

Date: 26th September, 2024

By: Cjfrankie and TonyAkins

5.0 Òrò Sàtòṣí Nakamòtò: Bitcoin àti Ìyípadà Àṣírí

Sàtòṣí Nakamòtò, oníṣe ẹdá òhímò-àyé àti òṣùwàdà alágbára, ní àlá fún ìjòwọ̀ ojọ̀ iwájú níbi tí ìṣètò ìnàwó yóò di ẹ̀ni-gbàlẹ̀mọ̀, ìmọ̀lẹ̀ àti ìdánílójú—nílẹ̀ fún ìdíyelé ijọba àti àwọn ilé-ifowópamọ̀. Ní ọdún 2008, Sàtòṣí dàgbára ìyípadà òmìnira pẹ̀lú àkọ̀sílẹ̀ funfun Bitcoin. Ó ṣàlàyé ìmúlò àkókó tí ó ṣeéṣe fún ìmọ̀lẹ̀ ìmọ-ẹ̀rọ blockchain. Bitcoin dide gégé bí àmì ìrètí àti ìdààmú ní ayé tí àjàlù ìnàwó àti ìfòrònà ìgbẹ̀kẹ̀lé nínú àwọn ìgbésí ayé àwọn ilé-ẹ̀gbẹ̀ tí wọ̀lé. Ìgbésí ayé Bitcoin àkókó ṣẹ̀lẹ̀ ní oṣù Kínní ọdún 2009. Tí ó jẹ̀ mímúlọ̀ fún ìfẹ̀ láti dá ètò ìnàwó tí a kò dá lórí àwọn ètò aráàkó, Bitcoin Sàtòṣí gbé agbára pada sí àwọn ènìyàn, tí ó mú kí ìwàláàyé ayé gbogbo bẹ̀rẹ̀, tí ó ṣàtakó sí ìmúlò tó ti pé àti dásílẹ̀ àwùjọ̀ tí ó gba òmìnira ìṣètò ìnàwó.

5.1 Ìfìyèsí sí Bitcoin àti Zcash

Ní ọdún méje léhìn náà, ní ọdún 2016, ẹ̀gbẹ̀ àwọn onímọ̀ àti oníwádìí dá Zcash. Ètẹ wọn ní láti ṣètò òmìnira itòyẹ̀ tí Bitcoin Sàtòṣí dá sílẹ̀, ní pàtàkì nípa fífún un ní àwọn ìbèrẹ̀ àṣírí. (Àwọn àlàyé síwájú wà nípa èyí.) Zcash jẹ̀, ní otitọ̀, ètò tí ó ya sọtò láti Bitcoin, èyí tó túmọ̀ sí pé wọn kó kóòdù Bitcoin, wọn sì ṣe àtúnṣe. Èrò fún Zcash jẹ̀ àkókó tí wọn ṣàpẹ̀júwe nínú àkọ̀sílẹ̀ funfun tí wọn tẹ̀ jáde ní ọdún 2014 láti ọ̀dọ̀ àwọn àwọn òjìṣẹ̀ ojọ̀ wá nínú ilé-ẹ̀kọ̀ MIT, Johns Hopkins University, Technion, àti Tel Aviv University, tí wọn sì dáá ní ìgbà tí ó tó ọdún pẹ̀lú ẹ̀gbẹ̀ Zooko Wilcox-O'Hearn ní Electric Coin Co. (ECC; táńkálẹ̀ ní ilà ní Zcash Company).

Àwọn ènìyàn ló ZEC láti ṣe ìṣètò ìnàwó pẹ̀lú àìfọ̀yemọ̀ àti ní ìdánílójú, pẹ̀lú owó ìsúnàkò. Ó jẹ̀ ẹ̀ni-gbàlẹ̀mọ̀, yára, tó ní ànfààní, ó sì wà fún gbogbo ènìyàn—tí a kò fún ojọ̀ ori díjítàlì. Ẹ̀ lẹ̀ ló ó láti rà ohunkóhun, láti ọ̀mọ̀ duńdún títí di ìrìn-àjò sí etí òkun. Ẹ̀ lẹ̀ ló fónù alágbèéká yín láti san owó sí ọ̀rẹ̀ yín nínú Zcash ní àìmọ̀, fi owó ranṣẹ̀ sí òkèèrè, rà ounjẹ̀, tàbí fi owó ṣetí ẹ̀bun fún ìṣẹ̀ kan tó dáa. Ẹ̀ lẹ̀ ló àwọn ohun èlò ẹ̀gbẹ̀-ẹ̀kẹ̀ta bí Flexa SPEDN láti sanwo pẹ̀lú Zcash ní Lowe's, Nordstrom, Baskin Robbins, àti ọ̀pọ̀ èlò miíràn. Àwọn ìṣẹ̀ bí Moon nífẹ̀rí ó jẹ̀ kí ẹ̀ lẹ̀ ló Zcash ní ayélujára níbi gbogbo tí wọn bá gba Visa.

