Bitcoin

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Bitcoin

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Miguel Vidal-en materialetik birziklatua: https://speakerdeck.com/mvidal/

Aurkibidea

- Zergatik Bitcoin ISSKS-n?
- Sarrera
- Oinarrizko teoria monetarioa
- Zer da Bitcoin?
- Bitcoin-en etorkizuna

Zergatik Bitcoin ISSKS-n?

Kriptodiru erabiliena da, eta bere ideia nagusiak beste hainbat kriptodirutan aurki daitezke

Eskola hauek ...

... ez dira Bitcoin-en goraipatzea

... ez dira finantza-kontseiluak

Zergatik Bitcoin ISSKS-n?

Hauen aplikazio oso arrakastatsua da:

- Zifraketa asimetrikoa
- Laburpen zifraketa

Zergatik Bitcoin ISSKS-n?

Bermatzen ditu:

- Zapuztesintasuna: ezin da[1] transakzio bat desegin
- Osotasuna: ezin da[1] blockchain-aren historia aldatu
- Kautotzea
- Pseudo-anonimatua
- …

[1] Konputazionalki/sozialki oso zaila

Sarrera

Bitcoin-en bi aldeak:

- (Teknikoki) Kontabilitate-liburua deszentralizatua eta gardena
- (Politikoki) Moneta-sistema:
  - Austriar eskolaren arabera, "diru onean" (Sound Money) opinarritua
  - Moneta berria jaulkitzeko energia elektriko asko kontsumitzen du

Sarrera

Kontu politiko eta teknikoen arteko muga ez da argia (Kontu teknikoak politikoenak dira)

Interes handiagoa daukagu kontu teknikoetan, baina ezin dugu alde politikoa guztiz baztertu

Sarrera

Bitcoin, edozein ondasun urri bezala, inbertitzeko (eta espekulatzeko) erabiltzen da

Horregatik berrietan beti hitzegiten da bere balioaren gorabeherei buruz, baina hori ez da Bitcoin-en alor garrantzitsuena

Garrantzitsuena: diru transakzioak egiteko barne-funtzionamendua, ez inbertsio-balio moduan

Oinarrizko teoria monetarioa

Balio-transeferentziarako lehenengo metodoa: elkartrukea

Nik sagarrak ekoizten ditut, zuk ardiak

Nire etxeko teilatua konpontzen baduzu, sagarrak emango dizkizut

… Baina zuk ez dituzu sagarrak behar, zuk laranjak behar dituzu

… Zure teilatua konpontzen badut, ardiak emango dizkidazu, baina ez daukat lekua guztientzako

Dirua elkartrukea baino hobea den abstrazioa bat lortzeko sortu zen

Oinarrizko teoria monetarioa

Diru ona (Sound money):

- Eramangarria (Gainean eroateko erraza)
- Homogeneoa (Toki orotan berdina da)
- Zatigarria (Unitate txikiagotan)
- Iraunkorra (Bere balioa denboran zehar mantentzen du)

Oinarrizko teoria monetarioa

Diru ona (Sound money):

- Urria eta ekoizteko/lortzeko zaila:
  - Faltsuztapenak ekidin
  - Ekonomiaren benetazko aberastasunaren adierazpen zehatzena

    (Adibidez urrea lurretik ateratzea oso zaila da, mozkin-marjina oso txiki delarik)

Oinarrizko teoria monetarioa

Historian zehar diru ona era desberdinetan inplementatu da, batez ere urrearen bidez

Gobernu bakoitzaren urre-erretserbak diruari balioa ematen zioten (diru **fiduziarioa** -fidare: konfidantza eduki-)

Oinarrizko teoria monetarioa

70ko hamarkadan urre-patroia bertan behera utzi zuten gobernuek, eta dirua **fiat** izatera pasa zen ("Izan bedi")

Gaur egun dirua sortzeko bankuek banku zentralak (BCE, erretserba federala) jaulkitako zorra hartzen dute: urreak ez duenez babesten, gobernuek nahi beste diru "inprimatu dezakete" (Dirua sortzeko ez da urrea lortu behar, interes tasa aldatu soilik)

Oinarrizko teoria monetarioa

Austriar eskolaren arabera, fiat diruak inflazioa sorten du eta ondorioz "soldaten lapurketa"

Satoshi Nakamoto-k Bitcoin sortu zuen diru ona inplementatzeko, fiat diruaren kontra, erakundeen kontrolik gabe (Finantza-sistemaren kontra eta 2008ko krisiaren aurrean?)

