Anàlisi de la cripto-moneda Bitcoin

Isidro Pastor Jordà
Tutor: Jordi Herrera Joancomartí

Màster Interuniversitari de Seguretat de les Tecnologies de la Informació i de les comunicacions

Parlarem de ....

- Primera part - Anàlisi teòric
  - Què és bitcoin ?
  - Adreces i wallets
  - Les transaccions, els blocs i la cadena de blocs
  - Mineria i creació de blocs, com guanyar diners
  - Seguretat
- Segona part - Anàlisi de dades
  - L'script d'obtenció de dades
  - Dades analitzades
  - Comissions més comuns
  - Transaccions/blocks de un dia
  - Transaccions i comissions al temps

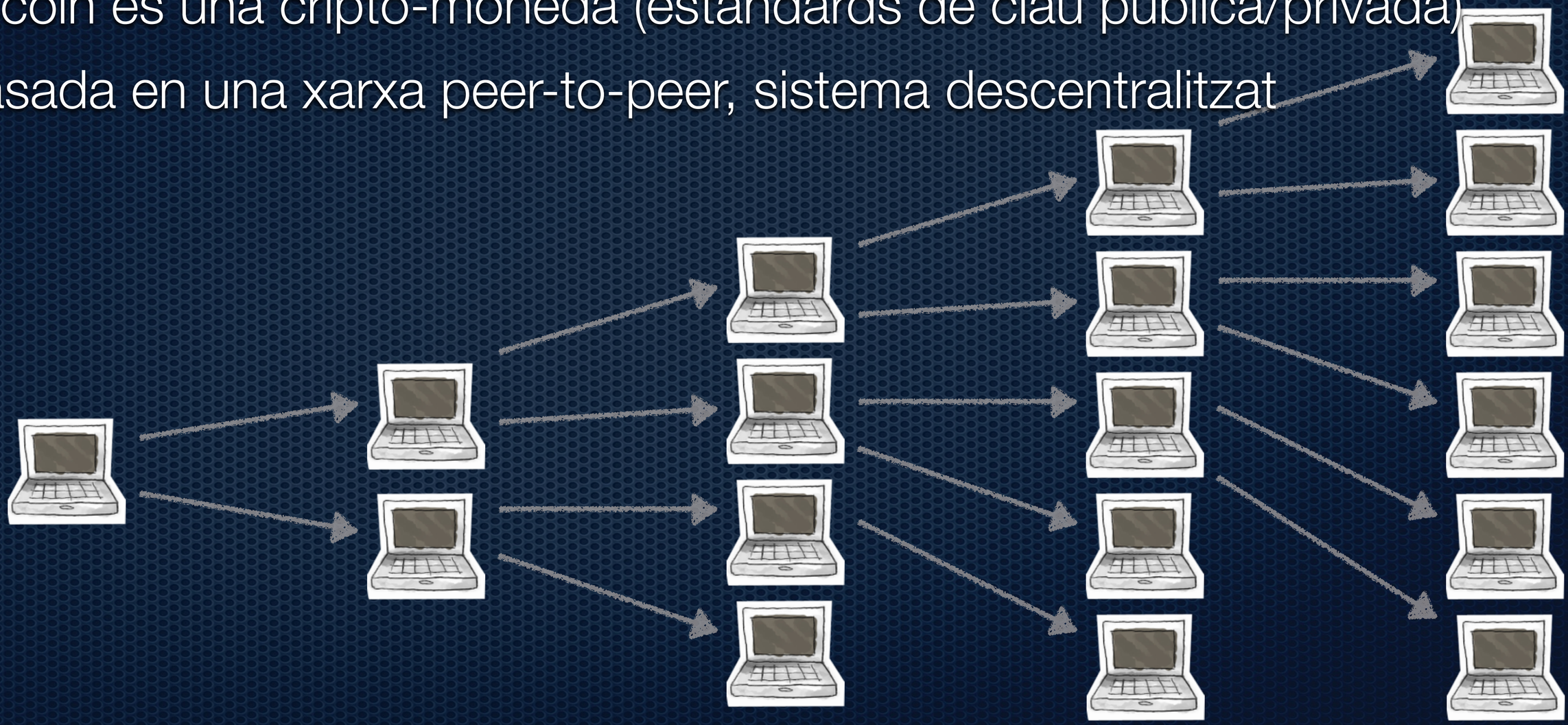
Tercera part - Conclusions i treball futur

Primera part

Anàlisi teòric

Què és bitcoin ?

