta láì sọ ùnkankan nípà àwọn ẹnì tó jẹ mọ́.

Gẹ́gẹ́bí àbò míràn, kọ́kọ́rọ́ tuntun gbọ́dọ̀ jẹ́ lílò fún ìdúnádúrà ọ̀tọ̀ọ̀tọ̀ láti dínà ìmọ̀ ọ̀dọ̀ ẹnì tí wọ́n wọn wá. Ìmọ ọ̀dọ̀ ẹni tí wọ́n tí wá lé mọ́ ṣe é dínà pẹ̀lú àwọn ìdúnádúrà ìkówọlé púpọ̀, nítorípé ó lé sàfihàn ọ̀dọ̀ ẹnì tí wọ́n ti wá. Ewu ibẹ̀ ni pé tí ẹni tó ni kọ́kọ́rọ́ kan bá jẹ́ mímọ̀, èyí le sàfihàn àwọn

ìdúnádúrà míràn tí onítọ̀hún ti ṣe.

Àwọn ìṣirò

A wò ó bóyá onípìbìtì kan le dá okùn búlọ́kù kan kíákíá ju okùn búlọ́kù òótọ́ lọ. Tí èyí bá ṣe é ṣe gan kò ní ṣe ìyípadà sí sístẹ́mù, bí i pé kó dá iye owó tí kò sí tàbí pé kó mú owó tí kì í ṣe tirẹ̀. Àwọn ẹ̀roiṣẹ́-ojúpópó kò ní gba ìdúnádúrà tí kò bójúmu gẹ́gẹ́bí ìsanwó, bẹ́ ẹ̀ sì ni àwọn ẹ̀roiṣẹ́-ojúpópó kò ní gbà búlọ́kù tó ní wọn nínú. Onípìbìtì kan ke gbìyànjú láti ṣe ìyípadà sí àwọn ìdúnádúrà ara rẹ̀ nìkàn ni láti gba owó tó ti ná láìpẹ́ padà.

Ìjàkadì láàrin okùn búlọ́kù oótọ́ àtí okùn búlọ́kù onípìbìtì ṣe é sàlàyé bí "ìrìnàkò olórúkọ méjì" (Binomial Random Walk). Ìyọrí sí rere ni okùn búlọ́kù òótọ́ tí búlọ́kù rẹ̀ únpọ̀si pẹ̀lú búlọ́kù kan, tó sì únlé wájú pẹ̀lú +1, tí ìyọrí sí ìkùnà jẹ́ okùn búlọ́kù onípìbìtì tí òhun náà búlọ́kù ti rẹ̀ náà únpọ̀si pẹ̀lú búlọ́kù kan, sùgbọ́n ó kàn jẹ́ kí ó dín pẹ̀lú -1.

Pé onípìbìtì yíò le mú u láti èyìn tó wà dà bí ìsòro atatẹ́tẹ́ tó ti pòfò (Gambler's Ruin problem). Ká sọ pé atatẹ́tẹ́ kan pẹ̀lú owó tẹ́tẹ́ tí kò lópin bẹ̀rẹ̀ ayò láti ìdínwó, pé ó sì ta ayò tì kò lópin láti jẹ owó rẹ̀ padà. A ṣe ìṣirò bóyá yíó jẹ owó rẹ̀ padà, tábí pé bóyá onípìbìtì yíò sáré bá okùn búlọ́kù òótọ́, bí báyìí[8]:

$$
\begin{aligned}
p = &\ \text{ìṣirò bóyá èrọiṣẹ́-ojúpópó olóòótọ́ yíò rí búlọ́kù tó kàn} \\
q = &\ \text{ìṣirò bóyá onípìbìtì yíò rí búlọ́kù tó kàn} \\
q_z = &\ \text{ìṣirò bọ́yá onípìbìtì yíò sáré bá a látí iye búlọ́kù } z \text{ látẹ̀yìn}
\end{aligned}
$$

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

A ti gbà pé $p > q$, ìṣirọ̀ bóyá rẹ̀ ún dín si gidigidi bí iye búlọ́kù tí onípìbìtì náà ní láti sáré bá únpọ̀ si. Pẹ̀lú áìtó yí látì bẹ̀rẹ̀, tí kò bá sorí rere kó fò síwájú láti bẹ̀rẹ̀, kò sí bọ́ ṣe le bá mọ́ torípé yíò mọ fà sẹ́yìn si ní.

Báyìí a wá wo dígbà wo ní ẹni tó gba ìdúnádúrà tuntun yẹ kó dúró kó tó mọ̀ dájú pé ẹni tó fi owó ránṣẹ́ si kó le ṣe ìyípadà ìdúnádúrà náà. A gbà pé ẹni tó fi owó ránṣẹ́ jẹ́ onípìbìtì tó fẹ́ parọ́ pé ohún sanwó tí kò san, tó fẹ́ yi padà láti wá sanwó fún ara rẹ̀ lẹ́yìn tí ìgbà díẹ̀ bá kọjá. Ẹni tó gba owó yíò gba ìkìlọ̀ tí èyí bá ṣẹlẹ̀, sùgbọ́n onípìbìtì náà lérò pé yíò ti pẹ́ jù.