Genesis blokea: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Oinarrizko teoria monetarioa

Gainera, Bitcoin urrea baino diru hobea da, bere urritasuna formalki frogatu baidaiteke:

Urrez betetako meteorito erraldoi bat eroriko balitz, urreak ez luke balioa izango diru gisa

Bitcoin-en jatorria

- 2008 urriak 31: Satoshi-k whitepaper-a argitaratzen du
- 2008 azaroak 17: kodea bidaltzen du (eta urte ta erdi horretan lanean egon dela dio)
- 2009 urtarrilak 3: genesis blokea lortzen da
- 2009 urtarrilak 8: Spourceforge-en kodea argitaratzen da
- 2009 urtarrilak 12: lehenego transakzioa (Satoshi-k Hal Finney-ri, 170 blokea)

Bitcoin-en jatorria

- 2009 urriak 5: BTC-ak aldatzeko lehenengo "exchange" zerbitzua, BTC-aren prezioa sortzeko beharrezkoa den elektrizitatea kontuan hartzen duena prezioa ezartzeko (1$ -> 1309 btcs)
- 2010 maiatzak 22: Pizza day (Laszlo, bi pizza 10k btcs)
- 2010 abendua: Satoshi-k proiektutik alde egiten du

Zer da Bitcoin?

- Kontu-liburua (Ledger):
  - Edonor nodo bezala gehitu ahal den sare P2P batean elkarbanatua
  - Edozein nodok bere edukia baliozta dezake
  - Behin balioztatuak, orrialdeak aldatzea ezinezkoa* (blockchain)

Zer da Bitcoin?

- Kontu liburuan oinarritutako balio-transferentzia sistema
- Inflaziorik gabeko moneta-sistema deszentralizatua, nodoentzako dirua jaulkitzeko eta transakzioak balioztatzeko eragingarriekin (**Biak batera**). Moneta jaulkitzeko gastatutako elektrizitatearen kostuan oinarritzen da.

Zer da Bitcoin?

- Protokoloa: Bitcoin
- Moneta: bitcoin. BTC edo XTC. Satoshi: 0,00000001 BTC
- API-a

Zer da Bitcoin?

- Sarearen nodoen artean transferitu ahal da
- Transakzioak itzulezinak dira
- Tranksazioak segundutan transmititzen dira eta minututan balioztatu
- Transakzioak edozein momentutan jaso daitezke, ordenagailua amatuta egon arren
- Transakzio bakoitzeko komisioa oso merkea da
- 21M-ko muga dago, baina 8 dezimaletaraino zatitu daiteke

Gardentasuna

- Mundu guztiak dena ikusten du
- Mundu guztiak kodea exekutatu ahal du
- Mundu guztiak transakzioak balioztatu ahal ditu

Gardentasuna

- Iraganeko eta oraingo transakzio guztiak publikoak dira, baina ez daude identitate batekin lotuak, helbide batekin baino (gainera hash bidez laburtua)
- Anonimotasuna erabiltzailearen ardura da
- Datu basean 10 minuturo transakzio blokeak gehitzen dira, onargarriak bihurtzen dituzten ezaugarriekin

Fidagarritasuna

- Osotasuna: ezin da faltsutu ezta aldatu
- Zapuztezintasuna
- Fidagarria da ez zarelako inortaz fidatu behar

Nola ekoizten dira Bitcoin-ak

- Meatzaritza deituriko prozesuan, Proof of Work (PoW)-ean oinarritzen dena
- PoW: eragiketa kriptografikoa indarraren bidez ebatzi
- Ez dago erakunderik ez banakorik diru-bolumen oso kontrolatu ahal duena, ekoizpena ("dirua inprimatzea") ezin baita kontrolatu

Meatzaritza

- Bi funtzio:
  - Eskaintza monetarioa: meatzariek moneta berria ekoizten dute (Modu matematikoki kontrolatuan)
  - Segurtasuna: bloke katearen osotasuna mantententzen dute, transakzioak barne