5.1.1 Kí ní Bitcoin? Kí ní Zcash?

Bitcoin (BTC) jẹ̀ irú owó ẹ̀lẹ̀trónìí tí ẹ̀nikẹ̀ni lẹ̀ fi ranṣẹ̀ àti gbà lórí nẹ̀tíwọ̀kì Bitcoin. A lẹ̀ fi Bitcoin pamọ̀ sínú apamọ̀wọ̀ díjítàlì, lórí fónù alágbèéká tàbí kọ̀ńpútà, tí ó n ń sí àkọ̀sílẹ̀ tí a pin

káàkiri. Ronú nípa rẹ̀ bii àtòtọ̀ akọsilẹ̀ nlá lóri ayélujára, tó jẹ́ tí gbogbo èniyàn lè wọ́le sí, níbi tí gbogbo ìṣètò ináwó ti jẹ́ iwólé.

Bí Bitcoin, Zcash jẹ́ owó díjítàlì, tó dá lóri orísun-sìsì, lẹ̀dàà tí ó da lóri ikànsí akọsilẹ̀ (blockchain), ṣùgbọ́n ní itọ́kasí Bitcoin, Zcash ní ètò ijádúró-ẹ̀rí àìmọ̀ tó gíga, tó daabobo akọsilẹ̀ kúrò nínú jìbítì, tí ó sì jẹ́ kí àwọn oníṣe owó lè tìkára wọn dáabobo àwọn akọsilẹ̀ ìṣètò ináwó wọn.

5.1.2 Kí ni iyàtò láàárín Zcash àti Bitcoin?

Ọ̀nà tí ó rọ̀rùn láti ṣàlàyé Zcash ni pé ó jẹ́ owó díjítàlì bii Bitcoin, ṣùgbọ́n ó daabobo àsírí àwọn oníṣe rẹ̀, dipo láti ṣàfihàn ìtàn ìṣètò ináwó wọn. Nígbà tí Bitcoin jáde ní ọ̀dún 2009, ó jẹ́ owó díjítàlì tí kò ní ilàna àárín àwọn ilé-ẹ̀gbẹ́ fún ìṣètò ináwó àkókọ̀. Gbogbo àwọn ìṣètò Bitcoin ni wọn fi àfihàn, wọn sì jẹ́ iwólé ní blockchain, akọsilẹ̀ tó gbàgbára, èyí tí ó túmọ̀ sí pé ẹnìkẹ̀ni lóri ayé lè rí àwọn àkọjó ìṣètò ináwó àwọn èniyàn àti iwòkànsí ináwó wọn. Àìní àsírí yìí ni ohun tí wọn fọ́júkò sí nípa bí àwọn onímọ̀ Zcash ṣe pinnu láti dá ohun tí ó dára síi, ní ọ̀dún 2016, àwọn àgbà-imọ̀ nínú ìmọ̀ye àsírí náà gba kóòdù orísun-sìsì Bitcoin wọn sì ṣe àfikún àwọn ẹ̀rí àìmọ̀ (zero-knowledge proofs) láti dá Zcash.

Zcash fúnni ní gbogbo irọ̀rùn tí Bitcoin fúnni, ṣùgbọ́n pẹ̀lú ààyè ifimọ̀ patápátá láti daabobo ìtàn ìṣètò ináwó àwọn oníṣe rẹ̀. Òmíràn iyàtò pàtàkì wà, bíi ètò tí ń ṣètò fún idàgbàsókè Zcash, àkókò idánilójú tí ó kù diẹ̀, ilẹ̀ imọ̀ra àsírí nínú akọsilẹ̀, ìṣètò tí ó yára, àti ọ̀pọ̀ èlò miiran.

5.1.3 Kí nìdí tí ó fi yẹ́ kí a kọ́ nípa Zcash?

Zcash fún àwọn èniyàn ni àhààní láti fi owó ẹ̀lẹ́trónì àti àwọn àlàyé miiran ranṣẹ́ ní àìmọ̀ àti láìní ilàna, láìsì olùdájọ̀ bí ilé-ifowópamọ̀ tàbí ilé-ẹ̀kọ̀ ijoba. Nípa ní ètò owó tó jẹ́ ẹ̀ni-gbàlẹ̀mọ̀, ibáṣepọ̀, àti láìní ilàna, Zcash ń fún àwọn èniyàn ní agbára láti pa owó wọn àti ṣe ìṣètò pẹ̀lú àwọn miiran, láìkòṣàrà kankan àfihàn àwọn ilé-ẹ̀gbẹ́ tí a ṣe àfihàn tí ó ń jẹ́ ipamọ̀ tàbí owó ìsúnàkò. Zcash ń fún àwọn èniyàn ní òmìnira láti yan bóyá kí wọn máa sọ ìtàn nípa àwọn ìṣètò ináwó wọn pẹ̀lú àwọn miiran.

