



BLOCKCHAIN:

kriptotxanpenez haratago,

teknologia ezagutu eta

trebatzeko tailerra.

Urko Larrañaga Piedra

Aurkezpena

- Zer da UEU?

- Euskal Unibertsitatea sortzea helburu
- Euskara oinarri
- Euskal komunitate zientifiko-intelektuala bildu

Aurkezpena

- Nor gara? Zer espero dugu ikastaro honetatik?
- Urko Larrañaga Piedra
 - Izertis
 - Stackoverflow-eko erabiltzailea
- Helburua
 - Blockchain azaldu eta interesa sortu
 - Tresna ezberdinak ezagutarazi
 - Aplikazio deszentralizatu baten garapena
 - Guztion parte-hartzea sustatu



BLOCKCHAIN

-UEU: Udako ikastaroa (2018)-

I. atala

Oinarriak eta Blockchainen aplikazioa

SARRERA

Zer dakigu
Blockchainen
inguruan?

Zein aplikazio ditu?

- https://www.ozy.com/need-to-know/blockchain-the-new-technology-of-trust/81602?utm_campaign=diaria3001&utm_medium=email&utm_source=newsletter
- <https://juegosrobotica.es/blockchain/>

SARRERA

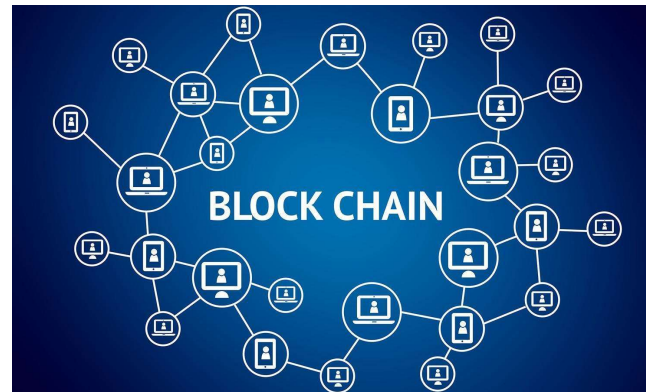
- Bitcoin

- 2009an sortutako kriptotxanpona
- Erabileraren goraldia
- Kriptotxanpon bat baino gehiago da



SARRERA

- Bitcoin
 - Irtenbide bat sistema zentralizatuari
 - Sare banatua
 - Informazio deszentralizatuia
 - Blockchain teknologia



