

# Zifraketa aplikazioak

Mikel Egaña Aranguren

[mikel-egana-aranguren.github.io](https://mikel-egana-aranguren.github.io)

[mikel.egana@ehu.eus](mailto:mikel.egana@ehu.eus)



# Zifraketa aplikazioak

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

<https://github.com/mikel-egana-aranguren/EHU-ISSKS-31>



# Zifraketa aplikazioak

- Sinadura
- Zertifikatuak
- TLS
- SSH
- Bitcoin

# Sinadura digitala

Mirenek Ikerreri mezua bidaltzen dio, gako publikoko sistema erabiliz

Edonork ezin du irakurri Mirenen Ikerrentzako mezua, baina edozeinek bidali  
ahal du

Nola daki Ikerrek Mirenek bidali diola edo inork ez duela mezua aldatu?

Soluzioa: Mirenek mezua sinatzen du

# Sinadura digitala

Erabiltzaile zilegiak soilik sinatu ahal du bere dokumentua

Ezin du inork sinadura faltsutu

Edozeinek balioztatu ahal du sinadura digitala

# Sinadura digitala

Ezin da sinadura bat berrerabili

Ezin da sinadura bat aldatu

Ezin da dokumentu bat sinatu izana ukatu

Ezin da dokumentu bat aldatu sinatu ostean

**Kautotzea, Osotasuna eta Zapuztezintasuna**

# Sinadura digitala

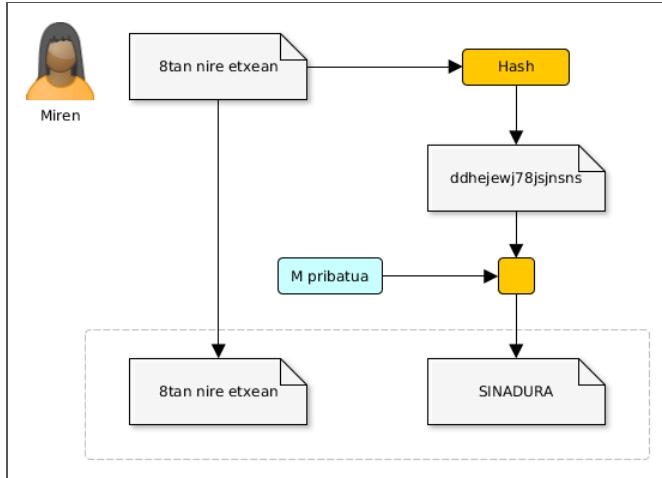
Mirenek mezuaren laburpen kriptografikoa lortzen du: **RC=hash(m)**

Mirenek bere klabearekin zifratzen du laburpen kriptografikoa:

**Sinadura=e(RC,M<sub>pri</sub>)**

Mirenek bere mezua (Zifratua edo zifratu gabe) eta bere sinadura bidaltzen ditu

# Sinadura digitala



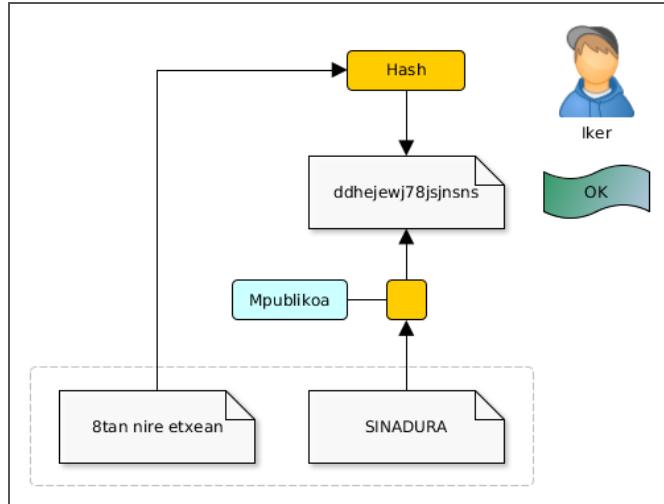
# Sinadura digitala

Ikerrek sinadura deszifratzen du Mirenen gako publikoa erabiliz: **RC=**  
**(Sinadura,M<sub>pu</sub>)**

Ikerrek mezuaren laburpen kriptografikoa lortzen du: **RC'=hash(m)**

Ikerrek RC' eta RC alderatzen ditu ezer aldatu ez dela baiezatzeko

# Sinadura digitala



# Sinadura digitala

Sinatzeaz gain, Mirenek mezua zifratzen badu, Ikerrek bakarrik irakurriko du:

**Konfidentzialtasuna, Osotasuna, Kautotzea, Zapuztezintasuna**

Hurrengoak erabiltzea dauka:

- Kriptografia asimetrikoa
- Kriptografia hibridoa

# Sinadura digitala

Kriptografia asimetrikoa. Ikerreri bidali:

- Mezu zifratuaren kriptograma ( $M_{pri}$  eta  $I_{pu}$ -rekin zifratua)
- Bere sinadura digitala (Laburpen kriptografikoa,  $M_{pri}$ -rekin zifratua)

# Sinadura digitala

Kriptografia hibridoa. Ikerrerri bidali:

- Saio gakoarekin zifratutako mezuaren kriptograma
- Saio gako zifratuaren kriptograma,  $I_{pu}$ -rekin zifratua
- Bere Sinadura digitala (Laburpen kriptografikoa,  $M_{pri}$ -rekin zifratua)