Zcash dá àṣìṣe tó tóbi jùlọ̀ ti Bitcoin lọ: Ìní àsírí àti ibáṣepọ̀ data. Ní ayé kan níbi tí àwọn ohun elo blockchain àti awọn owó ẹ̀lẹ́trónì ti ń gba àyípadà, àwọn ìṣètò àìmọ̀, bíi ti Bitcoin, kò sí ní àṣàyàn tó dáa mọ̀ láti daabobo àsírí àwọn oníṣe. Àwọn ohun elo àkúnya ń di alágbara jùlọ̀ ní gbogbo ọ̀jọ̀, wọn sì ti wa ni àfihàn pupọ̀ nipasẹ̀ àwọn èniyàn àti àwọn ilé-ẹ̀gbẹ́ láti ṣe àyẹ̀wò àti tọ́pa àwọn ìṣètò blockchain.

5.1.4 Kí ni n fún Zcash ní iye rẹ?

Àwọn èniyàn lè ló ZEC láti pa ìṣúra sínú ohun-ini tó lagbara, tí ó n daabobo àsírí. Kí í ṣe láìkòṣàrà yóò wà 21 milionu ZEC, tó tùmọ sí pé ohun-ini yìí ní ipò tó pèlú. Nígbà tí ZEC 21 milionu bá ti yò sílẹ̀, ohun-ini yìí yóò di ohun-ini tó kópa lórí àìdà owó. Àwọn ohun-ini tó kópa lórí àìdà owó jẹ̀ àpẹẹrẹ rere lórí àìdà ìsúnàkò nígbà tí àwọn olùdájọ́ aráàkó bá n pèyà owó àgbàlagbà orílẹ̀-èdè. Zcash ti ní àtúnṣe tó péye láti ikànsí nẹ̀tíwọ̀kì rẹ̀ ní ipèyà 2016, tí ó sì n bá a lọ pèlú ànfààní fún àwọn olùṣàkóso blockchain àti àwọn olùdàwò àìmọ̀ nínú àdúgbò àjà. Àwọn ẹ̀rí àìmọ̀ zk-SNARK ti ràn wọn lọwọ́ láti ṣètò àyípadà àsírí fún ìmúlò tí a dá lórí blockchain nínú ọ̀jà àgbáyé. Àwọn oníṣe tó yàtò síra àti àwọn oníbààrà ilẹ̀-ìṣẹ̀ bẹ̀ẹ̀ nífẹ̀ẹ̀ àfihàn ìmọ̀, ànfààní, àti ìṣàkóso tó dára ti Zcash.

5.1.5 Kí nìdí tí ó fi yẹ kí n ṣe àkíyèsí?

Zcash fún àwọn èniyàn ní ànfààní láti ṣe ìṣètò níta àwọn ètò aráàkó tó lè ṣe àfihàn ìtàn wọn àti/ tàbí ṣe àyíká àwọn èniyàn, àti láti sọ ìtàn nípa ìṣètò ináwó wọn pèlú àwọn mīràn tàbí láti pa àlàyé yìí sílẹ̀. Ẹ̀rọ ìsanwó ẹ̀lẹ̀trónìí tí kò ní ìlànà yìí n daabobo òmìnira èdè àti òmìnira ibáṣepọ̀—pèlú òmìnira láti jẹ̀ èniyàn, jẹ̀ àbẹ̀rẹ̀, tàbí jẹ̀ ohun tí wọn fẹ̀! Àwọn oníṣe Zcash lè fi owó ranṣẹ̀ sí àwọn àjọ, fi owó ranṣẹ̀ sí òkèèrè, tàbí kan fi ranṣẹ̀ sí ọ̀rẹ̀, láìfi ìdánílójú wọn hàn àti láì ní ibànújẹ̀ pé kì yóò jẹ̀ kí wọn ní ìgbàlà. Pèlú pé Zcash ní ipò tó pèlú 21 milionu, bíi Bitcoin, àwọn oníṣe lè ní ìdánílójú pé ZEC wọn kì yóò ní owó tó kù sílẹ̀ nípa ẹ̀gbẹ̀ aráàkó kan tí n tẹ̀síwájú láti ṣe ìdàgbàsókè síi.