SARRERA

- Blockchain

- Hasiara: Bitcoin

- Ondoren: bankuak eta kriptotxanponak

- Gaur egun

- Erabilera anitza

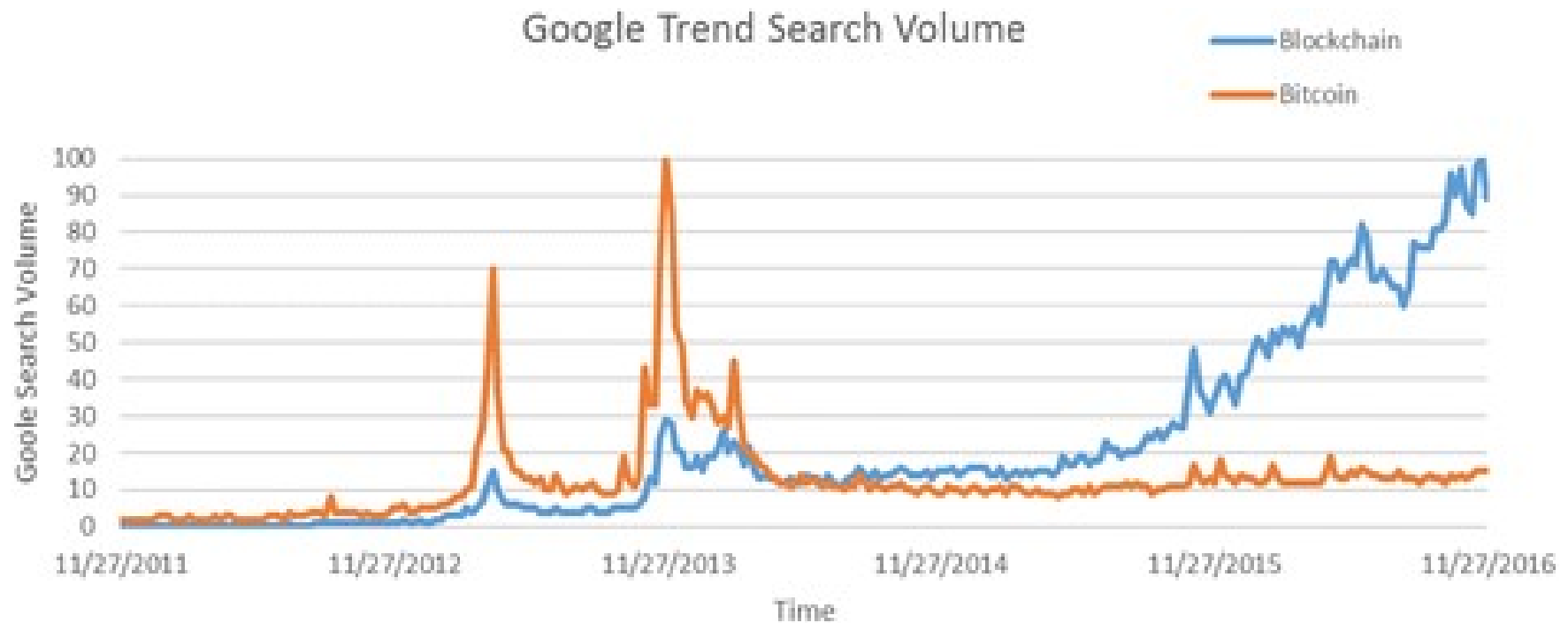
- ICOak

- Inplementazio ezberdinak



SARRERA

- Bitcoin eta Blockchainen bilaketak Googlen



SARRERA

- Blockchaineekin lotutako argitalpenak

<i>Urtea</i>	<i>WebOfScience</i>	<i>SSRN</i>
2014 aurretik	0	0
2014	0	6
2015	4	22
2016	11	79

SARRERA

- Blockchain

- Heldutasun gabeko teknologia
- Irtenbide edo aplikazio erreal ezagun gutxi
- Konpondu ditzakeen bestelako arazoak
 - Jabetza intelektuala
 - Bozketa elektronikoaren ondoriozko hauteskunde iruzurra
 - Identitate digitala
 - Trazabilitatea



BLOCKCHAIN

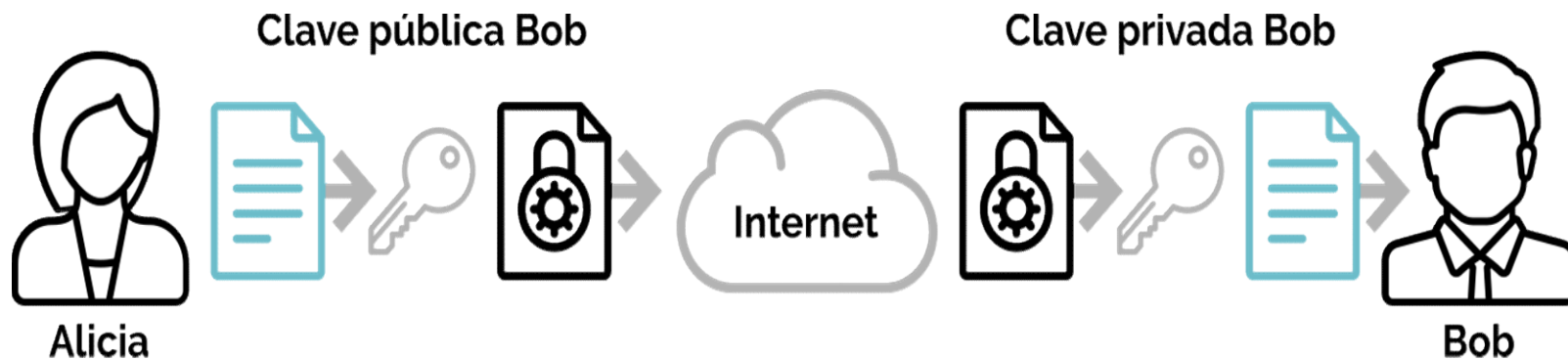
- Kriptografia
 - Hash algoritmoak

<i>Mensaje</i>	<i>Resultado hash (hexadecimal)</i>
<i>MASTERSIA</i>	<i>cf5236358ac7ebf9465d2b4e2a34a12f96ed3cd0</i>
<i>MASTER SIA</i>	<i>8176fc2467f9ef8b6fca6ef4ae54357e6419df2a</i>

