

Bitcoin

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



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/>



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 algoritmoak

Zergatik Bitcoin ISSKS-n?

Bermatzen ditu:

- Zapuztesintasuna: ezin da¹ transakzio bat desegin
- Osotasuna: ezin da¹ blockchain-aren historia aldatu
- Kautotzea
- Pseudo-anonimatuua
- ...

[1] Konputazionalki/sozialki oso zaila

Sarrera

[Bitcoin: A Peer-to-Peer Electronic Cash System \(Satoshi Nakamoto\)](#)

Sarrera

Bitcoin-en bi aldeak:

- (Teknikoki) Kontabilitate-liburua desentralizatua 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 berrieta 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

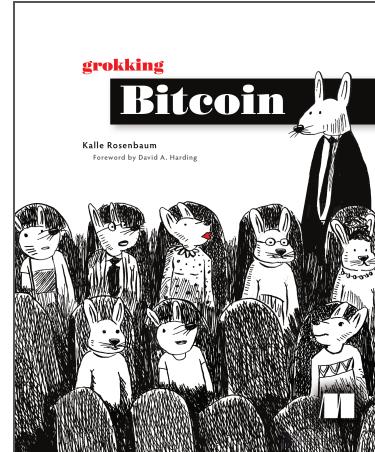
Zer da Bitcoin?

Grokking bitcoin (Kalle Rosenbaum, 2019):

[GitHub](#)

[Biblioteca EHU](#)

[Manning](#)



Zer da Bitcoin?

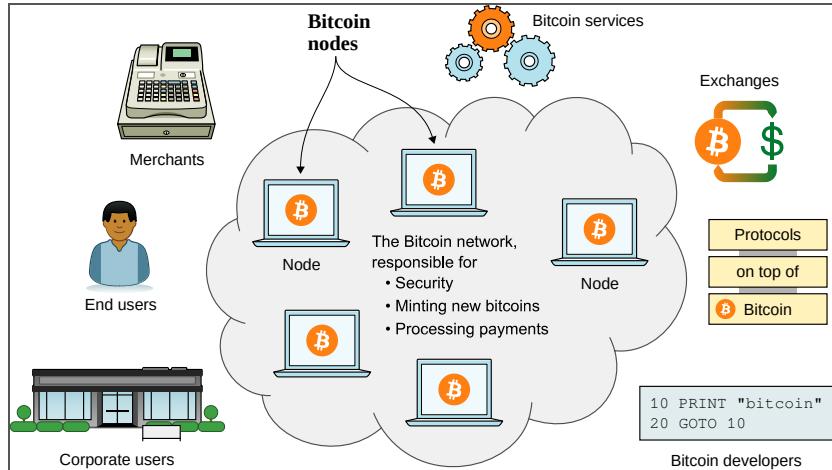
Diru digital sistema

Sare batean oinarritua. Sare horretara edozeinek bere burua gehitu ahal du, nodo baten bitartez, eta sare hori ez dago banku ez gobernuengatik kontrolatua

Protokoloa: Bitcoin (B)

