Bitcoin

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

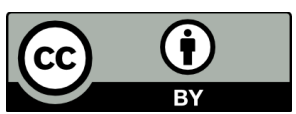
Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

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/



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

[1] Konputazionalki/sozialki oso zaila

Sarrera

Bitcoin: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto)

Bitcoin eta Troika: ideologia non-nahi

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

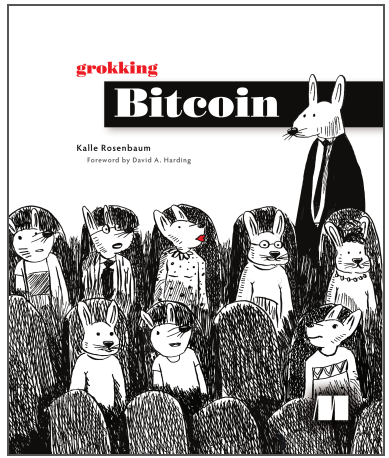
Zer da Bitcoin?

Grokking bitcoin (Kalle Rosenbaum, 2019):

GitHub

EHU liburutegia

Manning



Zer da Bitcoin?

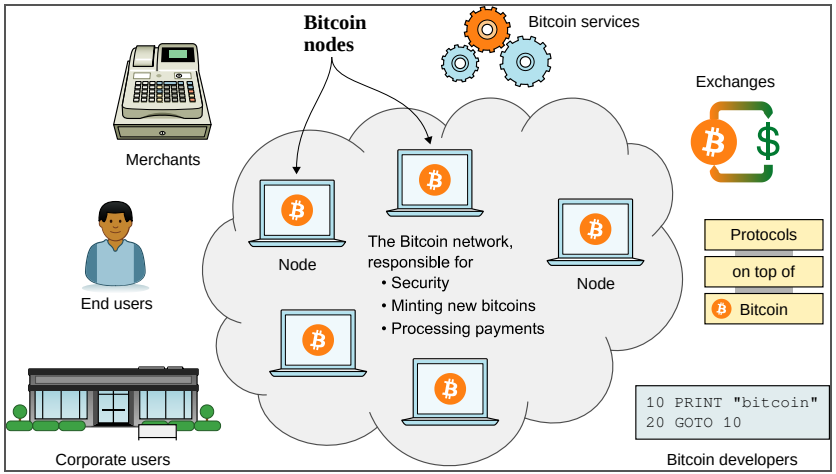
Diru digital sistema

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

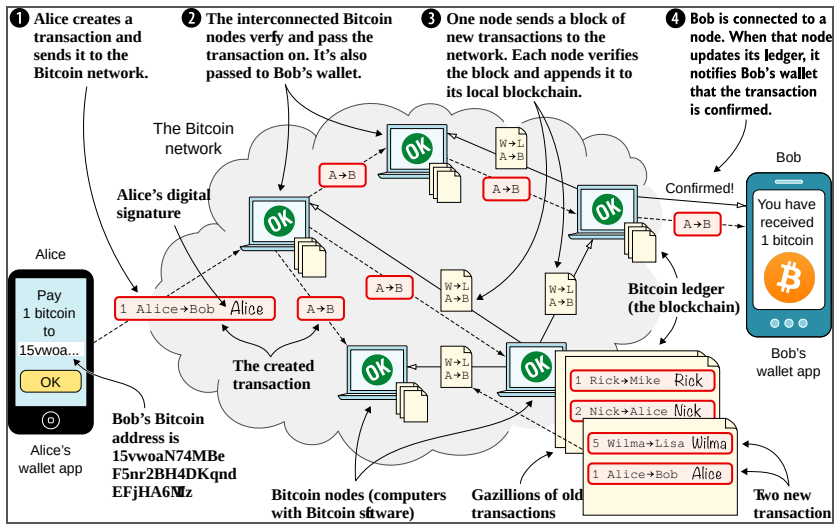
Zirkulazioan bitcoin berriak jarri, aurretik ezarritako abiaduran