BLOCKCHAIN

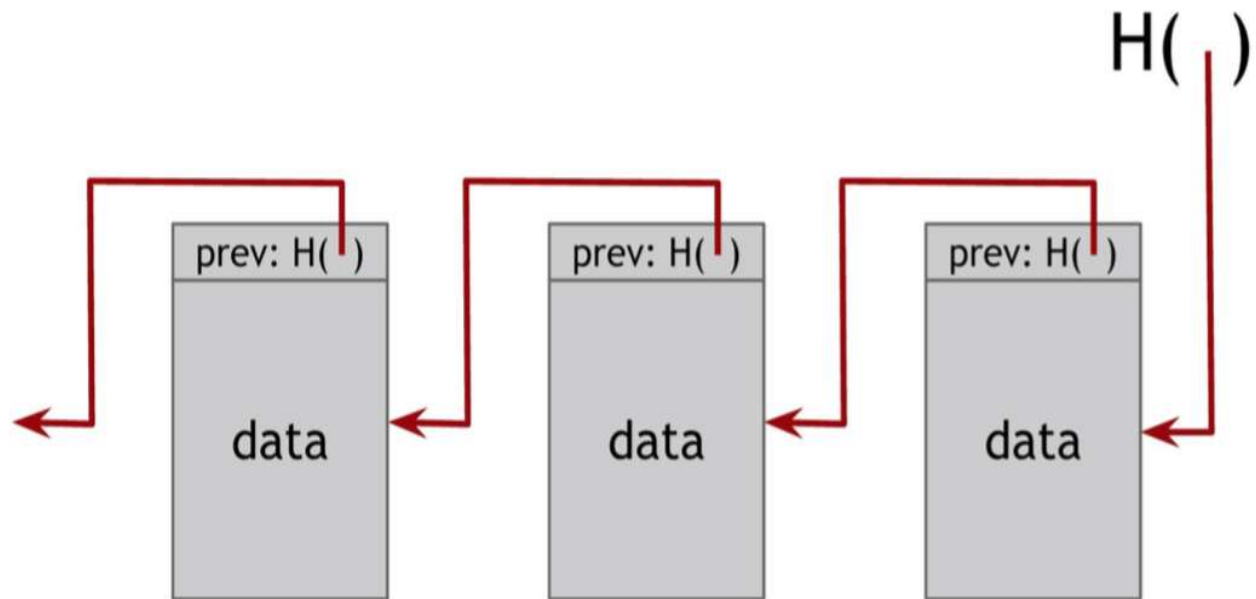
- Kriptografia

- Kriptografia simetrikoa
- Kriptografia asimetrikoa



BLOCKCHAIN

- Bloke katea



BLOCKCHAIN

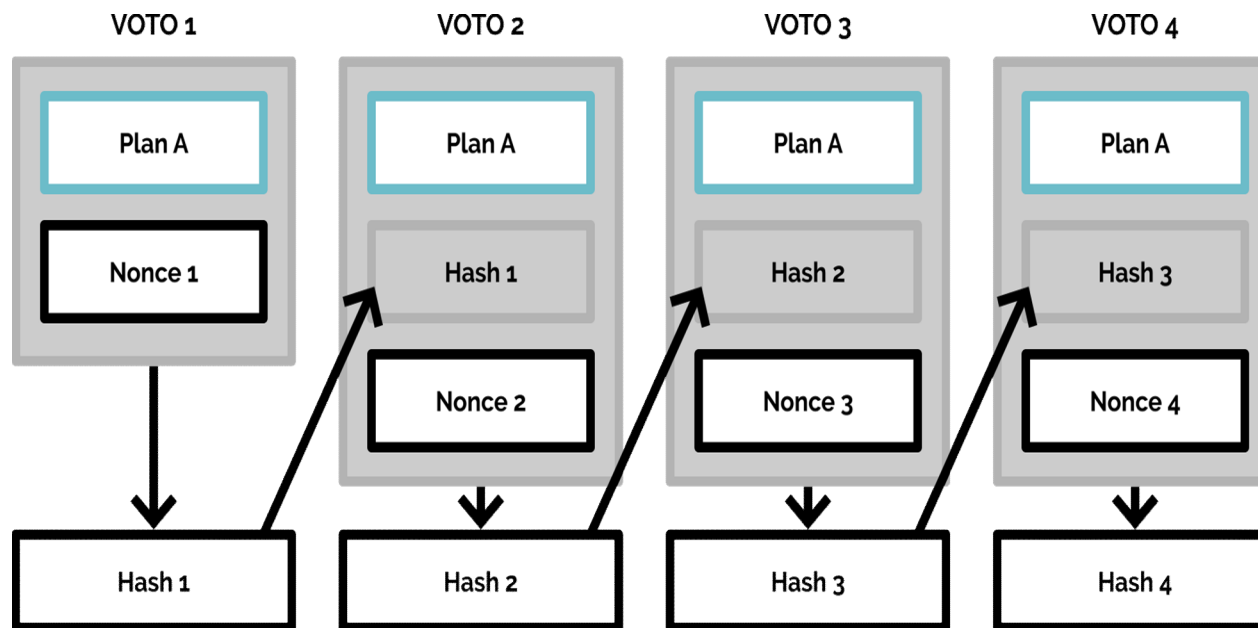
- Kontsentsua
 - Ebazten duen arazoa



BLOCKCHAIN

- Kontsentsua

- Bozketen katea

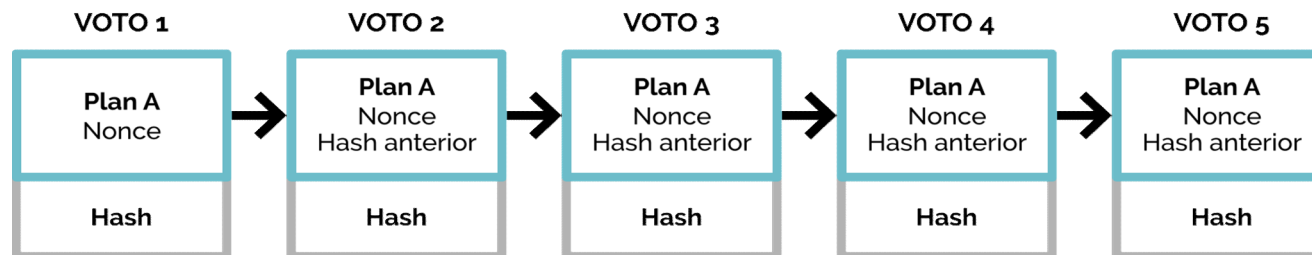


BLOCKCHAIN

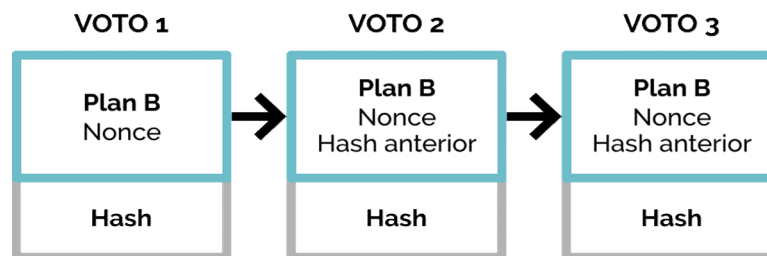
- Kontsentsua

- Kontsentsua adar bitan

Blockchain del plan A



Blockchain del plan B



BLOCKCHAIN

•Praktikan

- <https://github.com/anders94/blockchain-demo>
- <https://github.com/anders94/public-private-key-demo>

•Aplikazioak

- Enerchain
- B3i
- R3
- Provenance



BLOCKCHAIN

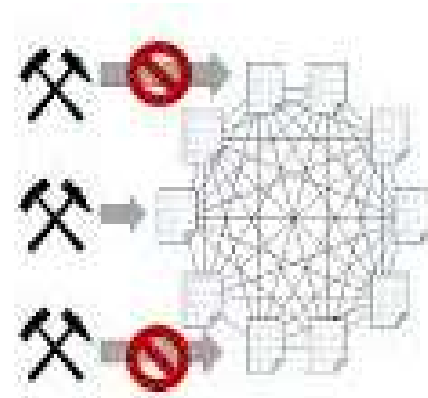
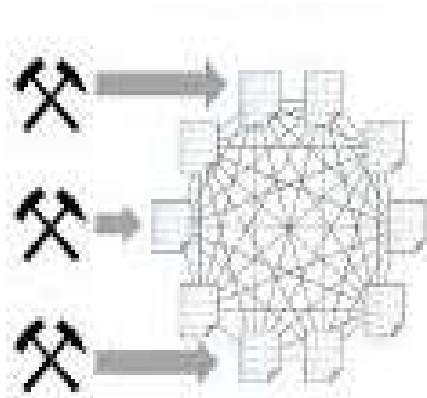
-UEU: Udako ikastaroa (2018)-

II. atala

Blockchain motak, minatua
eta ICOak

BLOCKCHAIN MOTAK

- Publikoak - permissionless
- Pribatuak - permissioned
- Hibridoak



BLOCKCHAIN MOTAK

- Publikoak - permissionless
 - Mugarik gabeko sarrera
 - Info publikoa
 - Anonimatua
- Pribatuak - permissioned
 - Partehartze mugatua
 - Kontrolatua → Partehartzaileak ezagutzen ditugu
 - Informaziora sarbide mugatua

BLOCKCHAIN

- Kontsentsu algoritmoak

- Bitcoin → Proof of Work (PoW) <https://blockchain.info/>
- Ethereum → Proof of Stake (PoS)
- Hyperledger Fabric → PBFT

BLOCKCHAIN

- Smart Contract