# Sinaduren konfidantza

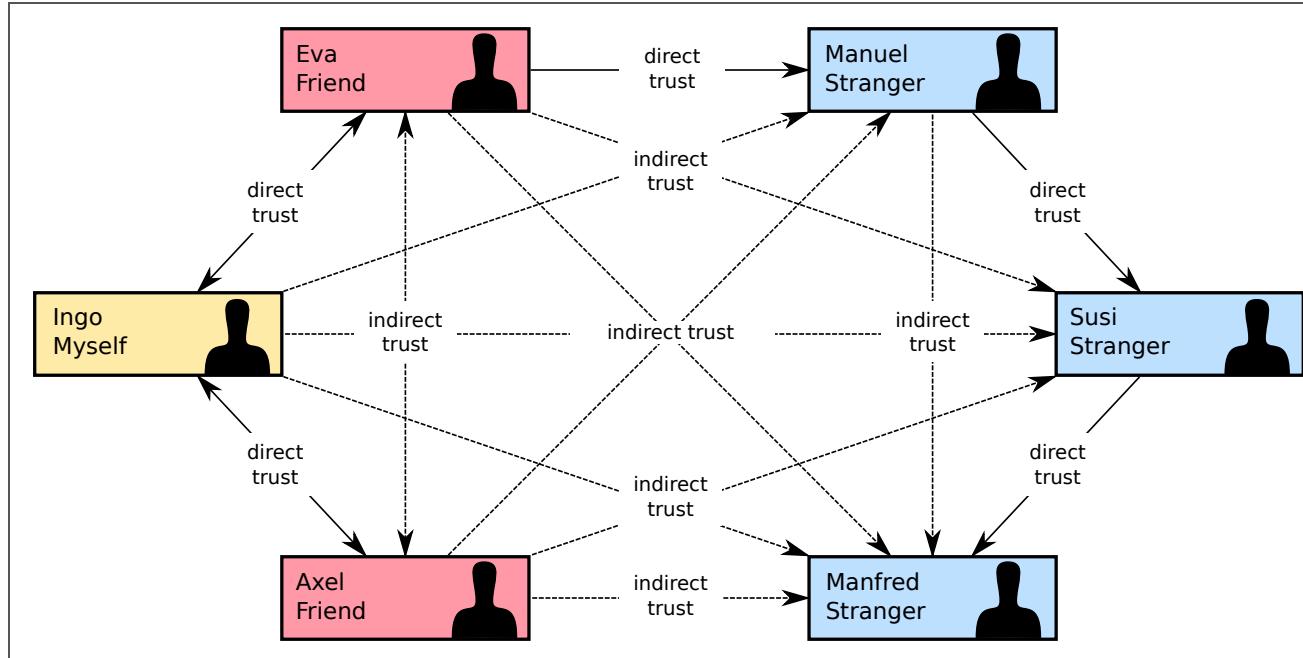
Sinadura digitalak erabilita ere:

- Nola dakigu sinadura bat esaten duenarena dela?
- Nola bermatzen du Zertifikazio Autoritate batek hori horrela dela?
- Ezin gara fidatu Zertifikazio Autoritate batek bermatu duen sinadura batetaz?

# Sinaduren konfidantza (Web of trust)

- PGP, GnuPG eta horrelakoak erabiltzen dira
- Erabiltzaile batek bermatzen du, bere gako pribatuarekin sinatuz, beste erabiltzaile baten gako publikoa fidagarria dela
- Konfidantza hedatzen doa, gakoak sinatzen dituzten erabiltzaileei ematen diegun konfidantzaren arabera

# Web of trust



# Konfidantza mailak

- Ezezaguna: erabiltzaile horrek sinatzen duenaz ez gara fidatzen (ezezaguna delako)
- Eza: erabiltzaile horrek sinatzen duenaz ez gara fidatzen (Badakigulako txarto egiten duela)
- Marginala: konfidantza marginala duten bi erabiltzailek sinatutako klabeengan konfidantza dugu
- Osoa: Erabiltzaile horrek sinatzen duen guztiaz fidatzen gara

# Public Key Infrastructure (PKI)

Erakundeak/pertsonak beren gako publikoekin lotzeko aukera ematen duen azpiegitura

- Web of Trust: PKI autoritate zentralik gabeko PKI-a, edonork ziurta dezake beste baten gako publikoa
- Ziurtagiriak: aginte zentrala duen PKI-a, CA-ek (Certification Authority) soilik eman dezakete bermea

# Ziurtagiri digitalak

- Erakunde batek (AC) erabiltzailea/erakundea (bere gako publikoa) benetan esaten duena dela bermatzen du (AC-rekiko daukagun konfidantzaren araberakoa)
- Gako publiko guztiak guk gorde beharrean, AC-ak gordetzen ditu

# Ziurtagiri digitalak

- CA-ak ziurtagiri digitala argitaratzen du
- Ziurtagiri digitalean CA-ak bere gako pribatuarekin erabiltzaile/entitatearen gako publikoa sinatzen du

# Erregistro Agentzia

- CA-rekiko independientea
- Erabiltzaile/erakundearen identitatea bermatu ziurtagiria sortu baino lehen
- Aldundiak, Gizarte Segurantza, Zuzenean,...