Bitcoin sarea

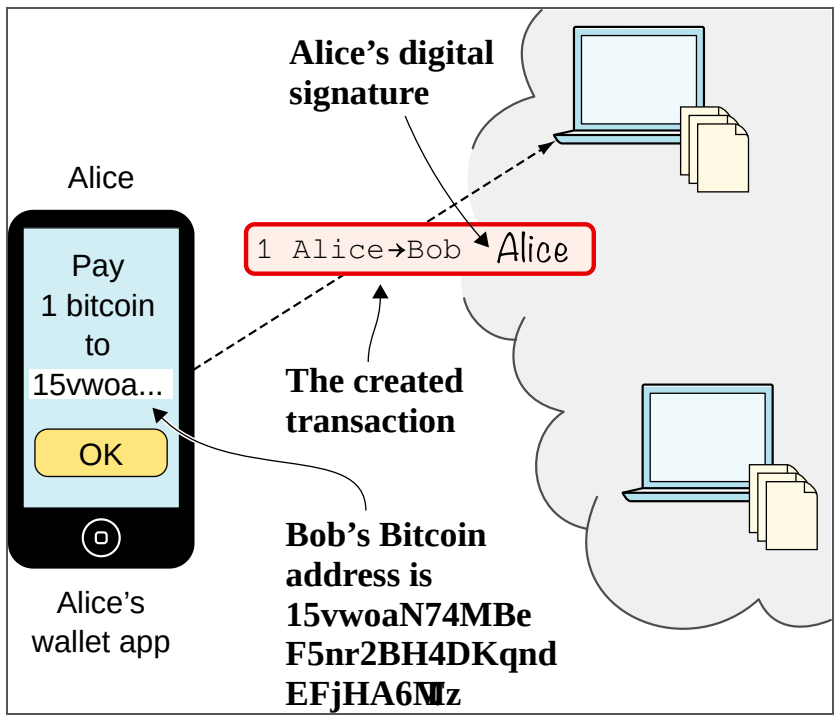
Kontabilitate-liburu elkarbanatua (Nodo guztiek kopia bat dute)

Kontabilitate-liburuak egin diren transakzio guztiak ditu

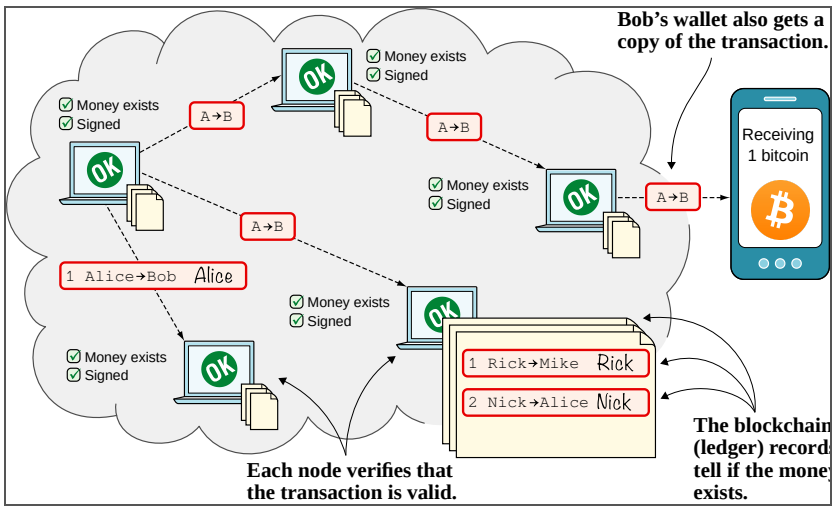
Ordainketa


1 Alice creates a transaction and sends it to the Bitcoin network.
2 The interconnected Bitcoin nodes verfy and pass the transaction on. It's also passed to Bob's wallet.
3 One node sends a block of new transactions to the network. Each node verifies the block and appends it to its local blockchain.
4 Bob is connected to a node. When that node updates its ledger, it notifies Bob's wallet that the transaction is confirmed.
The Bitcoin network
Alice's digital signature
Alice
Pay 1 bitcoin to 15vwoa...
OK
Alice's wallet app
1 Alice→Bob Alice
A→B
W→L
A→B
OK
Confirmed!
Bob
You have received 1 bitcoin
Bob's wallet app
Bitcoin ledger (the blockchain)
The created transaction
Bob's Bitcoin address is 15vwoaN74MBeF5nr2BH4DKqndEFjHA6NIz
1 Rick→Mike Rick
2 Nick→Alice Nick
5 Wilma→Lisa Wilma
1 Alice→Bob Alice
Bitcoin nodes (computers with Bitcoin software)
Gazillions of old transactions
Two new transaction