- Blockchainean exekutatuko den makina kodea



MINATUA

- Nola egin?
 - Hardware
 - Edozein ekipo: CPU edo GPU
 - HW espezializatua
 - Software prestatua
- Bakarrik, aukerarik badaukazu?
- Zer minatu?
- Bictoinen minatuaren “negozioa”?

MINATUA

- Hardware

- Ant min

- https://shop.bitmain.com/antminer_s9_asic_bitcoin_miner.htm

- Interfaze bat dauka

- Tamaina: zapata kutxa bat

- Esperientzia

- Mesfidantza

- Zarata → Poligono batera

- ASIC-ak arin hobetzen dira, GPUak luzera begira



MINATUA

- Hardware: <https://vimeo.com/240523807>
- Google “Bitcoin minado”



MINATUA

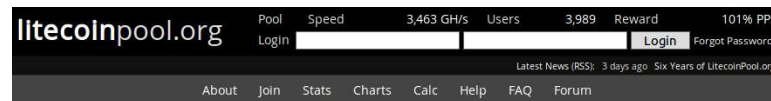
•Bakarrik, aukerarik badaukazu?

- Poolen sorrera

<https://www.litecoinpool.org/>

- Pool nagusiak

<http://blockchain.info/pools>



The screenshot shows the header of the litecoinpool.org website. It features a dark background with white text. On the left, the site name 'litecoinpool.org' is displayed. To its right, there are several statistics: 'Pool Speed 3,463 GH/s', 'Users 3,989', 'Reward', and '101% PPS'. Below these statistics, there is a 'Login' button and a 'Forgot Password?' link. At the bottom of the header, there is a navigation menu with links for 'About', 'Join', 'Stats', 'Charts', 'Calc', 'Help', 'FAQ', and 'Forum'. Additionally, there is a link for 'Latest News (RSS): 3 days ago' and 'Six Years of LitecoinPool.org'.