- Bitcoin és una cripto-moneda (estàndards de clau pública/privada)
- Basada en una xarxa peer-to-peer, sistema descentralitzat



Què és bitcoin ?

- Bitcoin és una cripto-moneda (estàndards de clau pública/privada)
- Basada en una xarxa peer-to-peer, sistema descentralitzat
- Garanteix l'anonimat de les transaccions
- No hi ha cap regulador central

Adreces i wallets

- L'adreça bitcoin deriva de la clau pública del parell de claus pública/privada que podem generar
- Té la forma de nombres i lletres 14dQ1DZCYTpPZRxjMqjDySZHF1Fz8J8VnN
- Un wallet o cartera guarda les adreces de bitcoin i els seus parells de claus
- Si perdem les claus d'una adreça perdrem també els diners que hi teníem en aquesta adreça

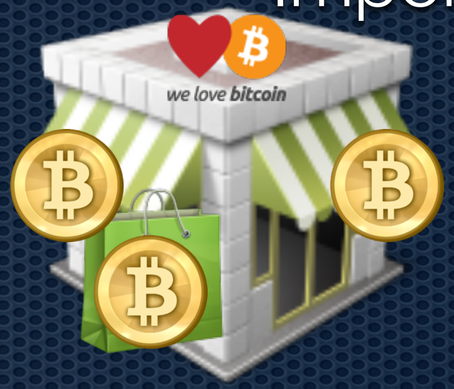
Les transaccions

inputs

Canvi

Comissió

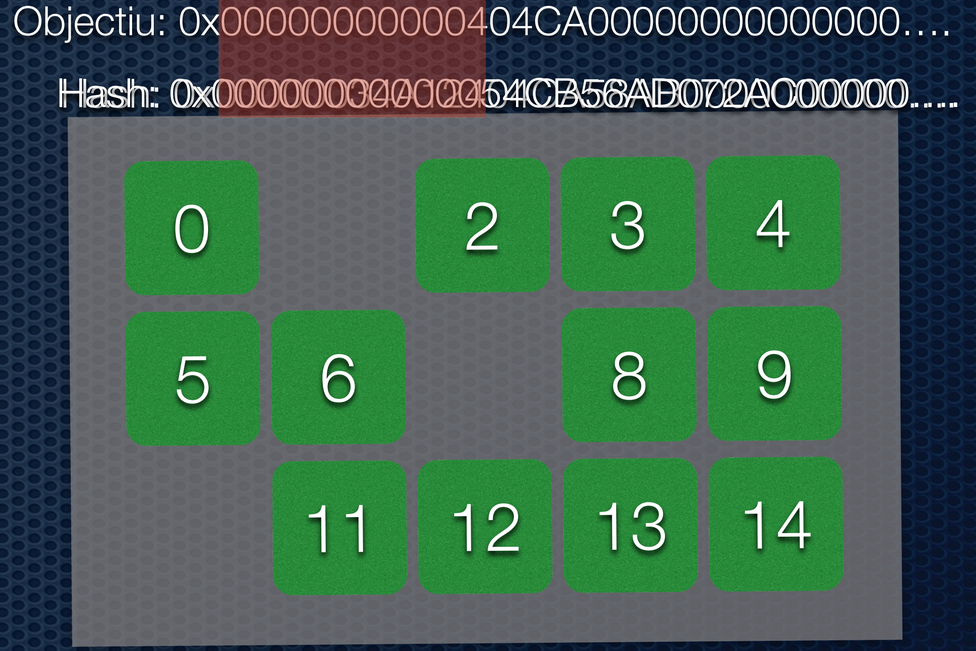
Import de la compra



- Les transaccions estan compostes per inputs i outputs
- Els inputs són referències a transaccions anteriors que han ingressat diners a la nostra adreça.
- Els outputs són els diners que es queda qui rep la transacció, el canvi i la comissió.