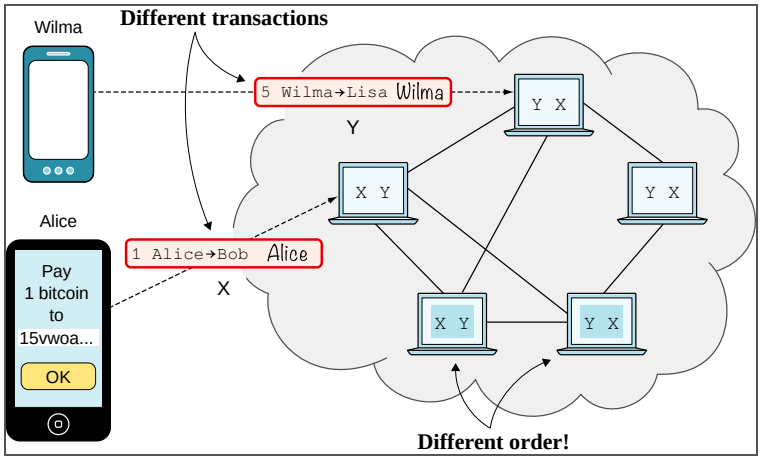
(1) Transakzioak

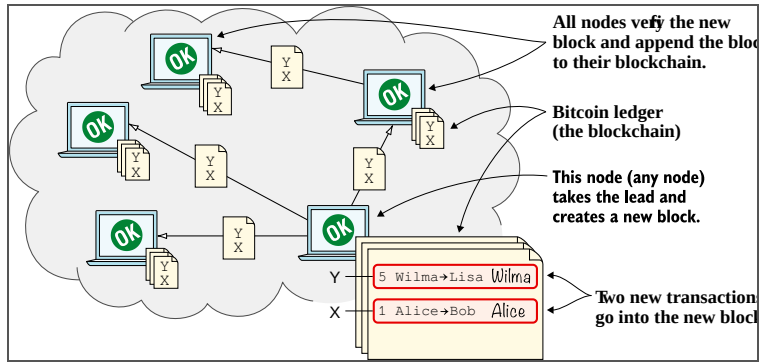


(2) Sarea

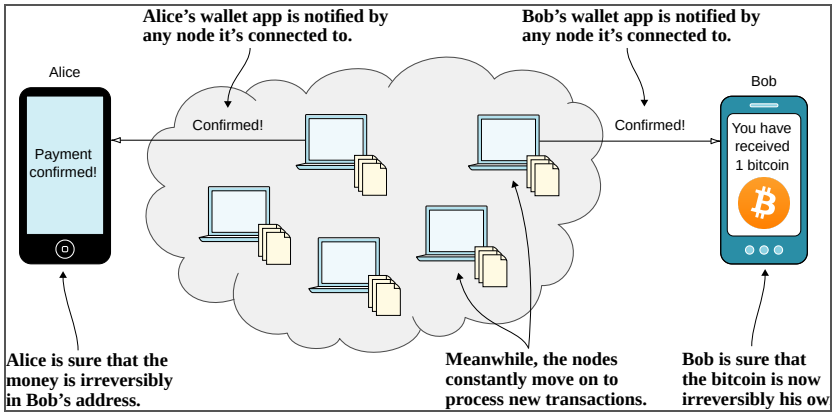

Bob's wallet also gets a copy of the transaction.
Money exists
Signed
A→B
Receiving 1 bitcoin
1 Alice→Bob Alice
1 Rick→Mike Rick
2 Nick→Alice Nick
Each node verifies that the transaction is valid.
The blockchain (ledger) record
tell if the mone
exists.

