Bitcoin eta Troika: ideologia non-nahi

1 Kriptomonetak: inbertsiotik haratago

Azken aldian kriptomonetak inbersio tresna oso garrantzitsuak bihurtu dira, gazte askok "Cryptobro" mugimenduarekin liluratuta dirua irabazteko modu azkartzat jo dituztelako (1 irudia).

1. Irudia: Cryptobro mugimenduaren erakusle den "Wall Street Wolverine" eta Iván Espinosa de los Monteros Vox-eko politikaria. (elespanol.com).

Espekulazio burbuila guztiekin gertatzen den legez, kriptomoneten burbuilak eztanda egin du eta kriptomoneta askoren balioek beherakada nabarmena pairatu dute, Bitcoin-ena barne. Hedabide askok gainbehera honek eragindako galeren berri eman dute. Garrantzitsuak izanagatik, berri horiek kriptomoneten alde bakarra erakusten dute: kriptomonetak inbertsio tresna moduan. Baina kriptomonetek badaukate beste funtzio are garrantzitsuagoa: balio elkartrukea bideratzea, alegia zerbitzuak eta produktuak erosteko balio duen diruaren funtzioa betetzea.

Zer da dirua? Zein da gizarte batentzako dirurik hoberena? Ekonomilariak galdera hauei mendeetan zehar erantzuten saiatu dira. Bitcoin-en sortzaileak ere bazuen bere erantzuna, Bitcoin protokoloaren diseinuan gauzatutakoa. Kriptomonetaren batek aurrera egingo badu Bitcoin izango dela kontutan hartuta,

garrantzitsua da jakitea zein ideia dauden bere atzean, balitekeelako etorkizuneko gizarteko moneta Bitcoin-a izatea.

2 Diru sendoa eta inflazioa

Historian zehar dirua mekanismo ezberdinekin inplementatu da, baina gehien erabilia urrea izan da. Zergatik? Urria eta lortzeko zaila delako: eskasia horrek faltsuztapenak zailtzen ditu, eta ekonomiaren benetazko aberastasunaren adierazle bihurtzen dute (Urrearen meatzaritza oso nekeza da, mozkin-marjina oso txikiarekin).

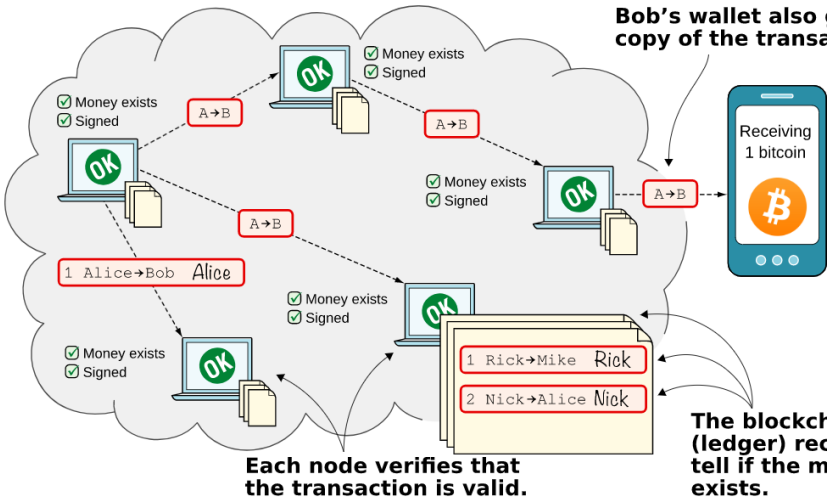
Urre-patroia deritzon diru-sistema 1970. hamarkada arte oso erabilia izan zen estatu askotan. Sistema horretan, estatu bakoitzaren banku zentralak urrea gordetzen zuen, eta jaulkitzen zuen diru-paper unitate bakoitza urre kantitate finkoaren baliokidea zen. Alegia, edozein hiritar banku zentralera joan ahal zen bere monetak urreagatik tasa finkoan aldatzera. Honek ondorio garrantzitsua zuen: banku zentralak ezin zuen nahi beste diru jaulki edo "inprimatu", diru hori beti izan behar zelako urrearekiko parekidea. Urrea, eta berarekiko parekidea den edozein moneta, diru sendo edo "Sound Money"-ren adibideak dira: beraien balioa ezin da manipulatu. Hain zuzen ere diruaren balioa inflazioarekin oso lotuta dago: diruaren balioa behera badoa, diru kantitate berarekin gauza gutxiago erosi ahal ditugu, eta inflazioa gora doa.