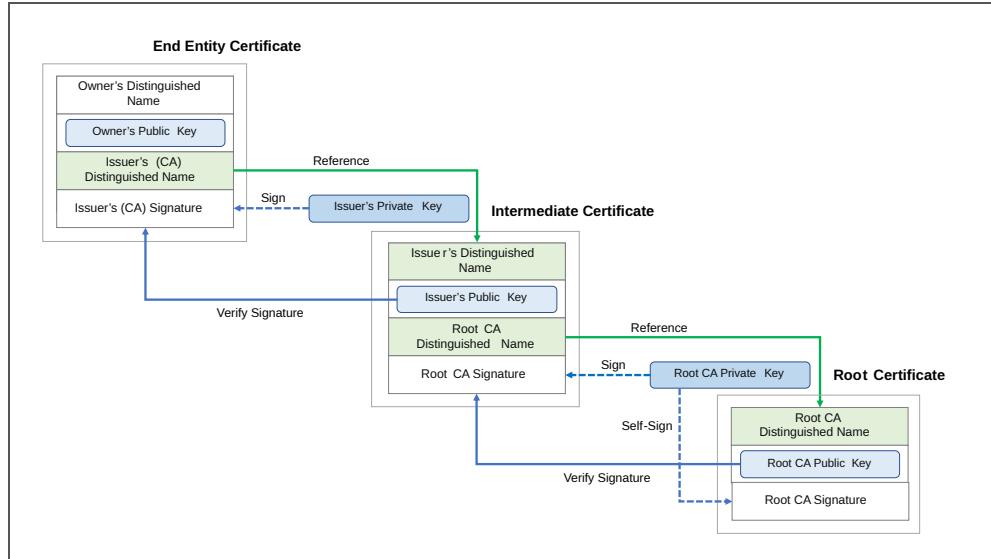
# Ziurtagiri digitalak: X.509

- International Telecommunication Union (ITU): [X.509](#)
- Nortasun bat (pertsona, erakundea...) eta gako publiko bat dauzka
- AC batek sinatua - ziurtagiria duen pertsona/erakundeak:
  - Bere gako pribatuarekin sinatu ahal du (Sinadura hori bermatua -AC-ak sinatua- dagoen gako publikoarekin konprobatu ahal da)
  - Komunikazio seguruak ezarri (SSL, ...)
- AC-ak bere datu basean gorde behar du: Distinguished Name zerrenda bat, eta azpiko CA-en zerrenda bat

# Ziurtagiri digitalak: X.509

- Konfidantza katea (Certification path validation algorithm)
- Certificate Revocation List (CRL)

# Konfidantza katea



[https://upload.wikimedia.org/wikipedia/commons/0/02/Chain\\_Of\\_Trust.svg](https://upload.wikimedia.org/wikipedia/commons/0/02/Chain_Of_Trust.svg)

# Certificate Revocation List (CRL)

Ezeztatutako ziurtagirien zerrenda publiko bat, CA-k mantentzen duena

Ezeztatzea: AC-ak adierazten du ziurtagiri hori ez dela fidagarria

# Certificate Revocation List (CRL)

RFC 5280-an definitua

ezeztatzeko arrazoi posiblak: unspecified, keyCompromise, cACompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL, privilegeWithdrawn, aACompromise

# OCSP (Online Certificate Status Protocol)

- [RFC 2560](#)
- Ziurtagiri digital baten egoera online baliozkotzea
- CRLs bidezko egiaztapena baino eraginkorragoa: CRL-ak gero eta gutxiago erabiliak
- Abantaila: etengabe egunерatzea
- Desabantaila: konexioaren beharra egiaztapenerako

# OCSP (Online Certificate Status Protocol)

- Zerbitzua ematen duen AC bakoitzak OCSP zerbitzari bat mantentzen du
- Zerbitzu honek eskaera estandarizatu bat igortzen duten eta erantzuna interpretatzen dakin bezero-aplikazioei erantzuten die

# Ziurtagiri egitura

Certificate

Version Number

Serial Number

Signature Algorithm ID

Issuer Name

Validity period

Subject name

# Ziurtagiri egitura

Subject Public Key Info

Public Key Algorithm

Subject Public Key

...

Certificate Signature Algorithm

Certificate Signature

# Ziurtagiri egitura

Distinguished Name

- C: country
- SP: state or province
- Locality: L
- Organization: O
- Organizational Unit: OU
- Common Name: CN