Welcome to litecoinpool.org

Mining litecoins since October 21, 2011

New to Litecoin mining? Read our [Beginner's Guide!](#)

Welcome to the first true pay-per-share (PPS) Litecoin pool. Some of our key features:

- Exclusive ultra-low-latency Stratum server implementation, written in C
- Support for Stratum over TLS, to prevent MITM attacks
- Merged mining (AuxPoW) of several altcoins, paying out in litecoins
- Support for the resume extension to Stratum
- Adaptive share difficulty ("vardiff"), with support for manual tuning
- Network of 8 geographically-distributed, redundant servers
- Detailed stats updated every few seconds
- Email notification of idle miners
- Fee-free automatic and manual (instant) payouts
- Two-factor authentication support
- Website and mining interface also accessible as Tor hidden services
- Extensive JSON API

The Reward System

Every valid share you submit to this pool is instantly credited to your account at the current pay-per-share (PPS) rate. This rate, expressed in litecoins, also takes into account merged-mined coins such as Dogecoin, resulting in higher payouts than a regular Litecoin pool.

MINATUA

- Zer minatu?

- <https://whattomine.com/>

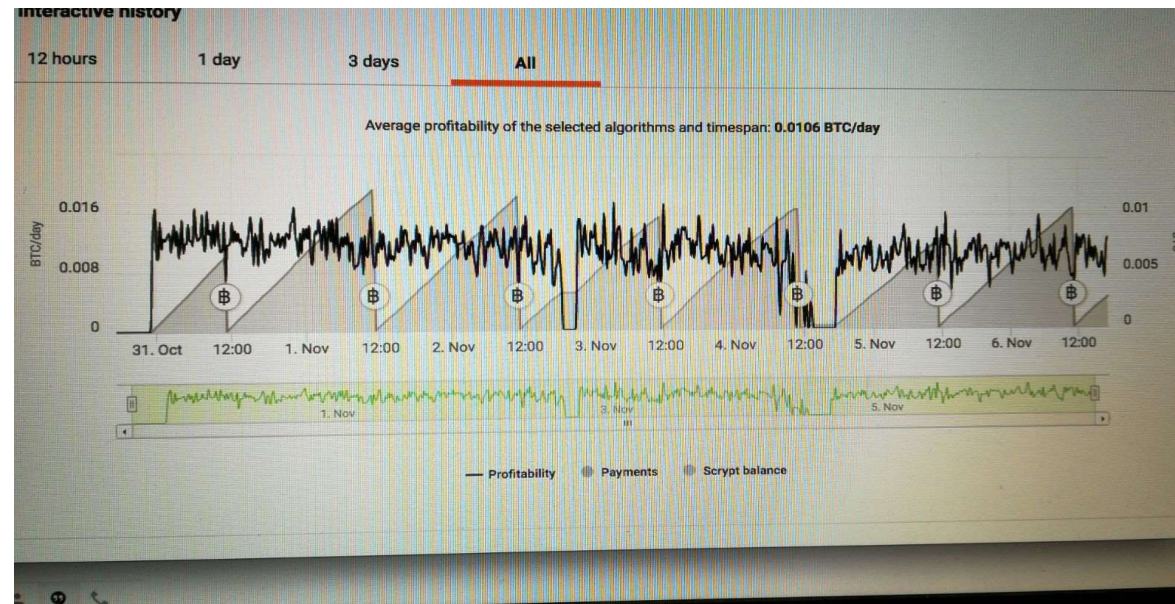
- <https://www.cryptocompare.com/>

MINATUA

- Marketplace espezializatuak

<https://www.nicehash.com/>

- Esperientzia

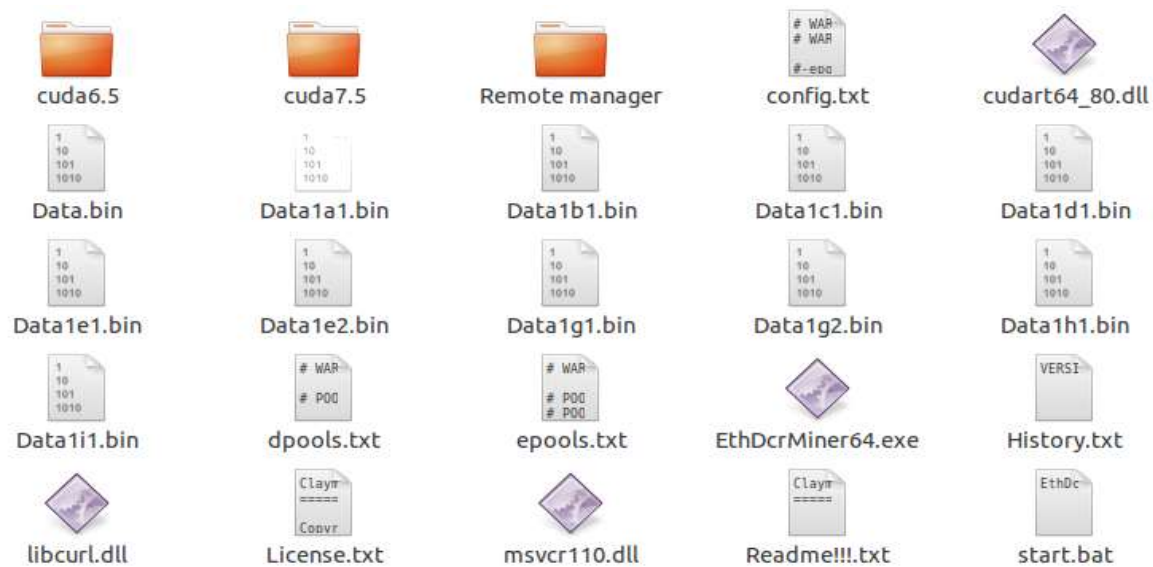


MINATUA

- Minatzeko softwarea

- "Claymore dual mining"

- https://mega.nz/#F!O4YA2JgD!n2b4iSHQDruEsYUvTQP5_w



MINATUA

- Softwarea

```
EthDcrMiner64.exe -epool us1.ethpool.org:3333 -ewal  
0xD69af2A796A737A103F12d2f0BCC563a13900E6F -  
epsw x -dpool stratum+tcp://dcr.suprnova.cc:3252 -  
dwal Redhex.my -dpsw x
```

MINATUA

- Zer dakizue Bitcoinen sortzaileari buruz?
- Minatuko zenukete?

ICOak

- ICO (Initial Coin Offering) crowdfundinga dira
 - Ekitaldi bat (crowdsale)
 - Finantzazioa lortzeko martxan jartzen da.
 - Token bat
 - Entitatearen zati bat ordezkatzeko du
 - Edozelako ondasun edo ondare bat ordezkatu dezake