1970. hamarkadan urre-patroia desagertu zen eta urrearekin parekideak ez ziren monetak ezarri ziren: "fiat" monetak (Gaur egungo Euroa fiat moneta da). Banku zentralek fiat diru nahi beste jaulkitzea dute, diru hori ez delako urrearekin parekidea izan behar. Fiat diruak inflazioan duen eragina hainbat eskola ekonomikoren aztergaia izan da. Hain zuzen ere, Austriar eskola ekonomikoaren arabera, inflazioaren gorakadaren arrazoi nagusia fiat dirua da, bolumen monetarioa hainbeste handitzeak diru horren balioa jaistea dakarrelako. Gainera, Austriar eskola ekonomikoa pentsamendu ekonomikoaren korronteen artean inflazioari garrantzi handiena eman izan diona da.

3 Bitcoin meatzaritza

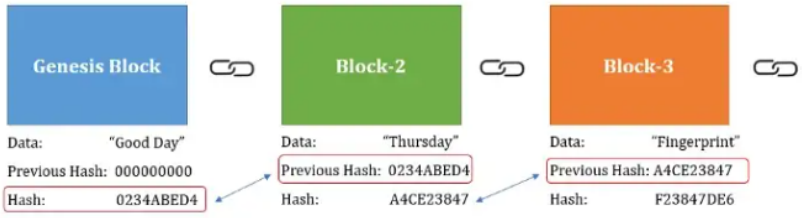
Bitcoin diru digital sistema da, transakzioen bidez balioa transferitzeko erabiltzen dena. Bitcoin sarea guztiz deszentralizatua da eta edozeinek gehitu ahal du bere burua sarera nodo baten bitartez. Beraz, Bitcoin sarea ez dago ez banku ez gobernuengatik kontrolatua. Halaber, Bitcoin-ek transakzio guztiak gordetzen dituen kontabilitate-liburu publikoa du (2 irudia). Kontabilitate liburua Bitcoin sareko nodoetan dago sakabanatua, aldaketak daudenean sinkronizatzen delarik.

Kontabilitate liburua bloke-kate baten moduan uler daiteke: transakzioak blokeetan taldekatzen dira, eta bloke bakoitza aurrekoarekin lotzen da, historia aldaezina osatuz (3 irudia). Bitcoin sareko nodoek ordainketak prozesatzen dituzte, partekatutako kontabilitate-liburua aldatzen ez dela ziurtatzen dute, eta



2. Irudia: Bitcoin-en sarea eta kontabilitate-liburua [1]. Transakzio berria (Adibidez Alice-k Bob-eri bitcoin bakarra bidaltzea) sarean sartzen denean nodo guztietara balioztatzeko bidaltzen da. Balioztatu ondoren transakzioak taldekatzen dira eta kontabilitate-liburu publikoan idazten dira.

bitcoin unitate berriak Bitcoin sarera jaulkitzen dituzte (Dirua "inprimatzen" dute).



3. Irudia: Bloke-katea. Bloke bakoitzak datuak ("data") eta goiburua dauzka. Datuetan transakzioak daude. Goiburuak metadatuak dauzka eta aurreko blokearekin lotuta dago laburpen kriptografiko baten bitartez ("Previous Hash"). (Venkat Kasthala/medium.com).