# Ziurtagiri egitura

IZENPE

Izenpe ziurtagiriak deskargatzea

Ziurtapen-politika: certification practice statement

# Ziurtagiri egitura

<b>Izenpe.com</b>
Identity: Izenpe.com
Verified by: Izenpe.com
Expires: 13/12/37
<a href="#">Details</a>
<b>Subject Name</b>
C (Country): ES
O (Organization): IZENPE S.A.
CN (Common Name): Izenpe.com
<b>Issuer Name</b>
C (Country): ES
O (Organization): IZENPE S.A.
CN (Common Name): Izenpe.com
<b>Issued Certificate</b>
Version: 3
Serial Number: 00 88 87 5A 16 48 5F BF E1 CB F5 8B 07 19 E6 7D
Not Valid Before: 2007-12-13
Not Valid After: 2037-12-13
<b>Certificate Fingerprints</b>
SHA1: 2F 78 3D 25 52 18 A7 4A 65 39 71 B5 2C A2 9C 45 15 6F E9 19
MD5: A6 88 CD 85 80 DA 5C 50 34 A3 39 90 2F 55 67 73
<b>Public Key Info</b>
Key Algorithm: RSA
Key Parameters: 05 00
Key Size: 4096
Key SHA1 Fingerprint: C4 52 72 20 A9 58 C9 6E 9D 4B F2 0B 21 12 3C EB 3A 0B 6B 6F
Public Key:
30 82 02 0A 02 82 02 91 00 C9 D3 7A CA 0F 1E AC A7 86 E8 16 05 6A B1 C2 B1 45 32 71 95 D9 FE 10 5B CC 99 15 D4 81 A2 26 77 89 58 AD D6 EB 0C B2 41 7A 73 6E 60 D8 7A 78 41 E9 08 88 12 7E 87 2E C3 8C 34 C5 95 7E 75 C2 3C 26 8A 51 47 20 98 93 A1 98 03 F3 0B 85 45 9A 04 05 87 22 BC 8C 43 FE 26 8A 51 47 FC 84 19 81 88 93 A2 85 F3 0D 74 85 CC 06 C2 CB A9 0F 44 E5 18 41 CF E1 86 A7 CA 09 6A 9F BC 4C 80 66 33 5A A2 85 E5 98 35 A9 02 5C 16 4E F0 E3 A2 ED 7B 70 D7 02 D6 ED 87 18 28 2C 04 24 4C 77 E4 4B 8A 1A C6 3B 9A D4 0F CA FA 75 D2 01 40 5A 8D 79 BF A6 05 46 F1 A8 16 EC 47 A4 17 02 03 01 00 01
<b>Subject Alternative Names</b>
Email: info@izenpe.com
Directory Name: OfIZENPE S.A. - CIF A01337260-RMervitoria-Gasteiz T1055 F62 58, STREET=Avda del Mediterraneo Etorbidea 14 -01010 Vitoria-Gasteiz
Critical: No
<b>Basic Constraints</b>
Certificate Authority: Yes
Max Path Length: Unlimited
Critical: Yes
<b>Key Usage</b>
Usages: Certificate signature ↗ Revocation list signature
Critical: Yes
<b>Subject Key Identifier</b>
Key Identifier: 1D 1C 65 0E A8 F2 25 7B B4 91 CF E4 B1 B1 E6 BD 55 74 6C 05
Critical: No
<b>Signature</b>
Signature Algorithm: 1.2.840.113549.1.1.11
Signature Parameters: 05 00
Signature:
78 A6 0C 16 4A 9F E8 88 3A C0 C8 0E A5 16 7D 9F B9 48 5F 18 8F 0D 62 36 F6 CD 19 6B AC AB 05 F6 91 7D 92 E1 60 AE TA 6B 09 AA C6 29 EE 68 49 67 30 80 24 7A 31 16 39 5B 7E F1 1C 2E DD 6C 09 AD F2 31 C1 81 EC BE 6D 26 E6 IC E4 42 20 9E 47 8B AC 83 59 70 2C 35 D6 AF 36 34 B4 CD 3B F8 32 AB EF E3 78 89 FB A7 8C E1 B9 7B 3C DE BE 1E 79 84 CE 9F 70 0E 59 C2 35 2E 90 2A 31 D9 E4 45 7A 41 A4 2E 13 9B 34 0E 66 23 A7 1F 4B 0D 35 46 9B B2 10 6B E4 A5 31 C2 04 56 2E 19 81 10 C9 56 43 FC EA 5A 10 CE 11 57 EE EP 56 80 3E 9D A3 3C 4C 72 C2 57 C4 AD D4 C4 3B 9A D4 0F CA FA 75 D2 01 40 5A 8D 79 BF 88 C7

# Erro-ziurtagiria

Subject Name == Issuer Name

Bere burua sinatzen du: konfidantzaren jatorria da (Entitate horrekiko  
zuzeneko konfidantza dugu, ez dago kanpoko gako pribaturik bere gako  
publikoa sinatzen duena)

# Ziurtagiria

- Azken erabiltzailearen ziurtagiria (pertsona juridikoa)
- Software-sinaketaren ziurtagiria
- SSL zerbitzariaren ziurtagiria

# Implementazioa

- Sistema eragileek eta nabigatzaileek erro-ziurtagiriak dituzte, berezko konfidantza hartuz
- Firefox OCSP query responder, Izenpe

# Implementazioa

The image shows two overlapping windows from the Firefox interface. The background window is titled 'Firefox Data Collection and Use' and contains sections for privacy notices, security features like Deceptive Content and Dangerous Software Protection, and certificate management. The foreground window is a 'Certificate Manager' dialog titled 'Authorities' which lists several certificate authorities with their names and security devices.

**Certificate Manager**

Authorities

Certificate Name	Security Device
iTrustChina Co.,Ltd.	Builtin Object Token
vTrus ECC Root CA	Builtin Object Token
vTrus Root CA	Builtin Object Token
IZENPE S.A.	Builtin Object Token
Izenpe.com	Builtin Object Token
Japan Certification Services, Inc.	Builtin Object Token
Security Devil CA 11	Builtin Object Token

View... Edit Trust... Import... Export... Delete or Distrust... OK

**Firefox Data Collection and Use**

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.