Meatzaritza

- Meatzariek saria jasotzen dute (Bitcoin moduan) eta horrela Bitcoin-ak jaulkitzen dira
- Transakzioen komisio txikiak meatzariek ere jasotzen dituzte

Bitcoin sarea

"Grokking bitcoin" liburua:

GitHub (Adibidea)

Manning

Bitcoin sarea

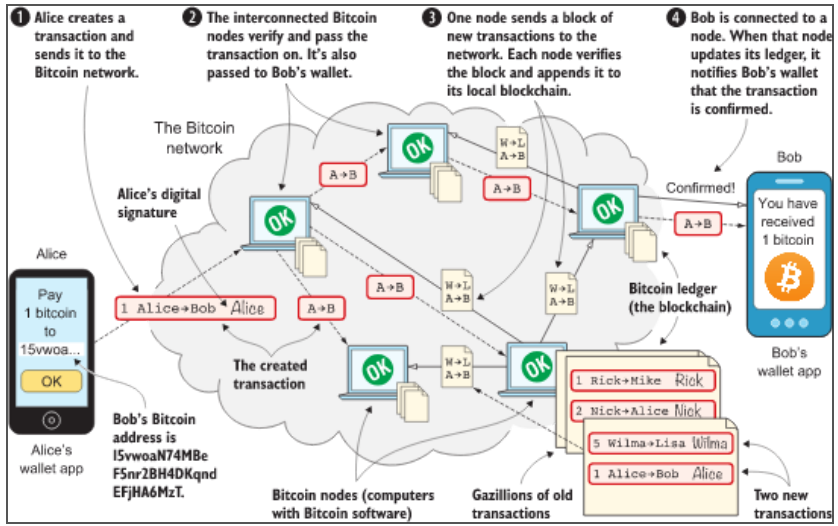
8.5.1. Bitcoin at a glance

The Bitcoin peer-to-peer network is huge. As of this writing:

- There are about 10,000 publicly accessible full nodes.
- Bitcoin's money supply is about 17,400,000 BTC.
- Each bitcoin is worth around $6,500.
- Bitcoin processes about 250,000 transactions per day.
- An estimate of 100,000 BTC, valued at $630 million, is moved daily.
- The total mining hashrate is about 50 Ehash/s, or 50×10^{18} hash/s. A typical desktop computer can do about 25 Mhash/s.
- The transaction fees paid each day total around 17 BTC. This averages to 6,800 satoshis per transaction, or about $0.40 per transaction.
- People in all corners of the world use Bitcoin to get around problems in their day-to-day lives.

bitnodes.io

Bitcoin sarea



Bitcoin sarea

"Dirua bidali": Gako publikoa --> Gako pribatua

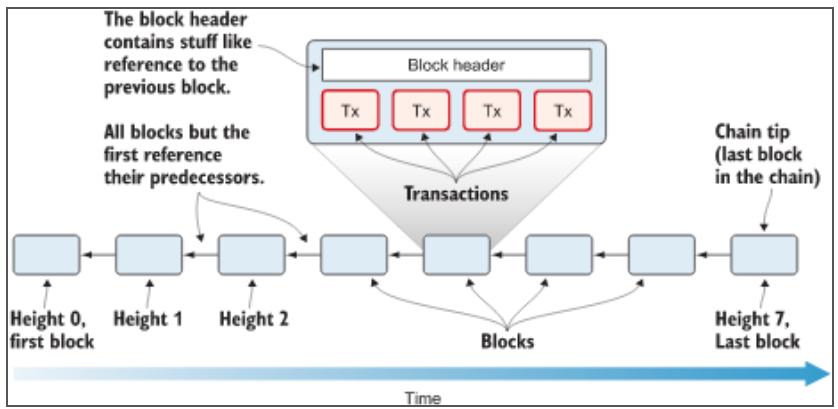
"Transakzioak sinatu": Gako pribatua --> Gako publikoa