(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

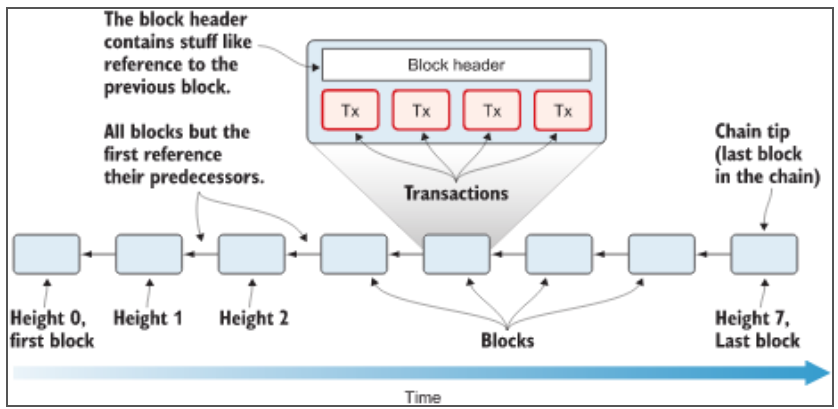
- Meatzariek saria jasotzen dute (Bitcoin moduan) eta horrela Bitcoin-ak jaulkitzen dira
- Transakzioen komisio txikiak meatzariek ere jasotzen dituzte

Bitcoin sarea

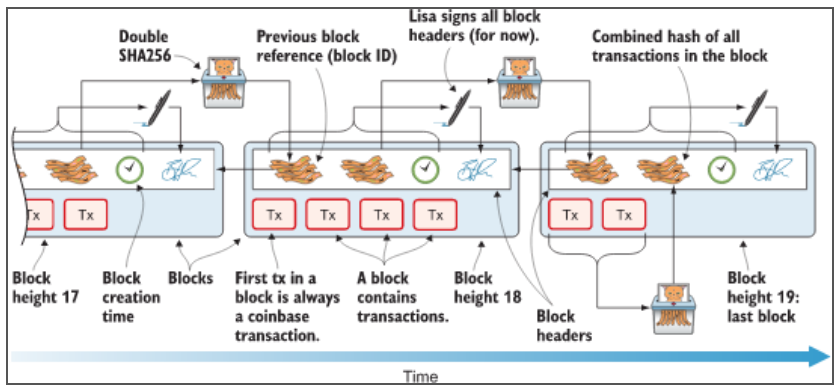
Laburpen zifraketa (Hash):

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

Bitcoin sarea (Blockchain)



Bitcoin sarea (Blockchain)



Bitcoin sarea (Proof of work)

Blokeak balioztatu --> bitcoin-ak sortu

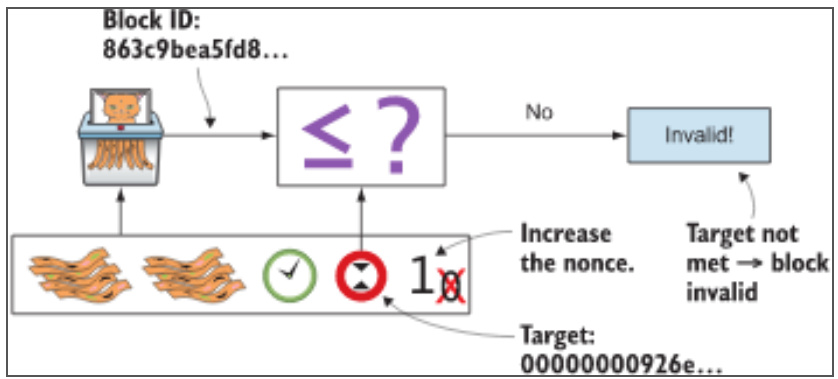
Balioztatu: gastu bikoitza ekidin, timestamp egokia, etab. --> hash bat sortu

Hash horrek aurreko hash guztiak dauzka

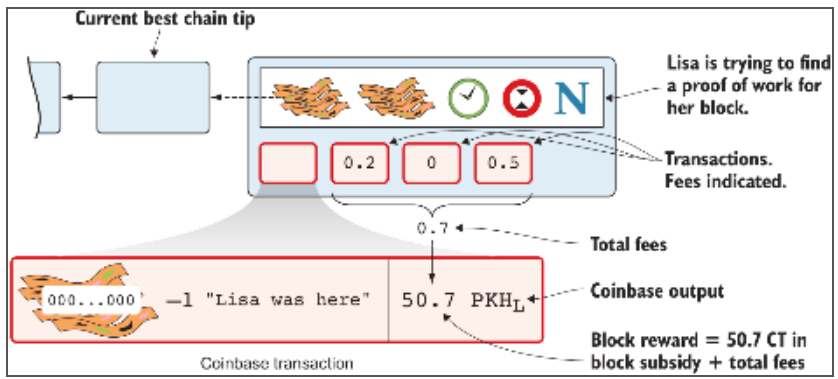
Baina hash hori **target** zenbakia baino txikiagoa izan behar du