**Privacy Notice**

- Allow Firefox to send technical and interaction data to Mozilla [Learn more](#)
- Allow Firefox to make personalized extension recommendations [Learn more](#)
- Allow Firefox to install and run studies [View Firefox studies](#)
- Allow Firefox to send backlogged crash reports on your behalf [Learn more](#)

**Security**

**Deceptive Content and Dangerous Software Protection**

- Block dangerous and deceptive content [Learn more](#)
- Block dangerous downloads
- Warn you about unwanted and uncommon software

**Certificates**

- Query OCSP responder servers to confirm the current validity of certificates [View Certificates...](#)
- [Security Devices...](#)

# Let's encrypt

Ziurtagiriak doan ematen dituena CA-a, HTTP konexio guztiak zifratuak izan daitezen

<https://letsencrypt.org/>

# Komunikazio seguruak

TLS/SSL - X.509 ([RFC 5280](#)) protokoloan oinarritutakoak:

- HTTPS: web
- S/MIME, SMTP, POP, IMAP: email
- EAP-TLS: wifi
- LDAP: kautotzea
- VPN (OpenVPN): sare seguruak

# Transport Layer Security (TLS)

- Internet Engineering Task Force (IETF)-k proposaturiko estandarra
- Oraingo bertsioa 1.3 (RFC 8446)
- SSL (Secure Sockets Layer) ordezkatzen

# Transport Layer Security (TLS)

1. TLS hasiera
2. TLS hand-shake
3. TLS konexioa

# TLS hasiera

- Bezeroak zerbitzariari TLS erabiltzeko eskatzen dio
- HTTP: 80 portutik 443 portura aldatu
- Email: STARTTLS komandoa

# TLS hand-shake

- Bezeroak zerbitzariari balio zaizkion algoritmoen zerrenda bat aurkezten dio: simetrikoak, asimetrikoak, laburpen
- Zerbitzariak zerrenda horretatik balio zaizkionak hautatzen ditu
- Zerbitzariak bezeroari ziurtagiria aurkezten dio, bezeroak CA-ri esker baliozkotzen duena

# TLS hand-shake

- Bezeroak saio gako bat sortzen du (Zifraketa simetrikoak):
  - Bezeroak ausazko zenbakia ekoizten du, zerbitzariaren gako publikoarekin zifratzen du eta zerbitzariari bidaltzen dio. Bai bezeroak bai zerbitzariak gakoa sortzen dute zenbaki horretatik abiatuta
  - Diffie-Hellman algoritmoa erabiliz gako amankomun bat sortzen dute bezeroak eta zerbitzariak

# TLS konexioa

- hand-shake ondo atera bada soilik
- Datuak sesio gakoarekin zifratzen dira eta osotasuna adostutako laburpen algoritmoekin bermatzen da
- Egoera mantentzen duen konexioa da ([stateful](#))

# SSH (Secure Shell)

- Urruneko zerbitzarietara konektatzeko erabiltzen den protokolo kriptografikoa
- Trust On First Use (TOFU): konexioa ezartzeko gure klabe publikoa urruneko zerbitzarian jartzea nahiko dugu
- Hortik aurrera, TLS moduan, saio gako bat erabiltzen da datuak transmitizeko

# SSH: erabilpenak

- Urruneko makina batean sartu eta komandoak exekutatu
- SFTP bidezko artxiboen transferentzia
- SCP bidez datuak kopiatu
- Tunelak
- Port fowarding
- X11 (Grafikoak)

# 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\* transakzio bat desegin
- Osotasuna: ezin da\* blockchain-aren historia aldatu
- Kautotzea
- Pseudo-anonimatuua
- ...

# 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 desentralizatua eta gardena
- (Politikoki) Moneta-sistema:
  - Austriar eskolaren arabera, "diru onean" (Sound Money) oinarritua
  - 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

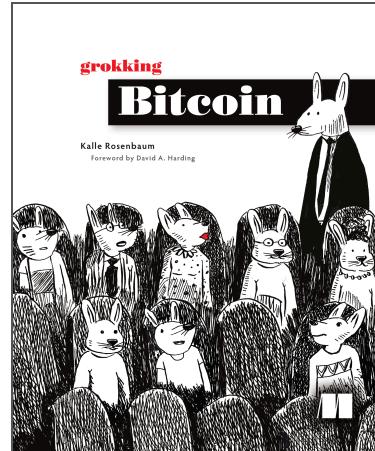
# Zer da Bitcoin?