Ẹni tó gba owó dá kọ́kọ́rọ́ tuntun, ó sì fún ẹni tó fowó ránṣẹ́ ní kọ́kọ́rọ́ ìgboro kó tó tọwọ́bọ̀wé rẹ̀. Èyí dínà ẹni tó fowó ránṣẹ́ láti pèsè okùn búlọ́kù sílẹ̀ tẹ̀lẹ̀ nípa síṣẹ̀ṣẹ́ lórí rẹ̀ títí tí yíò fi bọ́ síwájú dáadáa, kó tó wá fẹ́ ná ìdúnádúrà náà nígbà náà. Lẹ́yìn tí ìdúnádúrá bá ti lọ tan, onípìbìtì bẹ̀rẹ̀ iṣẹ́ ní kọ̀rọ̀ lórí okùn búlọ́kù tó ní irú ìdúnádúrà rẹ̀.

Ẹni tó gba owó yíò dúró títí tí ìdúnádúrà yíò fi jẹ́ fífikún sínú búlọ́kù kan, ti iye búlọ́kù z ti so mọ́ ọ lẹ̀yìn rẹ̀. Kò mọ́ ibò ní onípìbìtì ti dé, sùgbọ́n tí a bá gbà pé búlọ́kù òótọ́ gba iye àsìkò tó yẹ fún búlọ́kù kan, ibi tí onípìbìtì yíò ti dé yíò jẹ́ iye ìpínká Poisson pẹ̀lú iye tí kò jọjú:

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

Láti mọ ìṣirò bóyá oníjìbìtì náà sì lé sáré báà báyìí, a ó ṣe ìsọdipúpọ̀ iye iwúwo-kíki Poisson fún ìkọ̀ọ̀kan ibi tó le ti dé pẹ̀lú ìṣirò bóyá ó le sáré báà láti ibẹ̀:

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

Tí a bá ṣe àtúntò rẹ̀ láti mọ́ ṣe aròpọ̀ ìdí rẹ̀ tí kò lópin...

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

Tí a bá yíi sí àmì-ọ̀rọ̀ C…

```
#include
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Ti a bá gbe àwọn èsì díẹ̀ jáde, a rí pé ìṣirò bóyá yíò kéré sí gidigidi pẹ̀lú iye z.

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012
```

```
q=0.3
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Tí a bá sójúùtú fún P tó dín ju 0.1% lọ...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

Òpin

A ti dá àbá síṣtẹ́mù kan fún ìdúnádúnà ẹlẹktróníìkì tí kò gbọ́nkàn le ẹnì kankan. A bẹ̀rẹ̀ pẹ̀lú àpẹẹrẹ pe áwọn owóníná jẹ́ dídá pẹ̀lú Ìtọwọ́bọ̀wé onínọ́mbà, èyí fún olùdáni ní ìjánu tó lágbára, sùgbọ́n kò tó lái sí ọnà dínà ìnáwó-lẹ́ẹ̀mejì. Láti ṣe ìsòro yìí, a dá àbá ẹ̀rọ-aṣeṣẹ́pọ̀ peer-to- peer tó lo ẹ̀rì-ìṣe-iṣẹ́ láti ṣe àkọsílẹ̀ ìtàn àwọn ìdúnádúrà tí ìṣirò rẹ̀ yíò sòro fún oníjìbìtì kan láti ṣe ìyídadà rẹ̀ tí àwọn ẹ̀rọiṣẹ́-ojúpópó olóòótọ́ bá ní àkóso ọ̀pọ̀ agbára CPU. Ẹ̀rọ-aṣeṣẹ́pọ̀ náà lágbára bótilẹ̀ jẹ́ pé kò sóro láti dásílẹ̀. Àwọn ẹ̀rọiṣẹ́-ojúpópó únsiṣẹ́ papọ̀ ní ẹ̀ẹ̀kannà lái sí àkóso. Kò pọndandan kí wọn ó jẹ́ dídámọ̀, nígbà tó jẹ́ pé àwọn ìrànṣẹ́ kò lọ síbì kan pàtó, kò sì sòro láti fi wọ́n ránṣẹ́. Àwọn ẹ̀rọiṣẹ́-ojúpópó le kúrò tàbí kí wọn ó padà bó bá ṣe wù wọ́n, kí wọn ó sì gba okùn ẹ̀rì-ìṣe-iṣẹ́ gẹ́gẹ́bí ẹ̀rí ohun tó ti ṣẹlẹ̀ nígbátí wọn kò sí níbẹ̀. Wọ́n úndìbò pẹ̀lú agbbára CPU wọn, wọ́n fi hàn pé àwọn gba àwọn búlọ́kù gẹ́gẹ́bí èyí tó tọ́ nípa ṣíṣeṣẹ́ lórí wọ́n láti fà wọ́n gùn, kí wọn ó sì kọ búlọ́kù èké sílẹ̀ nípa mí mọ́ ṣiṣẹ́ lórí wọ́n. Àwọn òfin àti ìwúrí le se é gbígbóró pẹ̀lú ònà ìkòẹnu yìí.

References

1. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with

minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

3. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
4. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
5. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.
6. A. Back, "Hashcash - a denial of service counter-measure,"]http://www.hashcash.org/papers/hashcash.pdf, 2002.
7. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
8. W. Feller, "An introduction to probability theory and its applications," 1957.