Target aldatzen doa, zailtasuna aldatzeko

Bitcoin sarea (Proof of work)



Bitcoin sarea (Proof of work)



Bitcoin-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

One of your critiques of Bitcoin as a currency (which you clearly state it is not and cannot be) is that it limits policy space available, such that, when there is a pandemic, it won't be possible to increase the money supply. I suppose this also covers 'printing money', with all of the perverse consequences of QE that you yourself have documented elsewhere. Wouldn't the Bitcoin maximalists be at least coherent in arguing that this inability to print money is a feature, not a bug, of the system?

When 'Bitcoin maximalists', as you call them, wax lyrical about the inability to print money (and celebrate this inability as Bitcoin's feature, rather than its bug), they are being terribly unoriginal – banal, I dare say. Capitalism nearly died in 1929, and tens of millions *did* die in the war that ensued, because of this toxic fallacy that underpinned the Gold Standard then and Bitcoin now. Which fallacy? The fallacy of composition, as John Maynard Keynes called it.

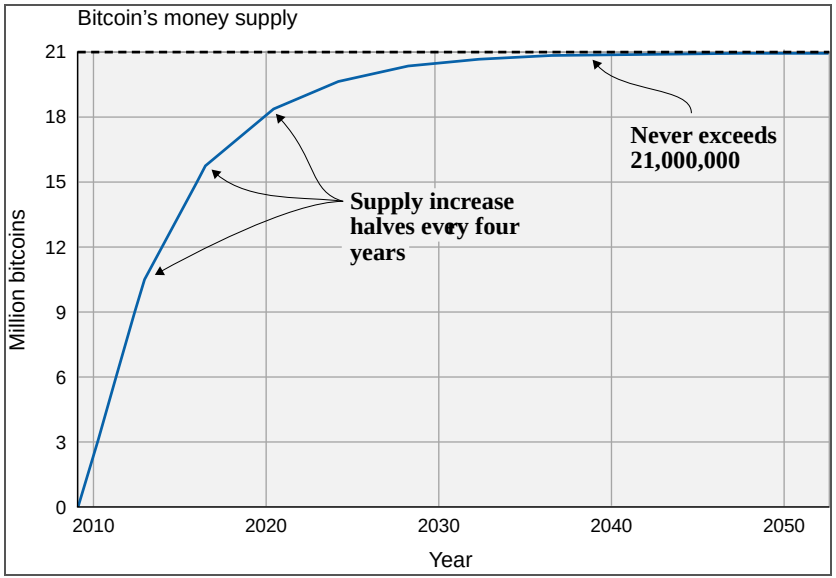
Its essence is a tendency to extrapolate from the personal realm to the macroeconomic one. To say that if something is good for me – if a practice is sound at the level of my family, business, etc. – it must also be good for the state, government, humanity at large. For example, yes, parsimony is a good thing for me, personally. If I can't make ends meet, I need to tighten my belt; otherwise, I shall sink more and more into debt. However, the exact opposite holds for a macroeconomy: If, in the midst of a recession, the government tries to tighten its belt as a means of eliminating its budget deficit, then public expenditure will decline at a time of falling private expenditure. And since the sum of private and public expenditure equals aggregate income, the government will be – inadvertently – magnifying the recession and, yes, its own deficit (as government revenues fall). This is an example of one thing (belt-tightening) being good at the micro-level and catastrophic at the macro level.

Similarly with gold, Bitcoin, and all other 'things' of exchange value: If you have gold, it is good for you if its supply is limited, fixed if possible. Same with Bitcoin, silver, dollars. (Nb. It is why the rich and powerful traditionally opposed expansionary monetary policy, crying 'hyperinflation' at the drop of a hat.) So, yes, if you

Bitcoin finantza-erakunde tradizionalen aurrean

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

Bitcoin hornidura



Bitcoinen egungo erabilerak

- 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 proiektuan adibidez aldiberean emango diren transakzio asko

batzen dira multzo bakar baten, prozesua azkartzeko