5.2 Kí ni Zcash jẹ?

Zcash fún àwọn ọ̀ṣùwóní ní àṣàyàn méjì fún ìṣètò owó: ifẹ̀hàn (tí ẹ̀nikẹ̀ni lè rí) àti ètò àyédá (tí a fi pa mọ̀). Méjèèjì ní a n ṣe lórí ayélujára Zcash kan náà, ṣùgbọ́n bí àwọn iyè àti ẹ̀rí owó ṣe n ṣiṣẹ̀ yàtò ní ọ̀nà. Látara ètò àyédá, Zcash n lo nnkan kan tí a mọ̀ sí zero-knowledge proofs láti pa ìṣètò náà mọ̀. Ní pàtàkì, Zcash n lo zk-SNARKs, irú zero-knowledge proof kan. zk-SNARK tùmọ̀ sí "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge," ó sì n tọka sí ìlànà ẹ̀rí tí ẹ̀ni kan lè fi dájú pé ó ní ẹ̀kúnrére ìmọ̀ nípa nnkan kan, bí àpẹẹrẹ̀, kó ṣe ifihàn bíi bọ̀tì bí wọn ṣe ní bọ̀tì àkòkò ní ọwọ́ rẹ̀, láì fihàn ìmọ̀ náà tàbí síbí èyí tí o wa, àti láìsí àpapọ̀ àjọṣe láàrin ẹ̀ni tó fẹ̀ fi dájú àti ẹ̀ni tí ó n fẹ̀ fi ẹ̀rí hàn. Ní ṣiṣe lóníí, zero-knowledge proof jẹ̀ ọ̀nà

àkòlẹ̀ ẹ̀dà tí ó lè fi ìbòyè hàn láìfihàn ìmò náà tí ó mú kí ó rí bẹ̀ẹ̀. Bí àpẹẹrẹ̀, ní Zcash, nígbà tí ẹnìkan bá ń ẹ̀ ẹ̀sètò owó, zero-knowledge proof n ẹ̀sẹ̀ láti jẹ́ kí ó dájú pé ẹnì tó ń fi owó sílẹ̀ ní owó tó pé lài ẹ̀ ẹ̀dí ohun tí ó wà nínú àpótí rẹ̀ fún ẹnìkẹ̀ni.

Báwo ni àwọn Zcash tuntun ẹ̀ ń wọ́lé sí nẹ̀tìwọ̀kù?

Ipele owó Zcash jẹ́ 21 million ZEC ní gbogbo iye rẹ̀. Ní gbogbo ọ̀sàwákiri 75 ọ̀sẹ̀jú-àáyá, a ń ẹ̀ àwọn ẹ̀sẹ̀ tuntun sí ayélujára Zcash àti àwọn ẹ̀rẹ̀ ẹ̀sẹ̀ jẹ́ 3.125 ZEC, tí wọn fi ń wọ́lé sí ìbẹ̀rẹ̀ ayélujára. Ẹ̀rẹ̀ ẹ̀sẹ̀ yìí yí ká lọ súnkẹ̀rẹ̀súnkẹ̀rẹ̀ lásìkò ọ̀pọ̀lọ̀pọ̀ ọ̀dún, tí àwọn ZEC kan gbogbo náà bá ti jẹ́ kí wọn wà nígbà gbogbo. Ìlẹ̀mọ̀ ẹ̀nu owó Zcash jọra gan-an pẹ̀lú ẹ̀ya Bitcoin. Ẹ̀yẹn tùmọ̀ sí pé nígbà tí owó tuntun bá ti jẹ́, ìlẹ̀mọ̀ náà pòkàdà lówó lówó, àti nígbà tí wọn bá ẹ̀ e ní kẹ̀rìn-kẹ̀rìn, ọ̀sẹ̀lẹ̀ náà wà kí ó gbé.

Ìfihàn sí ẹ̀sẹ̀ ọ̀fẹ̀hàn Zcash

Àdírí owó Zcash àyédá máa ń dàabò bo àwọn ọ̀tọ̀jú owó rẹ̀. Àdírí owó tí a fẹ̀hàn máa ń ẹ̀ àwọn àkójọpọ̀ àkànṣe náà sígbàgbé. Ẹ̀ ẹ̀ àbàjọ lórí ọ̀rọ̀ tí ẹ̀ ń lòka, o si jẹ́ aláírí, ó ń gbé àwọn ọ̀giri tán. Ẹ̀wọ̀ kò mò bí àwọn mejì náà jẹ́ àwọn awọ kanna, tàbí àwọn tó yatọ̀ síra. Ẹ̀wọ̀ sì fìkan kán án fún ẹnì tí ó ń bá ọ̀ ẹ̀ ajoṣe, ẹnì kan tí kò ní gèé. Ó sọ ohun tó ní nípa awọ rẹ̀. Ẹ̀wọ̀ kò mò bí ó ń ẹ̀ ọ̀ótọ̀ bí kòṣe, sùgbọ̀n síígbà, ẹ̀wọ̀ ti gbé e nípa kí o rí ọ̀nà láti bọ̀ àwọn kámẹ̀ra yìí sún mọ̀ra, tàbí pé o fẹ́ tún ún ẹ̀ ẹ̀sẹ̀yìn, tí ó tún gbé e síwájú láti tún gbé àwọn ọ̀fẹ̀hàn owó náà sọ lójú.