Bitcoin unitate berriak "meatzaritza" deritzon prozesuaren bidez sortzen dira. Bitcoin-en meatzaritzak badu urrearen meatzaritzarekin antza: azken finean bitcoin berriak lortzeko meatzarien norgehiagoka da (4 irudia).

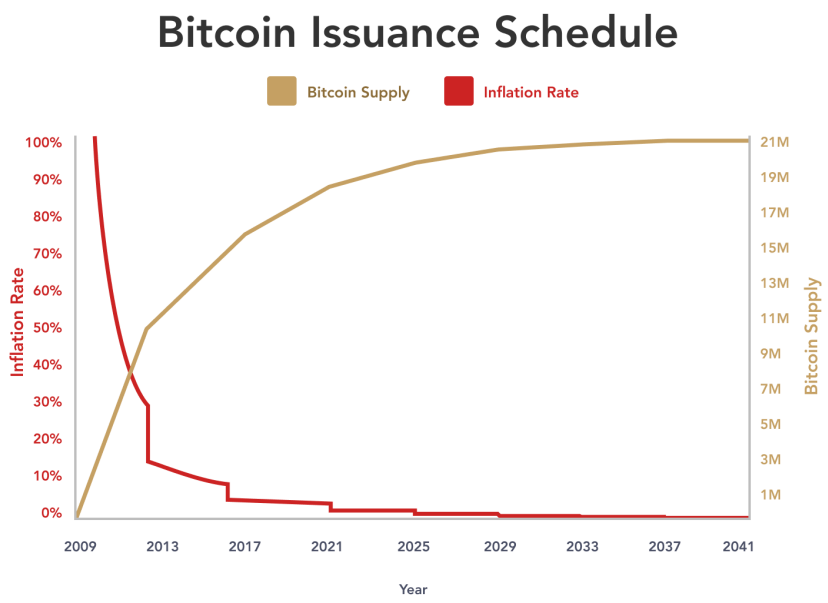
Bitcoin berriak lortzeko ("Urrea aurkitzeko") meatzariek arazo matematiko zehatza ebatzi behar dute, eta azkarren ebazten duenak bitcoin berriak jasoko ditu. Ebatzi beharreko eragiketa matematikoari "Laburpen kriptografikoa"

4. Irudia: Txinako bitcoin meatzaritza zentrua. Horrelako zentruek elektrizitate asko behar dutenez ingurugiroan kalte handiak eragiten dituzte. (Andrey Rudakov/Bloomberg).

deritzo (Ingelesez "Hash"). Laburpen kriptografikoa luzera finkoko kate alfanumerikoa da, edozein informaziori (Dokumentu bati, irudi bati, ...) laburpen funtzioa aplikatzean lortzen dena (Adibidez `8743952`). Laburpenek berezitasun garrantzitsua dute: jatorrizko informazioa oso gutxi aldatuta ere, sortzen den laburpena guztiz aldatzen da. Beraz jatorrizko informazioaren osotasuna bermatzeko erabiltzen dira, informazioa ez dela aldatu baieztatzen dutelako. Segurtasunaren arloan hainbat prozesutan berebiziko garrantzia dute: adibidez HTTPS web konexio seguruetako ziurtagiriak sinatzeko beharrezkoak dira.