Moneta: bitcoin (b). Sinboloa: BTC edo XTC. Satoshi: 0,00000001 BTC

Bitcoin sarea



Bitcoin sarea

Ordainketak prozesatu

Partekatutako kontabilitate-liburua aldatzen ez dela ziurtatzea

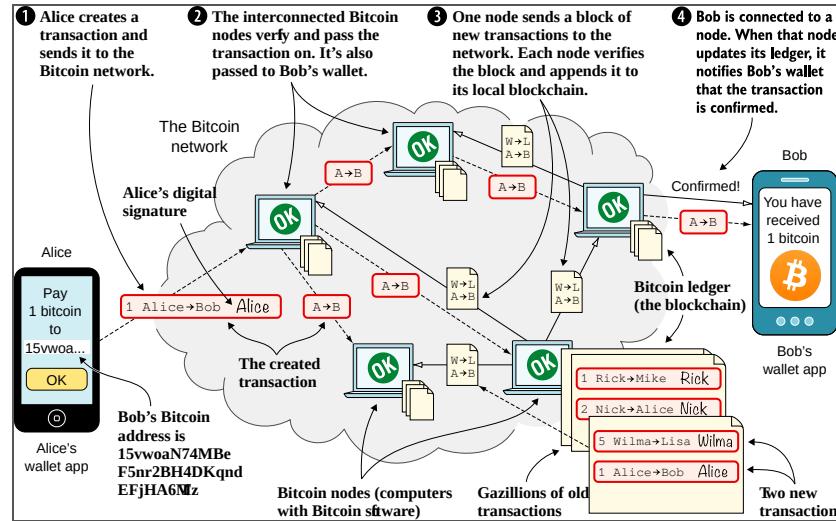
Zirkulazioan bitcoin berriak jarri, aurretik ezarritako abiaduran

Bitcoin sarea

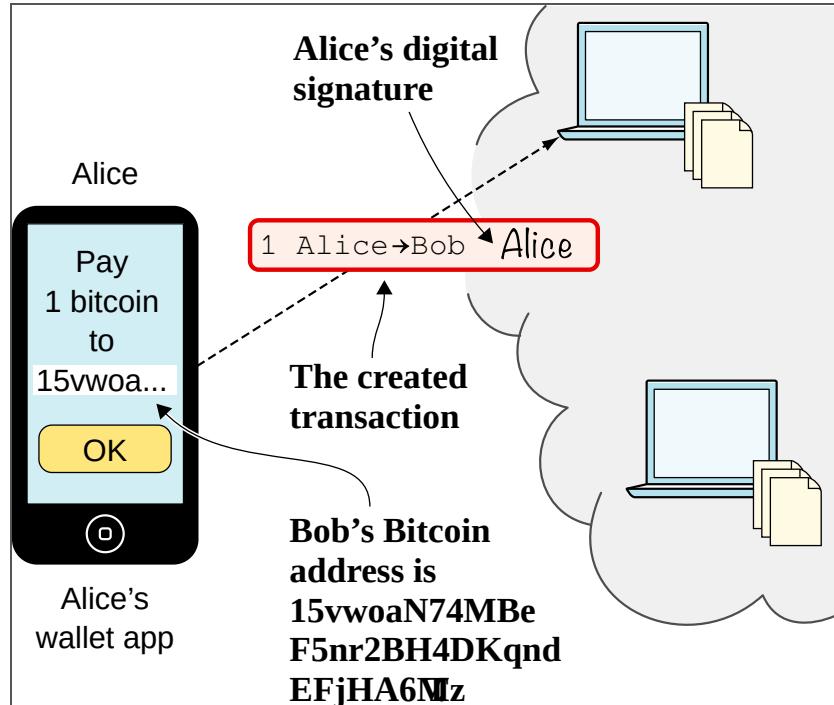
Kontabilitate-liburu elkarbanatua (Nodo guztiekin kopia bat dute)