5.2.1

Ipele owó Zcash jẹ́ ipò tó ẹ̀dédédé tí ó jẹ́ 21 milionu ZEC ní gbogbo iye rẹ̀. Ní gbogbo ọ̀sẹ̀jú-àáyá 75, a máa ń sá wàdádá tuntun sí ayélujára Zcash, tí ẹ̀rẹ̀ ẹ̀sẹ̀ 3.125 ZEC sì ń wọ́lé sí àtìpá. Ẹ̀rẹ̀ ẹ̀sẹ̀ yìí ni a máa pín fún àwọn onísáwàáda àti àwọn ináwo ètò ọ̀dàgbàsókè Zcash. Ẹ̀yọ̀ndà ẹ̀rẹ̀ ẹ̀sẹ̀ yìí máa ń dínkù ní ọ̀dún mẹ̀rìn-mẹ̀rìn títí gbogbo 21 milionu ZEC bá ti wọ́lé sí àtòjọ. Ìlẹ̀mọ̀ ẹ̀nu owó Zcash máa ń sàpẹẹrẹ̀ ti Bitcoin gan-an. Ó ẹ̀ pàtàkì láti mò pé bí àwọn owó tuntun ẹ̀ ń dá wá, ìlẹ̀mọ̀ náà ń kúrò, tí nígbà gbogbo ẹ̀kọ̀kan àwọn ọ̀dínákọ̀nà yìí bá ẹ̀lẹ̀, o máa ń ẹ̀bu gidigidi.

5.2.2

Àdírí Zcash àyédá máa ń dàabò bo àwọn ináwọ̀ rẹ̀ lórí ọ̀sètò owó, kí àwọn ètò ọ̀fẹ̀hàn ẹ̀ gbogbo àkójọpọ̀ ináwọ̀ rẹ̀ fún gbogbo ẹnìyàn láti rí.

Ẹ jẹ kí ó ẹ̀ ẹ̀lẹ̀rònàjìnká fún ìgbà diẹ pé a ti fi ìbojú pọ̀n ọ, ó sì jẹ pé o n di àwọn ètò owó méjì lẹ̀hìn ẹ̀hìn rẹ. O kò mò bí wọn jẹ àwọn tó ní iyàtò tàbí àwọn tí ó jọra. O fi ọ̀kan hàn fún ẹ̀ni tí kò ní ìbojú, ó sì sọ fún ọ̀ nípa awọ náà — sùgbọ̀n iwọ kò mò bí ó n sọ ọ̀ótọ̀. O sì tún gbé e sí ẹ̀hìn rẹ padà — bí o bá yí àwọn nnkan náà tàbí kò yí, ó sì jẹ kí o tún ẹ̀ ẹ̀yẹ̀wò. Nígbà tí o bá n ẹ̀ e lẹ̀pẹ̀lẹ̀pẹ̀ ìgbà, iwọ lè bèrẹ̀ sí ní gbéka pé ẹ̀ni náà n sọ ọ̀ótọ̀ tàbí òdì. Bí àpẹẹrẹ, tí o bá gbé ẹ̀yí náà jáde lẹ̀ẹ̀mejì, ó sì sọ fún ọ̀ pé "dúdú" ní ìgbà àkókó, àti "pupa" ní ẹ̀kejì, o ti mò pé ọ̀ n purọ̀. Bí àwọn idáhùn rẹ bá fara dajú pẹ̀lú ohun tí o mò nípa ohun tí o n fihan, iwọ máa ní ìgbàgbọ̀ tó láti mò bí ó n sọ ọ̀ótọ̀ tàbí òdì. Ẹ́dà bíi ẹ̀yí lè ẹ̀ amíbo àwọn idílẹ̀ àkólé inàwó tó ẹ̀ púpọ̀ jù lọ tí wọn kii sínì ilàna dídúró (bí ilò SNARKs alágbára láti dáabò bo Merkle root fún ipin ayélujára; sùgbọ̀n ẹ̀yí kojá àkíyèsí iwé yìi).