• DAICO

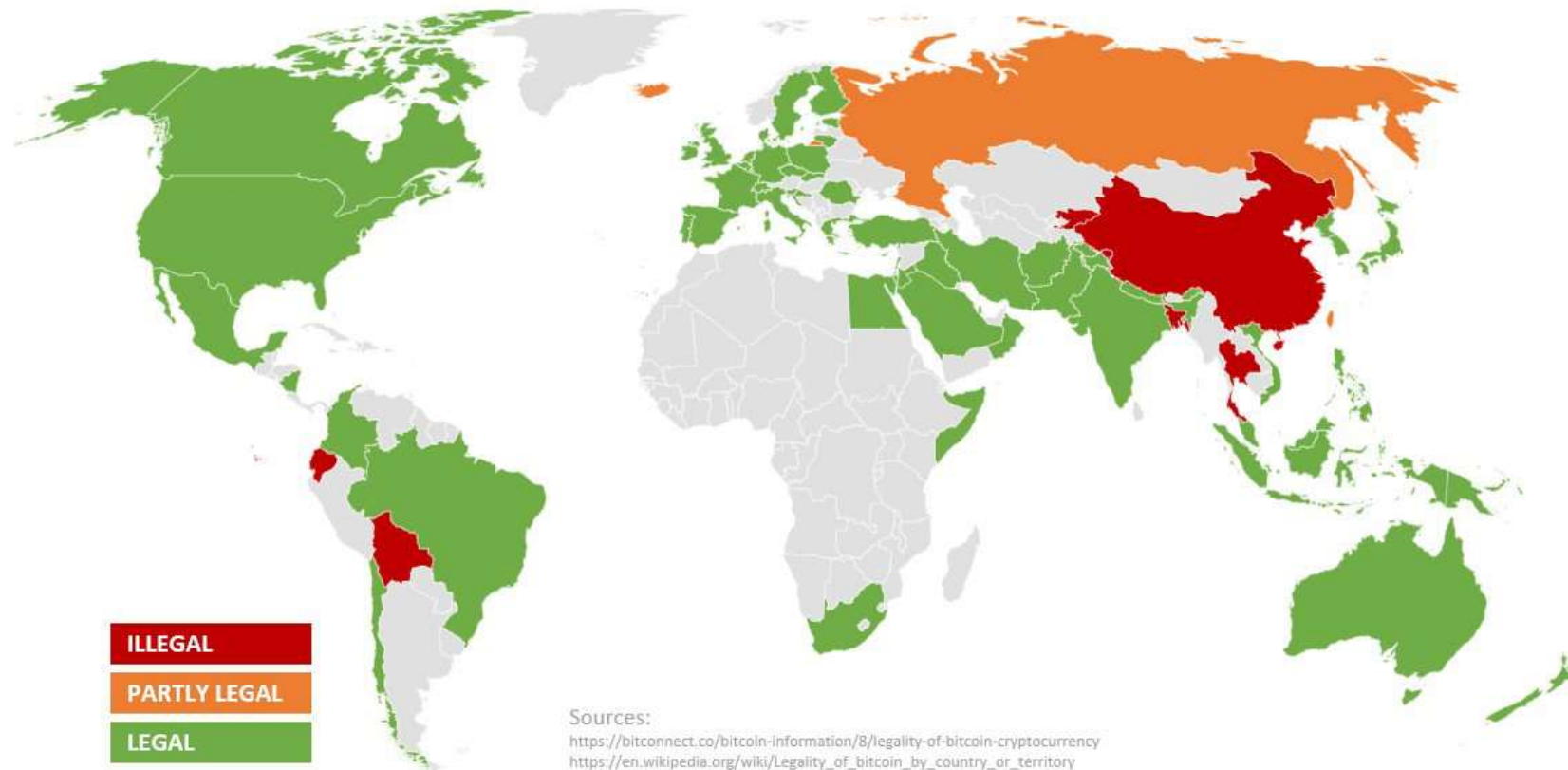
<https://icostats.com/>

<https://elementus.io/token-sales-history>



ICOak

•Kriptotxanponak



ICOak

ICO ROAD MAP



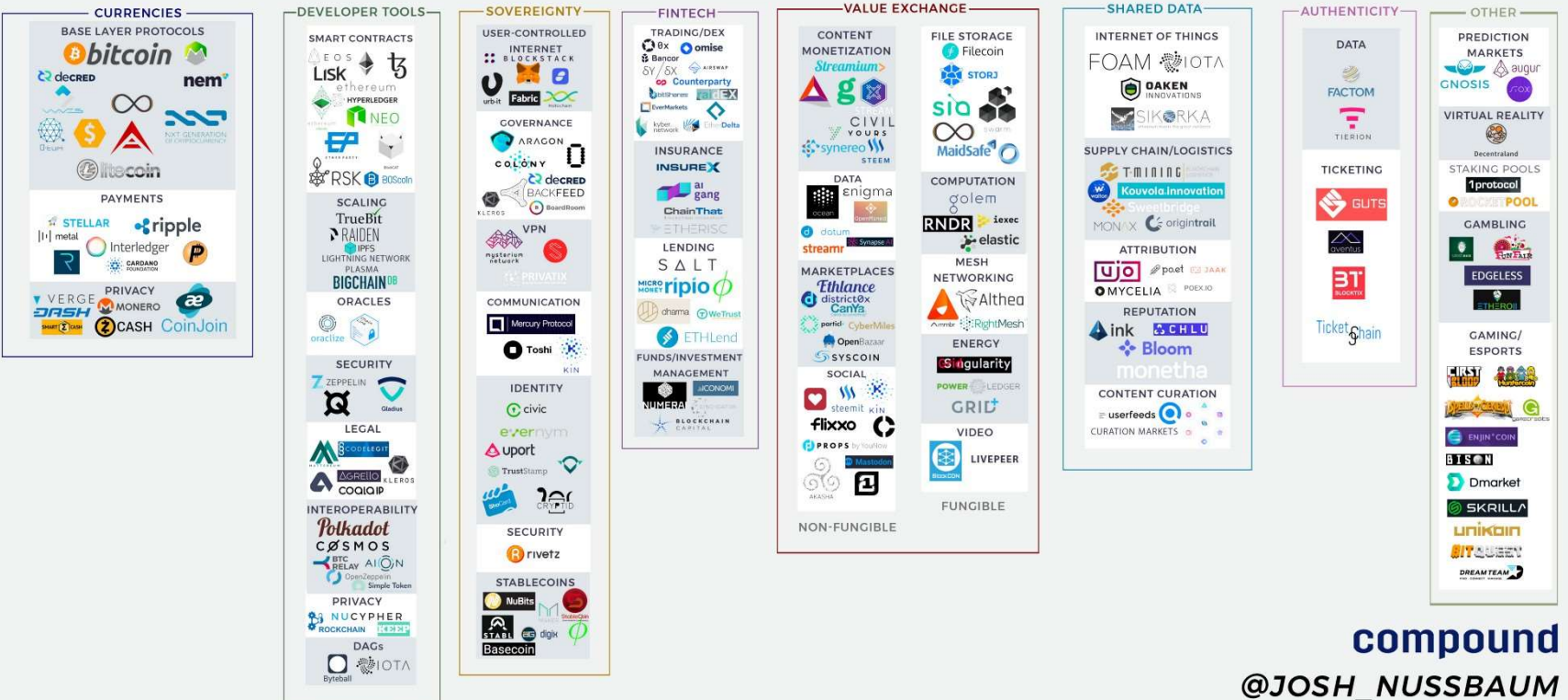
HAUSNARKETA

- ¿Etorkizunik badu?
- ¿Non erabiliko zenuke?



BLOCKCHAIN EKOSISTEMA

BLOCKCHAIN PROJECT ECOSYSTEM



compound
@JOSH_NUSSBAUM



BLOCKCHAIN

-UEU: Udako ikastaroa (2018)-
III. atala

Ethereum: zer da?

Metamask, Solidity eta Remix

ETHEREUM

- Zer da?

- Smart Contractak exekutatzen dituen plataforma deszentralizatua

- Nola erabili?

- Sare propioa eraiki
 - Egun dauden sareetara gehitu (Ropsten, Rinkeby...)
 - Nodo berri bat martxan jarriz edo ez
 - Geth
 - Parity
 - ...

ETHEREUM

- Nola funtzionatzen du?