Nola aplikatzen dira laburpena kriptografikoak bloke-katean? Meatzari batek bloke-kateko azken blokearen laburpena sortzean, aurreko bloke guztiak laburtzen dira, blokeak lotuta daudelako, blokeek eratzen duten historia kronologikoa aldaezin bihurtuz: transakzio guztiak dituen historia ezin da aldatu, Hash guztiak aldatu beharko liratekeelako. Eta hemen dago Bitcoin-en diseinuaren indargunea: ataza berean, meatzariek bloke-katearen osotasuna bermatzen dute eta bitcoin-ak jaulkitzen dira meatzarientzako sari gisa. Bitcoinek meatzariek jasotzen duten sariaren bidez kontrolatzen du jaulkitzen den diru bolumena. Hain zuzen ere, meatzari batek saria jasotzeko ekoizten duen laburpena zenbaki zehatza baino txikiagoa izan behar du (Target zenbakia). Target zenbakia zenbat eta txikiagoa izan, orduan eta zailagoa da laburpen egokia aurkitzea, zailtasuna handituz. Target zenbakia aurre-definitutako abiaduran aldatzen da, gero eta bitcoin gutxiago jaulki daitezen, nolabait urrearen erauzketa zailtasuna simulatzeko eta Sound Money-aren helburu nagusia lortzeko: inflazioa ekidin (5 irudia). Alegia, Bitcoin protokoloan bitcoin berrien jaulkitze abiadura aurretik

zehaztua dago, eta ez dago estaturik ezta banku zentralik abiadura hori alda dezakeenik.



5. Irudia: Bitcoin gero eta geldoago jaulkitzen da eta ez dira inoiz egongo 21 miloi bitcoin baino gehiago (2041 urte inguruan bitcoin guztiak jaulki izana espero da). Horrela, Bitcoin-ek urreak mundu fisikoan daukan eskasia mundu digitalean simulatzen du inflazioa kontrolatuz. (river.com).

4 Bitcoin eta Austriar eskola ekonomikoa

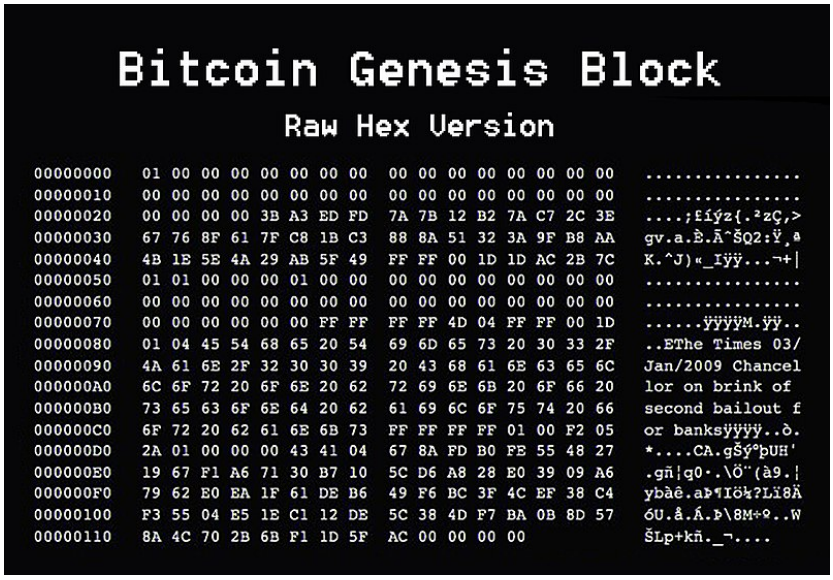
Bitcoin-en diseinuak Austriar eskolak hainbeste goraipatzen dituen ezaugarriak dauzka:

Bitcoin diru sendoa da: banku zentralek ezin dituzte bitcoin-ak jaulki, soilik meatzariek egin ahal dute abiadura definituan, inflazioa mugatuz.

Bitcoin estatuen kontrolpetik at dago: estatuek ezin dute Bitcoin-en oinarritzen den ekonomian eragin. Izan ere, Bitcoinen sortzaileak, Satoshi Na-

kamotok, lehenengo blokean ("Genesis" blokean) estatuen kontrolari kritika zorrotza txertatu zuen (6 irudia).

Bitcoin indibidualismoan oinarritzen da: Austriar eskolarentzat soilik banakoa da erabakiak har ditzakeen agentea, eta bere ongizatea bakarrik bilatu behar du. Bitcoin sarea ere banakoen berekoikerian oinarritzen da, sarearen segurtasuna mantentzeko meatzarien motibazioa bitcoin-ak lortzea baita, eta beraz ez da nodoen arteko konfidantzarik behar sarea seguru mantentzeko.