Ọ̀pọ̀ àwọn ayélujára inàwó máa n fihàn gbogbo ìṣètò àti iyè ìṣura ní gbangba fún gbogbo ẹ̀niyàn. Ẹ̀yí kii í ẹ̀ ifòkànbalẹ̀ tàbí àṣírí, ó jẹ gbòdò gbòdò ni bí wọn ẹ̀ ẹ̀ àtúnṣe wọn. Bí o bá n ṣètò inàwó pẹ̀lú àwọn ètò Zcash àyédá, iwọ máa ní ìṣàkóso kára kára lórí àwọn ìṣura rẹ, ó sì lè dáabò bo àwọn rẹ lójú àwọn ẹ̀ni tí wọn ní èròburúkú tàbí àwọn oníjòṣéburúkú. Nígbà tí o bá rán Zcash kúrò ní àpótí inàwó rẹ, iwọ yóò rí ibáṣepọ̀ rẹ tí ó jẹ pẹ̀lú àwọn àkójọ àwọn nọmbà àti lẹ̀tà. Ẹ̀ni tí o bá n rán sí náà tún máa ní ibáṣepọ̀ náà pẹ̀lú àkójọ àwọn nọmbà àti lẹ̀tà. Tí àdírí rẹ bá bèrẹ̀ pẹ̀lú "z," tí iwọ sì n rán owó sí ẹ̀ni tí àdírí rẹ tún bèrẹ̀ pẹ̀lú "z," o lè ní ifẹ̀hàn pé gbogbo ìṣètò náà sì dábo bo níká. Iyè ipín owó àti àwọn àdírí ìṣètò àwọn àpótí owó méjì náà ti wa ní àyédá lórí ayélujára. Ẹ̀yí jẹ ọ̀nà tó dára jù fún rírán àti gbígbà ZEC nígbà tí ipamọ̀ bá jẹ pàtàkì.

Nígbà tí o bá rán owó kúrò tàbí gbà owó ní àdírí tí o bèrẹ̀ pẹ̀lú "t," iyẹn, ìṣètò z-sí-t tàbí t-sí-z, ipamọ̀ náà kii ẹ̀ pé o tóbi, bí àwọn ilò bá yè wá níká ní ayélujára. Ìṣètò t-sí-t jẹ gbangba pátápátá, bíi àwọn ìṣètò Bitcoin. Àwọn oníṣe Zcash náà yóò tún rí àwọn àdírí tí o bèrẹ̀ pẹ̀lú "u." Wọn n pè àwọn wònyí ní unified addresses, wọn sì n ṣiṣe bíi universal travel adapter. Pẹ̀lú unified addresses, àwọn àpótí owó lè gba àdírí àwọn owó sí shielded pool tuntun. Ní àpẹẹrẹ, ẹ̀ jẹ kí o gbà Zcash kan nínú ilé ayélujára. Ilé ayélujára náà lè rán Zcash tí o jẹ ifẹ̀hàn kúrò ní t-address sí unified address rẹ. Sùgbọ̀n tí àpótí owó rẹ bá ní autoshielding, o máa yí àwọn owó wònyí padà sí ibi ipamọ̀ láì ẹ̀ ẹ̀yí kankan.

***Àwọn irú adireesi Zcash Ní báyií, àwọn irú adireesi méta ni wọn n lò títí di òní.
Ẹ̀yí ní àwọn wònyí:***

TYPES OF ZCASH ADDRESSES

Currently there are three main types of addresses in use to date. These include

TRANSPARENT

tlgoiSyw2JinFCmUnfiwwp72LEZzD42TyYu



SAPLING

*zslcpf4prtmnqpg6x2ngcrwelu9a39z9l9lquk
q9fwagnaqrkn k34a7n3szwxpjuxffdxkuzyl53*



UNIFIED ADDRESS (FULL) IMAGE PLACEHOLDER

*ulckeydud0996ftppqrnpdsqyeq4e57qcyjr4raht4dc8j3nju
yj3gmm9yk7hq9k88cdkqfuqsgpcpjfhwu3plm2vrd32g8du78k
zkm5un357r4vkhz4vhxd4yfl8zvszk99cmssc89qv4trd7jzks8
h6lukzgy25j8cv76p0g603nrrg6yt6cxsh2v8rmkasskd69ylfy
phhjv0cxs*



FOR MAXIMUM PRIVACY, ALWAYS USE Z- OR U-ADDRESSES.