Grokking bitcoin (Kalle Rosenbaum, 2019):

[GitHub](#)

[EHU liburutegia](#)

[Manning](#)



# Zer da Bitcoin?

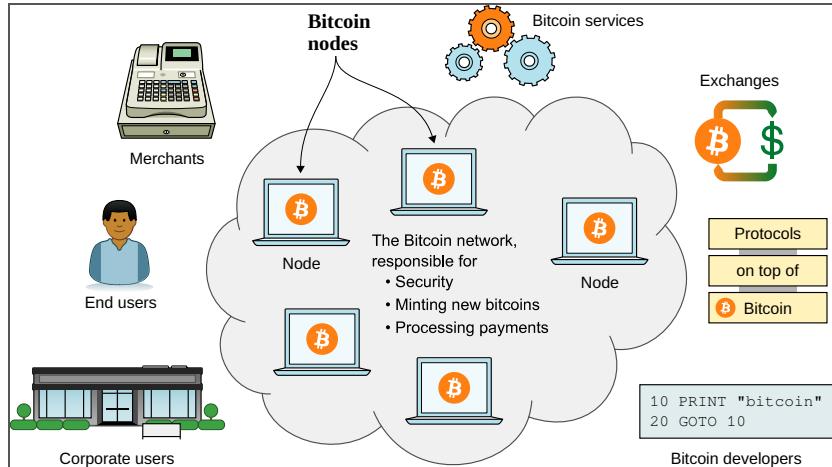
Diru digital sistema

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

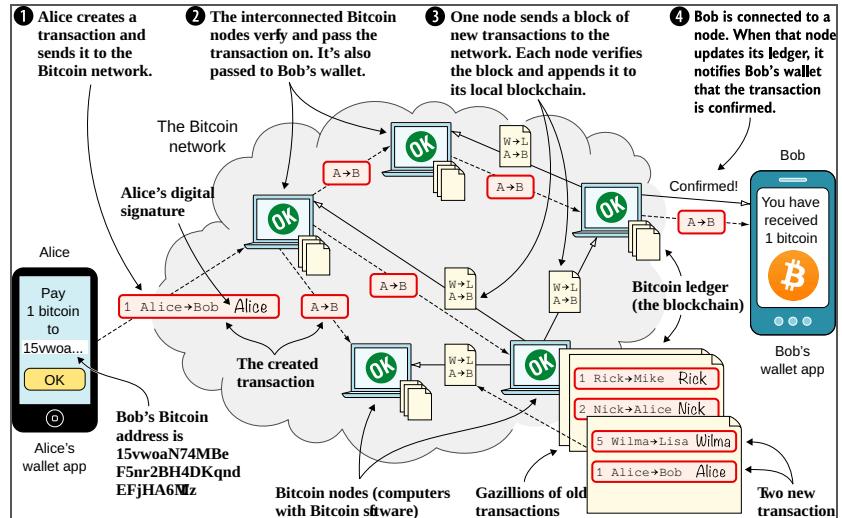
Zirkulazioan bitcoin berriak jarri, aurretik ezarritako abiaduran

# Bitcoin sarea

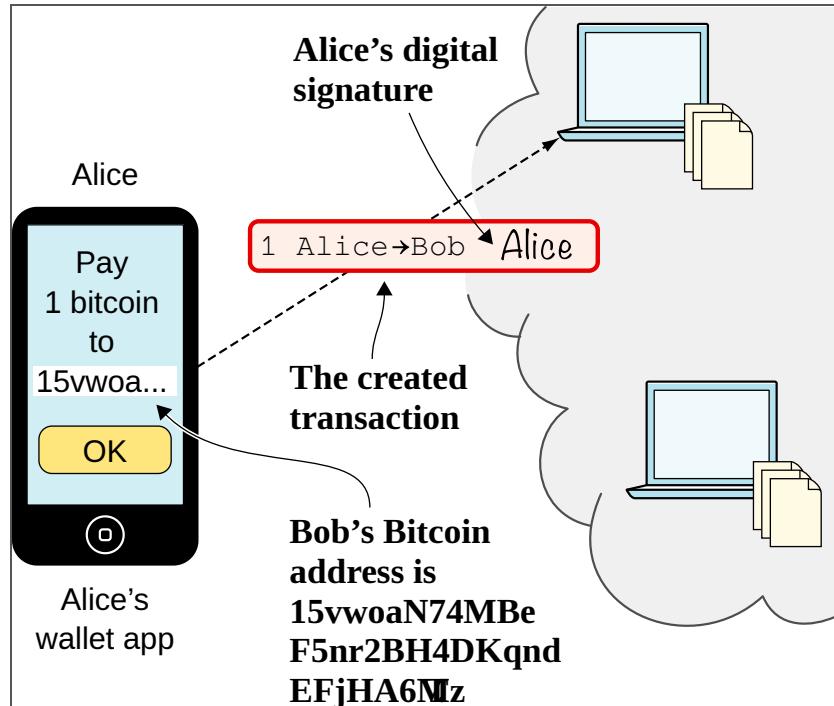
Kontabilitate-liburu elkarbanatua (Nodo guztiekin kopia bat dute)