6. Irudia: Bitcoin bloke-katearen jatorri blokea ("Genesis Block"). Bertan Satoshi Nakamoto-k "The Times 03/Jan/2009 Chancelor on brink of second bailout for banks" esaldia sartu zuen, The Times egunkariko izenburu hori zuen berriari erreferentzia eginez. Berri horrek 2008-ko atzeraldi handiaren ondoren Erresuma Batuak bankuei bigarren erreskate baten bidez lagunduko ziela aipatzen zuen. Austriar eskolaren ikuspegitik, ekonomian estatuaren edozein esku-hartze kaltegarria da, bankuak zein hiritarrak laguntzeko bada ere. Baliteke Satoshi Nakamoto-k berri hori estatuen ekonomiaren kontrolaren kontrako kritika bezala aipatzea: izan ere estatuen kontrolpetik at geratuko zen moneta berria bataiatu zuen. (Anita Evans Hunt/Wikimedia Commons).

5 Bitcoin-en etorkizuna, Troika eta erabaki teknikoen ideologia

Bitcoin-en transakzioen geldotasuna arazo larria da: transakzio berria sarean sartzen denetik bloke-katean betiko idatzi arte 10 minutu pasa ahal dira. Ho-

7. Irudia: Ianis Varoufakis ekonomialaria (Vilaweb.cat).

ri kontutan hartuta, aditu askok Bitcoin "Urre digitala" bihurtuko dela uste dute: urre-patroiaren urteetan bezala, ez da transakziotarako erabiliko, baina banku zentraletan gordeko da balio erretserba moduan, eta transakzioak balio horren parekideak diren prozesuekin egingo dira (billeteak, monetak, ordainketa elektronikoak, kreditu txartelak, ...).

Bitcoin erreferentzia moneta bihurtzen bada, hiritarrok argi eduki behar dugu zeintzuk diren bere diseinuan eragin nabarmena izan zuten Austriar eskolako ideiak, aurrerago azaldutakoak. Izan ere ideia hauekiko kritikoak diren pentsalari garrantzitsuak ere badaude, adibidez Yanis Varoufakis politikari eta ekonomia irakasle Greziarra (7 irudia). Europako Banku Zentralak, Nazioarteko Diru Funtsak eta Europako Batzordeak eratzen duten Troikari aurre egiteagatik sona handia hartu zuen. Irakasle honen iritziz, kriptomonetek badute etorkizuna, baina banku zentralek behar beste diru jaulkitzeko ahalmena izan behar dute, gizartearen beharrei aurre egiteko [2]. Halaber, hainbat ekonomilarik ez dute uste gehiegizko dirua jaulkitzea beti saihestu behar denik, eta badaude pentsamendu ekonomikoaren eskola heterodoxo berriak ideia hori defendatzen dutenak, adibidez Teoria Monetario Modernoa. Izan ere Troikak ere inflazioa kosta ahala kosta ekiditea du helburu, eta bere teknikarietan Austriar eskolako ideiek eragin nabarmena dute.

Argi eduki behar dugu bai Bitcoin bai Troikaren kasuan edozein erabaki teknikoren atzean beti dagoela ideologia, nahiz eta teknokratek kontrakoa adierazi. Ideologia hori modu zorrotzenean aztertu behar dugu, erabaki "Teknikoek" ondorio oso serioak baitituzte gure ongizatean, 2008-ko eta 2022-ko krisietan argi eta garbi ikusi genuen moduan.

Erreferentziak

[1] K. Rosenbaum. *Grokking Bitcoin*. Manning, 2019.

[2] Evgeny Morozov. *Yanis Varoufakis on Crypto & the Left, and Techno-feudalism*, 2022-ko abenduaren 5-ean ikusia. `https://labur.eus/0n3mx`.