FÚN ÌPAMỌ TÓ PÈKỌ, MÁA LÒ ÀWỌN ADIREESI Z- TÁBÍ U- NÍGBÀ GBOGBO ÌGBÀ

5.2.3

Báwo ni blockchain ẹe máa n tópa ẹni tó ná Zcash? Igi idánimọ àṣírí tàbí igi Merkle jẹ pípèlú àwọn ẹka àti àwọn nòdì ewé tí wọn ní àfihàn àṣírí cryptographic ti àkọsílẹ̀ ètò data kan. Àwọn igi Merkle jẹ àpẹrẹ̀ ti ètò idánimọ cryptographic. Gbòngbò igi náà ni wọn kà sí idánimọ tó dájú, tí àwọn nòdì ewé sì jẹríí pé wọn jẹ apá kan ti idánimọ ìbẹ̀rẹ̀ náà.

Wọn máa n fidí data tí wọn fipamọ tàbí rán lóri àwọn ẹgbẹ P2P náà múlẹ̀, ní dàkúdájú pé àwọn data tí wọn gbà láti ọdọ àwọn ẹlẹgbẹ kò ní àtúnṣe. Ní ikòtún àpamọ òrùlẹ̀ ZcashSapling àti Orchard, Ìtélẹ̀ Idánimọ (Note Commitment Tree) ni wọn máa n lò láti

fidí àwọn ìmúnisìn lésè múlè gégé bí òfin ibámu nígbà tí wọn bá dáa bo ẹni tó rán, ẹni tó gba, àti àwọn iye tí wọn ná pátápátá.

5.2.4 Šé àwọn ìmúnisìn Zcash jé ààbò?

Bèèni. Ètò Zcash lè jé kí a kà á sí pé ó dáàbò bo gégé bí ó ti jé ọkan lára àwọn ètò ìsanwó àṣírí àìmò tó dájú jùlò ní ayé. Ó ti jé àtúnṣe nipasẹ ọpọlọpọ ànfààní crypto tó tóbi bíi Namada àti Penumbra. Ní àfikún, ó ti ṣe àwárí ààbò púpọ lori àwọn apamọ àti àwọn eroja àṣírí cryptographic tó wà nínú àwọn oja tí Zcashers n ló.

5.2.5 Jé kí n fa ọ lẹnu iṣẹ ìmúnisìn abi Ìṣòwò Zcash kan

- Dáàbò bo pé apamọ rẹ ti ni ìbáṣepọ pẹlú àgbègbè àtúnṣe tuntun.
- Tí ó bá ti ni ìbáṣepọ pẹlú, o lè ní ìdániloju pé ìkànsí rẹ jé tuntun pẹlú gbogbo iye tó le na.
- Tẹ adireesi aṣọkan ti olugba rẹ sí inú àkọsílẹ “adireesi.” Tí o bá fẹ, kọ adireesi náà sílẹ láti inú ìkànsí rẹ tàbí ṣe àyèwò kóòdù QR ti ẹlẹgbé rẹ.
- Fẹgbé iye tí o fẹ rán; owó tí yóò rán ni a máa ṣe àfihàn laifowọsí.
- memo aṣọkan pẹlú ìmúnisìn rẹ. Rántí: Àwọn adireesi ifẹhàn kò lè gba mémọ.
- Dáàbò bo ìmúnisìn náà àti lehinna tẹ "rán.
- Àkókò bulọọki Zcash ni 75 ìṣẹjú-aaya, ó lè gba 1-2 ìṣẹjú fún olugba láti gba ìkilò owó tó n bọ. Gégé bí iye àfihàn tó yẹ kí apamọ olugba rẹ ní, wọn lè ní láti dúró de láti lè na Zcash náà.

5.2.6 Iṣẹ: Àwọn ìmúnisìn Abi Isowo Zcash nínú iṣe

Láti gbìmò pọ láti yíyí Zcash pẹlú ọrẹ, tẹlé àwọn ìgbésẹ wònyí:

1. Gbogbo yín yẹ kí ẹ ṣètò apamọ Zcash.
2. Ní apá "Rán," ṣe àyèwò kóòdù QR ti adireesi ọrẹ rẹ tàbí tẹ adireesi U tàbí Z
3. wọn.Rán mémọ, pé: "Báwo, kaabọ sí Zcash."

5.2.7 Šé Zcash lè dawó dúró?

Bée ni. Zcash jẹ àtẹjádé ìsanwó ìkàniyàn àìlera ti a ẹ pẹlú àìmòná àkókó, tí àwọn èniyàn ní gbogbo agbáyé nšìşé.

Sofitiwia node jẹ ọfẹ àti orisun şìşì. Kò sí ìjọba ààrẹ kan tí ó nípa nínú ìtẹwógbà ìmúnisìn Zcash.

Ní tòótó, nítorí ìkànsí ìpamọ Zcash, ó dájú pé ó jẹ àtẹgùn sí ìgbìmọ láti da nẹtíwọ̀kì dúró.