Kontabilitate-liburuak egin diren transakzio guztiak ditu

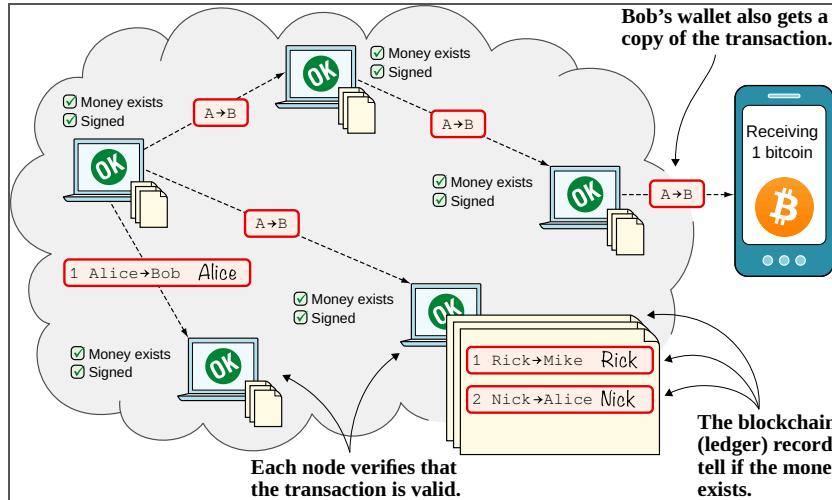
# Ordainketa



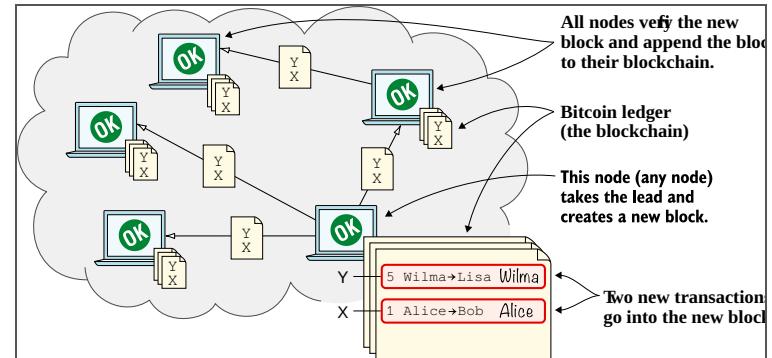
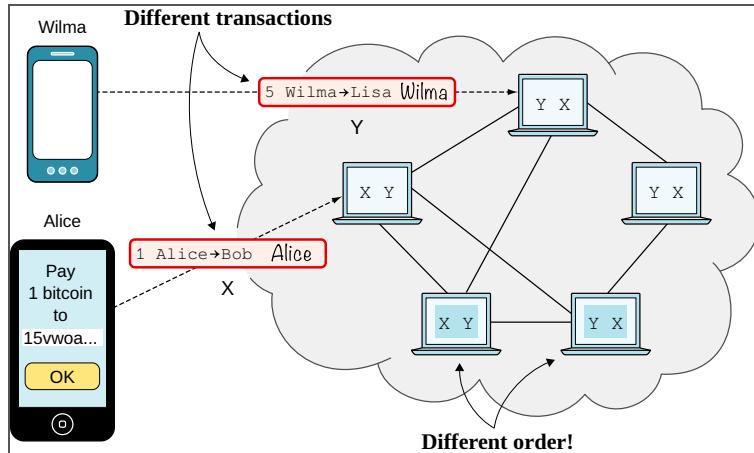
# (1) Transakzioak



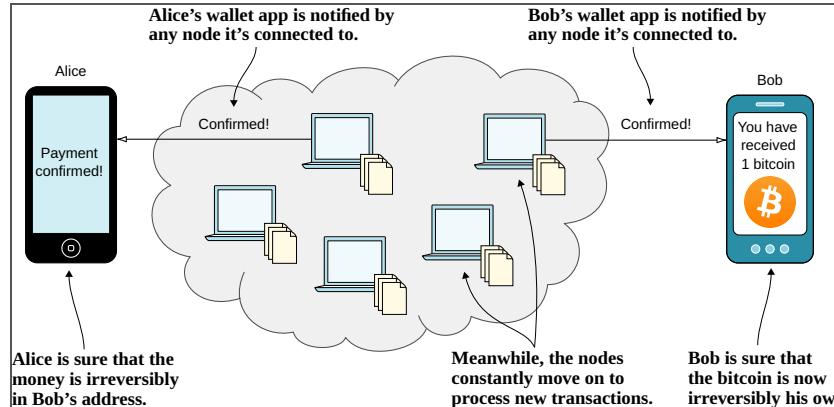
## (2) Sarea



# (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

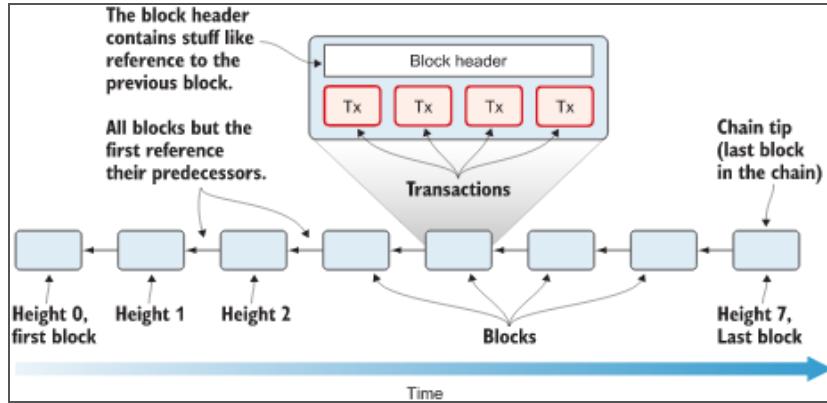
- Meatzariekin saria jasotzen dute (Bitcoin moduan) eta horrela Bitcoin-ak jaulkitzten dira
- Transakzioen komisio txikiak meatzariek ere jasotzen dituzte