Kontabilitate-liburuak egin diren transakzio guztiak ditu

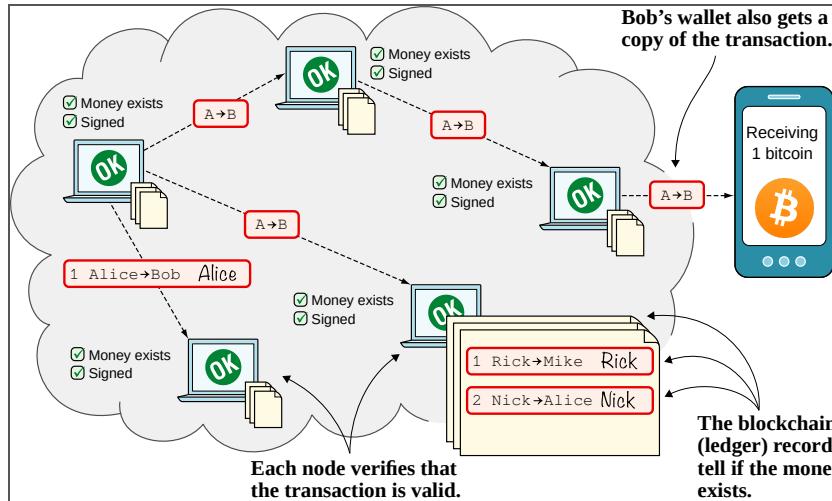
Ordainketa



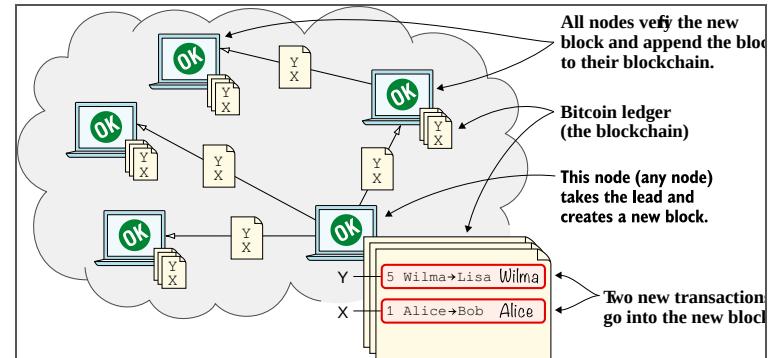
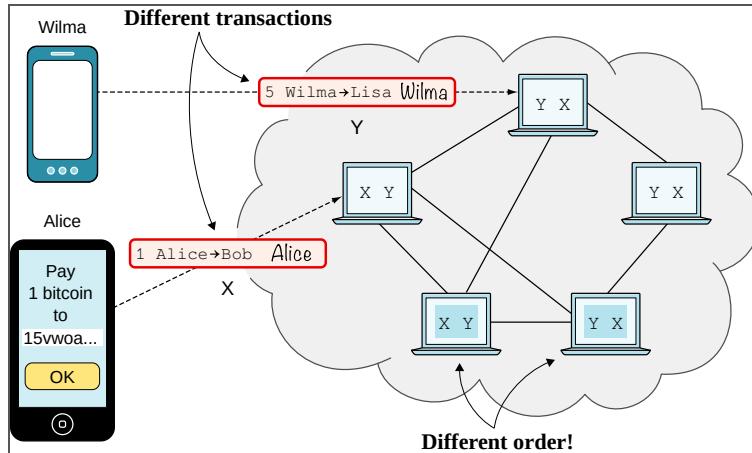
(1) Transakzioak



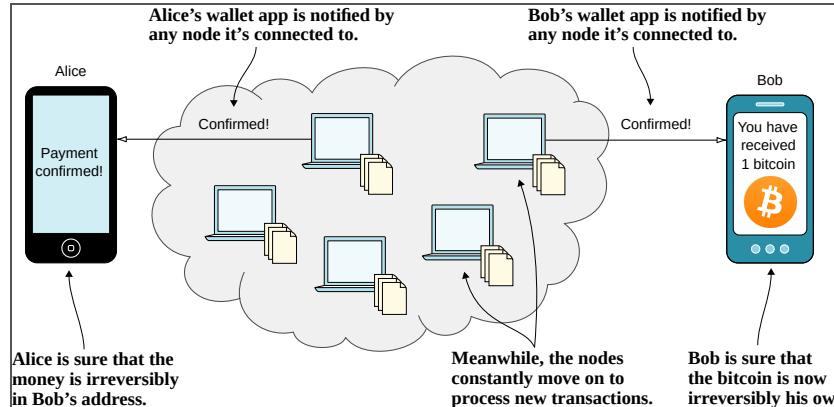
(2) Sarea



(3) Blockchain



(4) Diru-zorroa



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 mantentzen dute, transakzioak barne