5.3 Taa ni Tani ati Kin ni Kin ni Ni Zcash Ni Agbaye?

Electric Coin Co. (ECC) Electric Coin Co. (ECC) ni ile-işẹ ti o şeda ati tu owo oni-nomba Zcash silẹ ni ọdun 2016. Loni, ECC, ni afikun si awọn ẹgbẹ ominira ati awọn oludasilẹ miiran, n tẹsiwaju lati ẹ atilẹyin agbegbe Zcash nipasẹ idagbasoke oja, iwariiri ati gbigba, ati ọpọlọpọ awọn iru iwadi. ECC jẹ olokiki gẹgẹ bi ọkan ninu awọn ẹgbẹ cryptography ti o lagbara julọ ni agbaye. Ni ọdun 2016, o jẹ akọkọ lati ẹ aseyọri ilowosi imọ-ẹrọ cryptography zero-knowledge ni ohun elo gidi (Zcash), ati ni ọdun 2022, awọn onimọ-ẹrọ ECC ẹ awari Halo, ọna idaniloju zero-knowledge ti o yipada, ti o funni ni ikọkọ blockchain ti o daju ni igba akọkọ, ati ilọsiwaju scalability. Awọn ẹgbẹ mewa lo wa lori ọpọlọpọ awọn işẹ ominira ti n şìşẹ lati ẹ imuse Halo ninu awọn ifilọlẹ wọn.

Zcash Foundation (ZF)

Ile-işẹ Zcash (ZF) jẹ ajoye alaanu 501(c)(3) ti o kọ ile-işẹ ikọkọ inawo fun igbadun gbogbo eniyan, ni akọkọ ti n şìşẹ fun awọn olumulo ti ilana Zcash ati blockchain. Wọn, ni afikun si awọn miiran, n şìşẹ lati rii daju pe ilana Zcash ati nẹtiwọ̀kì şìşì ti o n şìşẹ rẹ wa ni idasilẹ ati orisirisi. Diẹ ninu awọn ilowosi imọ-ẹrọ pataki ti ZF si ẹka naa ni idagbasoke Zebra, nodi Zcash ti ode oni, ati FROST, ilana aşekagba. Ile-işẹ naa tun n şeto Zcon, apejọ ọdun kan ti o dojuko imọ-ẹrọ ikọkọ ati eto Zcash, ati atilẹyin awọn işẹ agbegbe ipilẹ gẹgẹbi Zcon Vozes, Ẹgbẹ A/V ati ọpọlọpọ awọn ipe agbegbe şìşì miiran ati AMAs. Ni afikun, Ile-işẹ naa n gbe Zcash siwaju nipa ifowosowopo si ọpọlọpọ awọn işẹ ni eto Minor Grants rẹ, awọn işẹ iwadi inu ati ita, ati pese atilẹyin işakoso fun Zcash Community Grants (ZCG).

Zcash Community Grants (ZCG)

Zcash Community Grants (ZCG) n funni ni atilẹyin si awọn işẹ ti o n mu ilọsiwaju si lilo, aabo, ikọkọ, ati gbigba Zcash. ZCG jẹ igbimọ imọran imọ-ẹrọ ti o jẹ apakan ti Ile-işẹ

Zcash, labẹ awọn ofin rẹ. Awọn agbanisise ni a yan nipase igbimọ ti awọn omọ egbe marun ti a yan nipase Igbimọ Igbimọ Agbegbe Zcash.

Iṣe akanṣe to ṣeṣe ti a ti fowosi nipase ZCG ni:

- *Zcash Shielded Assets (ZSA) ti o jẹ oludari nipase egbe QEDIT, ti o mu DeFi wa si Zcash pẹlu ilana isanwo tuntun ti o fi kun awọn ẹya afikun si mainnet.*
- *Iwe aiyede kukuru ti Zcash Media ti o fihan awọn Zcashers ti o ni akiyesi gege bi Edward Snowden, Zooko Wilcox, ati Deirdre Connolly.*
- *Ilana isanwo ati eto Point-of-sale ti o rọrun ti o ni bọtini kan fun awọn ile itaja ti o wa ni ile, ti ZGo n ṣe.*
- *Eto Agbaye Ambassador, eyiti o ṣe iranlọwọ fun Zcash lati ni aṣoju jakejado agbaye.*

ZecHub

ZecHub jẹ ile-iṣe ẹkọ orisun ṣiṣi ti o dojukọ Zcash, pẹlu agbegbe ti o ni awopọ ti awọn oluranlọwọ ti o tẹjade awọn ẹya, awọn iwe iroyin, awọn bulọọgi, awọn itọsọna, awọn ikede, ati diẹ sii.