Bitcoin sarea

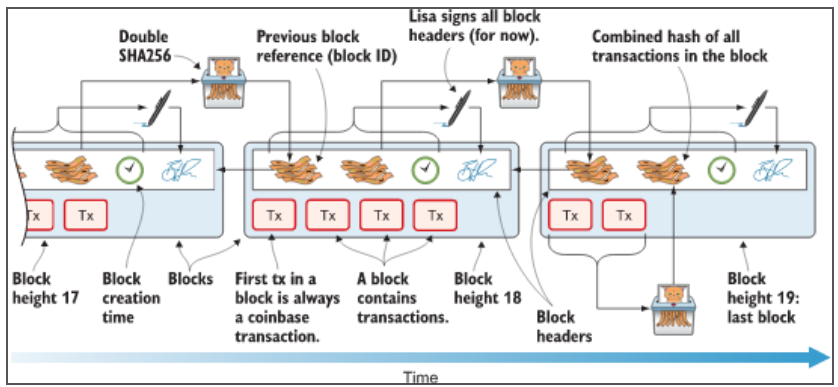
Laburpen zifraketa (Hash):

- **btc-ak sortzeko, meatzariek hash bat lortu behar dute**
- Gako publikoak laburtu
- Transakzioak laburtu
- Etab.

Bitcoin sarea (Blockchain)



Bitcoin sarea (Blockchain)



Bitcoin sarea (Proof of work)

Blokeak balioztatu --> bitcoin-ak sortu

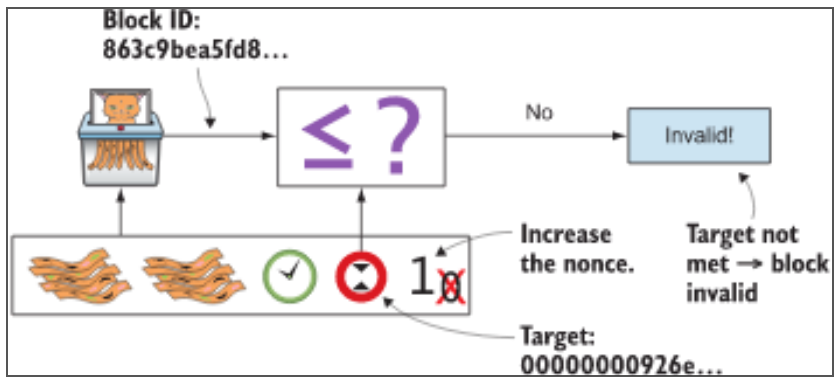
Balioztatu: gastu bikoitza ekidin, timestamp egokia, etab. --> hash bat sortu

Hash horrek aurreko hash guztiak dauzka

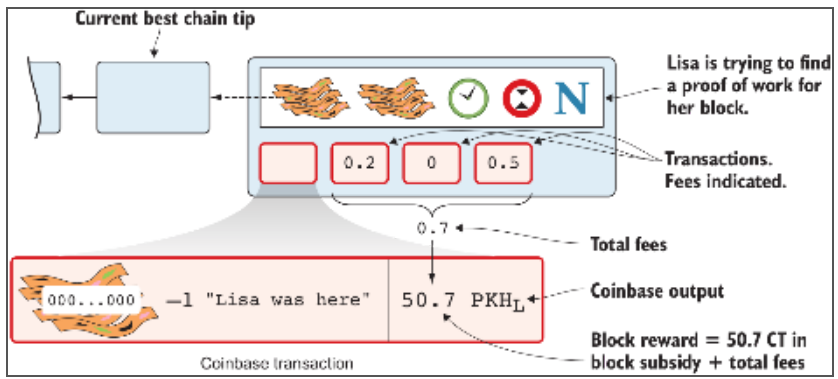
Baina hash hori **target** zenbakia baino txikiagoa izan behar du

Target aldatzen doa, zailtasuna aldatzeko

Bitcoin sarea (Proof of work)



Bitcoin sarea (Proof of work)



Bitcoin Core

https://bitcoincore.org/en/about/

https://github.com/bitcoin/bitcoin/

BIPs

BitCoin improvement proposal

https://github.com/bitcoin/bips

Bitcoin-en etorkizuna

- Balio erretserba, transakzio azkarragoen sistemen oinarri (Adibidez VISA-k 90 behar ditu transakzioak balioztatzeko)
- Adibidez lightning proiektuan transakzio asko biltzen dira, aldi berean egiteko