Meatzaritza

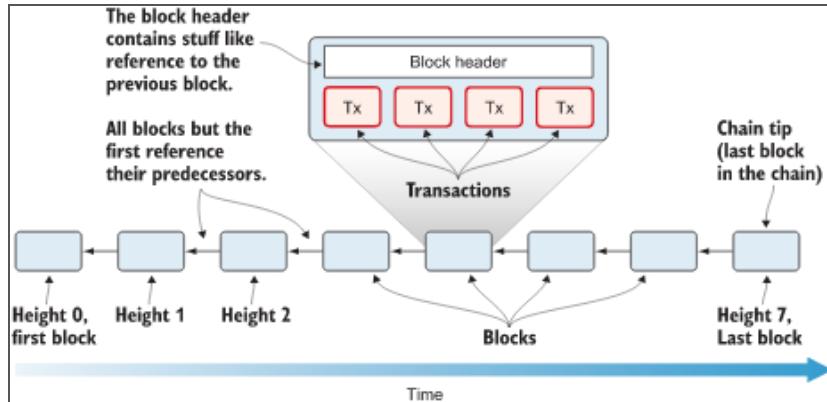
- Meatzariekin saria jasotzen dute (Bitcoin moduan) eta horrela Bitcoin-ak jaulkitzen dira
- Transakzioen komisio txikiak meatzariek ere jasotzen dituzte

Bitcoin sarea

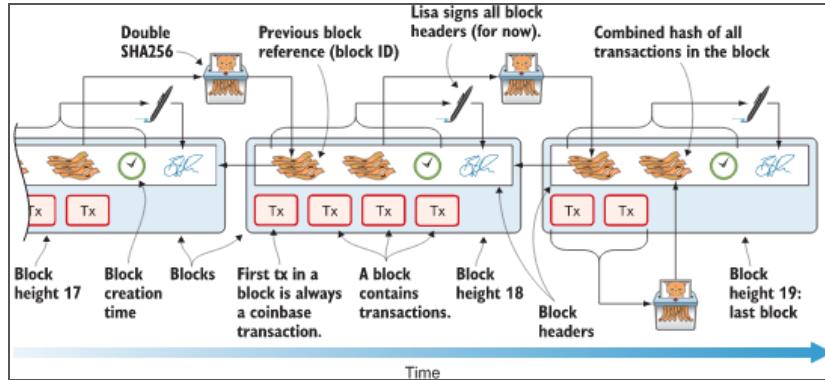
Laburpen zifraketa (Hash):

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

Bitcoin sareea (Blockchain)



Bitcoin sareea (Blockchain)



Bitcoin sarea (Proof of work)

Blokeak balioztatu --> bitcoin-ak sortu

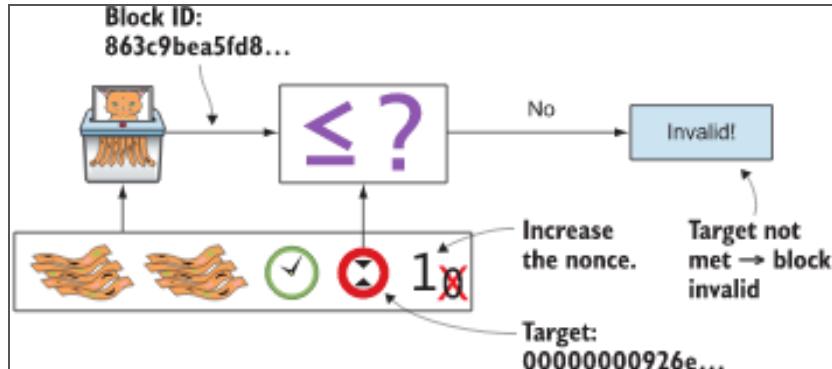
Balioztatu: gastu bikoitza ekidin, timestamp egokia, etab.--> hash bat sortu