# Bitcoin sarea

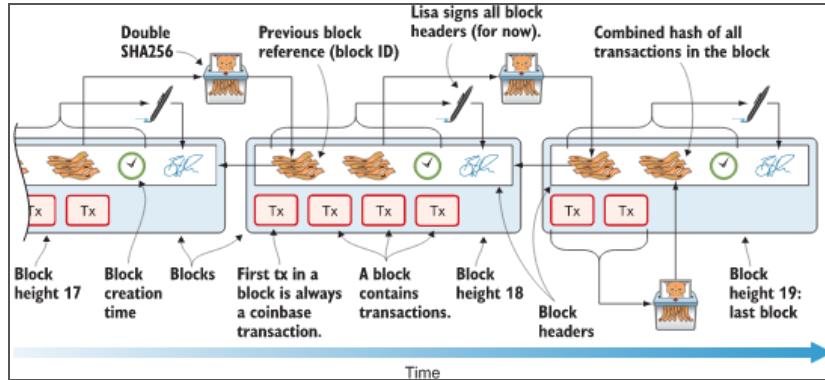
Laburpen zifraketa (Hash):

- **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

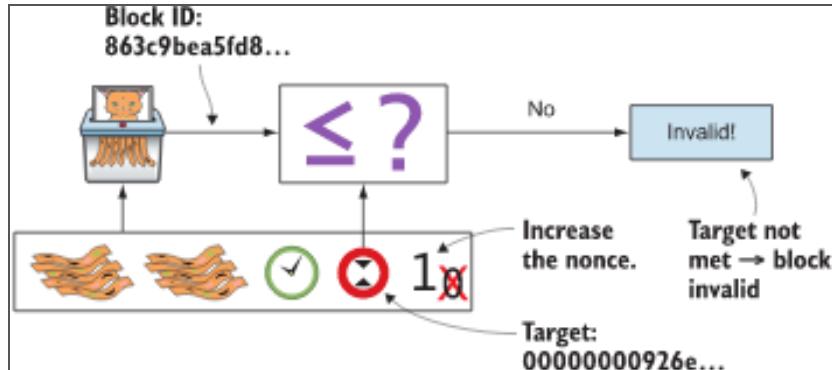
Balioztatu: gastu bikoitza ekidin, timestamp egokia, etab.--> hash bat sortu

Hash horrek aurreko hash guztiak dauzka

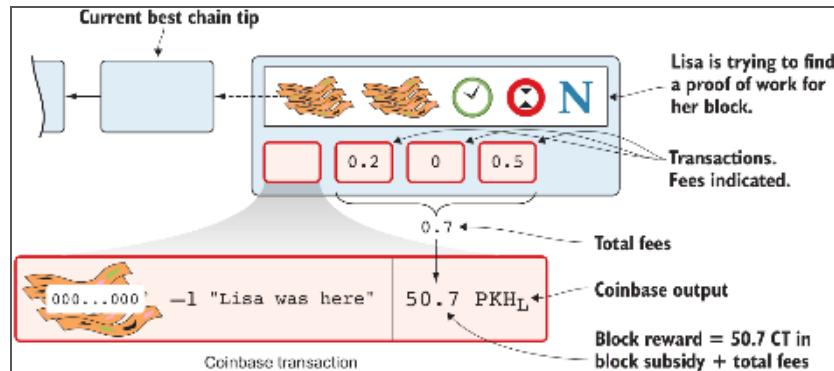
Baina hash hori **target** zenbakia baino txikiagoa izan behar du

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

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.

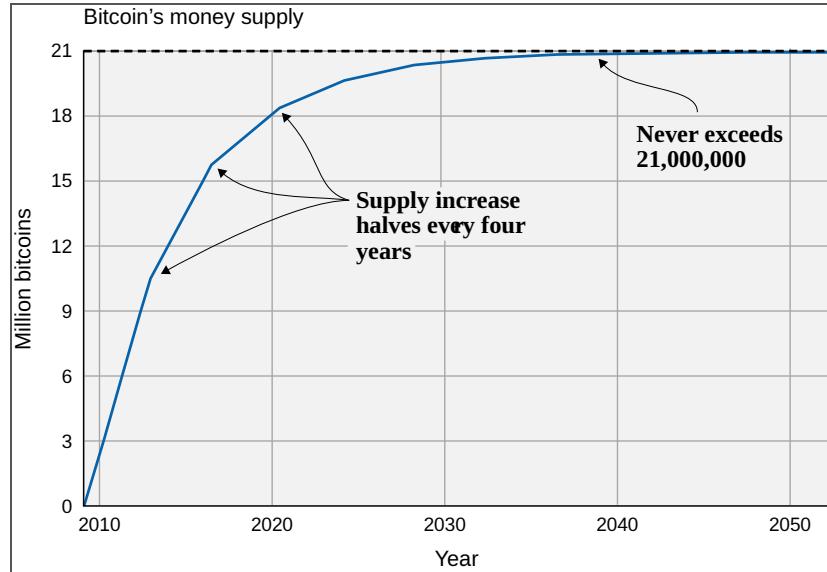
Its essence is a tendency to extrapolate from the personal realm to the macroeconomic one. To say that if something is good for me – if a practice is sound at the level of my family, business, etc. – it must also be good for the state, government, humanity at large. For example, yes, parsimony is a good 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 are invested in Bitcoin, or for some reason you are elated every time its dollar exchange rate rises, you have

# 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