- Helbideak
- Ethereum Virtual Machine

- Programazio lengoaia

- Solidity
- Ikasteko: <https://cryptozombies.io/>

DAPP baten garapena

1. Ideia
2. Diseinua
 1. Blockchain mota
 2. Inplementazioa
3. Smart Contracta
4. Aplikazioa (frontend-a)

DAPP baten garapena

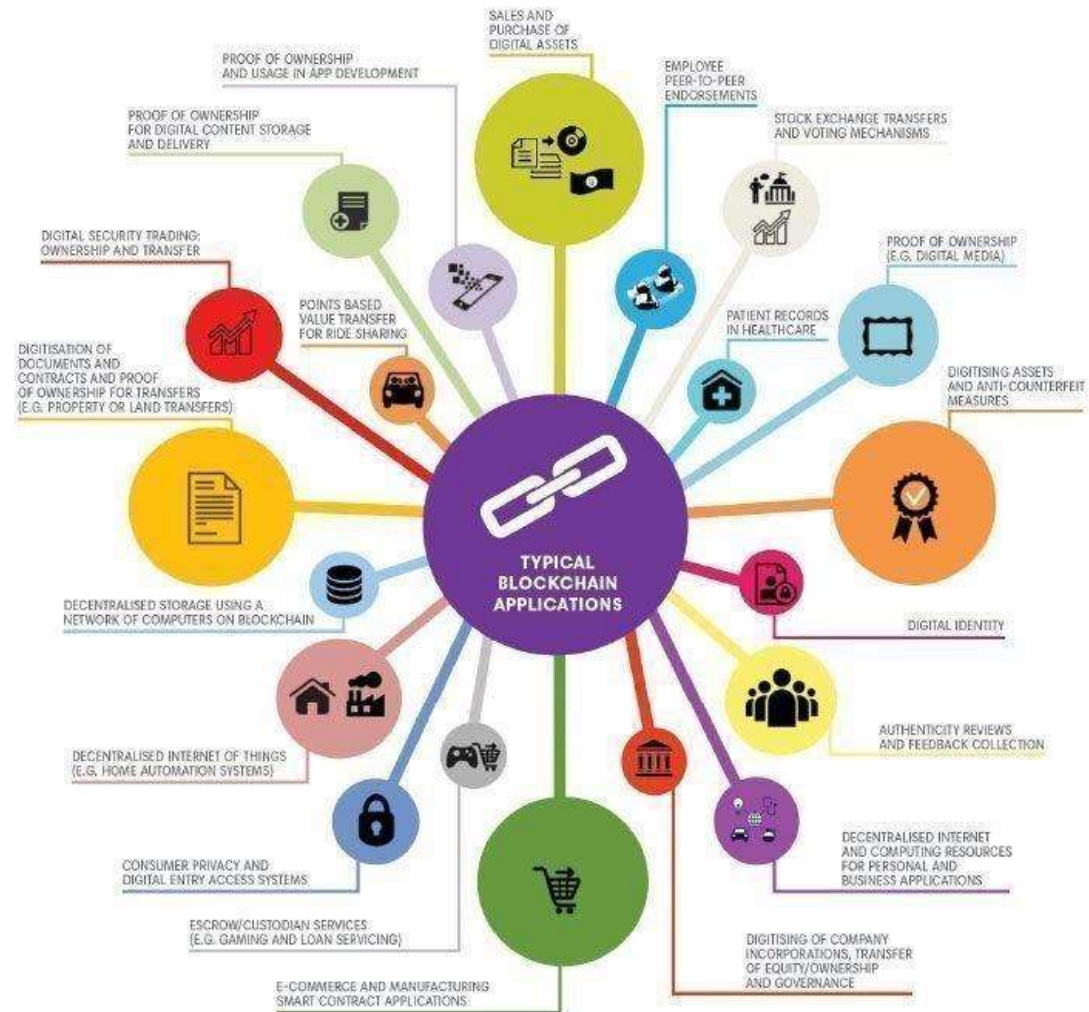
•Ideen zerrenda

•Gincana

•Bozketa elektronikoa

•Zenbatera arte nahi
dugu zerbaiten
garatzen sartu?

•Taldeka?



TRUFFLE & GANACHE

- Metamask

- Ethereumeko nodoetara konektatzeko tresna

- Remix

- Garapen ingurune bat

- Solidity



BLOCKCHAIN

-UEU: Udako ikastaroa (2018)-
IV. atala

Ethereum: Truffle eta Ganache

TRUFFLE & GANACHE

- Truffle

- Garapenerako Framework bat

- Ganache

- Lokalean Ethereumeko Blockchain bat sortzeko tresna:
probetarako



BLOCKCHAIN

-UEU: Udako ikastaroa (2018)-
V. atala

Ethereum: DAPP baten garapena (Web3.js)

WEB3

- API bat Ethereumentzako

- JSON RPC protokoloa implementatzen du
- Lengoaia ezberdinetan dago eskuragarri

- Web3.js

- Javascripteko APIa
- <https://github.com/ethereum/web3.js/>



BLOCKCHAIN

-UEU: Udako ikastaroa (2018)-
Bonusa

Hyperledger Fabric