Hash horrek aurreko hash guztiak dauzka

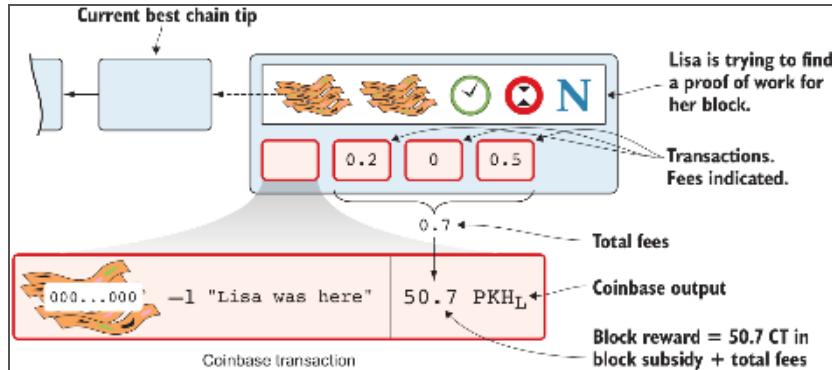
Baina hash hori **target** zenbakia baino txikiagoa izan behar du

Target aldatzen doa, zaitasuna aldatzeko

Bitcoin sarea (Proof of work)



Bitcoin sareja (Proof of work)



Bitcoin-ek ebazten dituen arazoak

- Banku-kontu lortzea ezinezkoa
- Pribatutasun falta
- Herrialdeen arteko transferentziak
- Hiper-inflazioa (*)

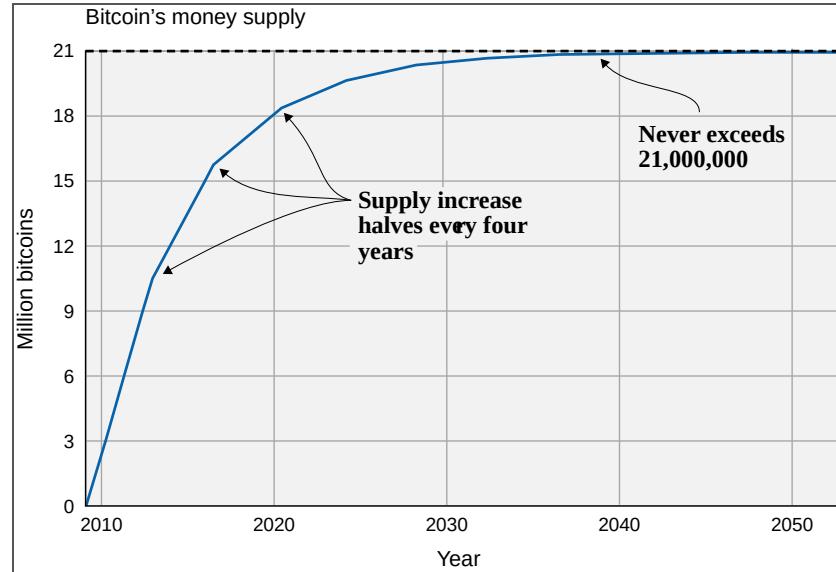
(*) Keynes fallacy of composition

Discussing Crypto, the Left & Technofeudalism with Evgeny Morozov -
CRYPTO SYLLABUS long interview

Bitcoin finantza-erakunde tradizionalen aurrean

- Desentralizatua
- Hornidura mugatua: 21 milioi bitcoin
- Muga gabekoa

Bitcoin horridura



Bitcoinen egungo erabilera

- Aurrezkia
- Nazioarteko transferentziak
- Erosketak
- Finantza-espekulazioa
- Jabetza-ziurtagiria
- Esistentziaren ziurtagiria
- ...

Nola ez erabili Bitcoin

- Ordainketa txikiak (Lightning Network?)
- Berehalako ordainketak (Lightning Network?)
- Gure aurrezki guztien inbertsioa (Edozein finantza-jarduerari aplika dakioke)

Bitcoin Core

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

<https://github.com/bitcoin/bitcoin/>

BIPs

BitCoin Improvement Proposal

<https://github.com/bitcoin/bips>

Economic majority

Bitcoin-en etorkizuna

- Transakzio-sistema bizkorragoak babesten dituen balio-erreserbatzea
(Kreditu txarteletan bezala)
- [Lightning](#) projektuan adibidez aldiberean emango diren transakzio asko
batzen dira multzo bakar baten, prozesua azkartzeko