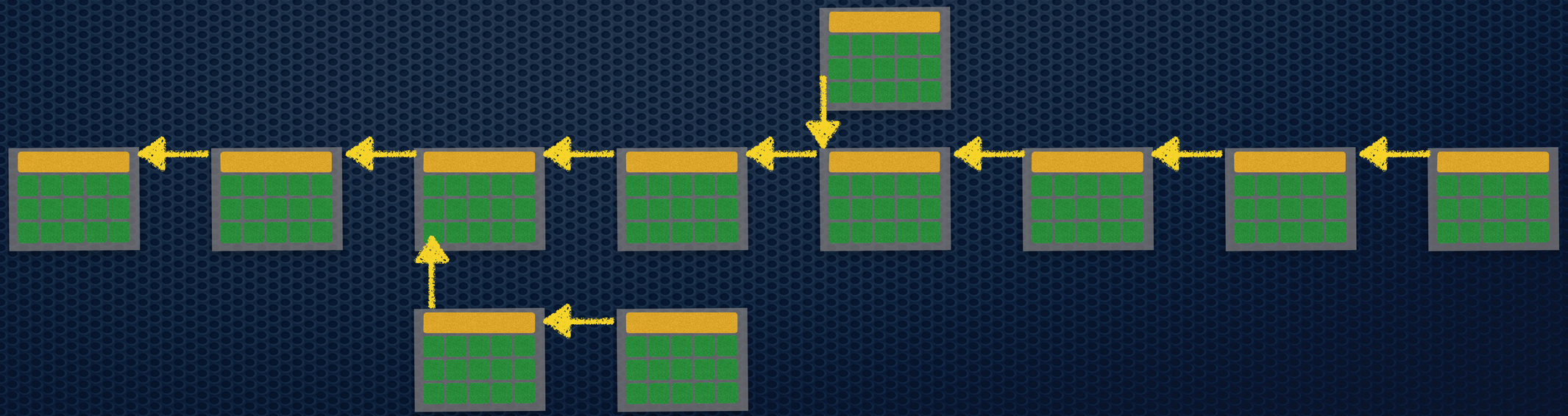
Blocks

- Un block conté un grup de transaccions
- A la capçalera del block hi ha un hash de les transaccions
- Es fa un segon hash de la capçalera que ha de complir un objectiu de dificultat
- Canviant la posició de les transaccions dins el block canviem el hash de les tx i per tant el hash de la capçalera per complir l'objectiu



Cadena de Blocks

- Els blocks s'agrupen formant una cadena o blockchain
- Aquesta cadena es forma afegint a la capçalera de cada block el hash del block anterior de la cadena
- Només la cadena més llarga és vàlida



Cadena de Blocks

- Els blocks s'agrupen formant una cadena o blockchain
- Aquesta cadena es forma afegint a la capçalera de cada block el hash del block anterior de la cadena
- Només la cadena més llarga és vàlida
- L'existència d'aquest mecanisme de cadena evita el problema de la doble despesa
- Doble despesa: Gastar dues voltes el mateixos diners

Mineria i creació de blocks

- Ens referim com a mineria a la creació de nous diners
- Quant s'accepta un block a la xarxa qui l'ha generat guanya 25 bitcoins (transacció de generació)
- Els miners es poden agrupar formant pools i repartir el treball de generació del block i els diners que genera
- Qui crea un block també rep les comissions de les transaccions
- Les comissions són un incentiu per incloure aquestes transaccions abans als blocks

Seguretat

- L'ús de criptografia permet ajustar la longitud de les claus
- La recompensa per generar un block no es pot gastar fins a 17 hores després de generar-se per si és descartat
- Manipular el timestamp als blocks està limitat en un marge de 140 minuts (màxima variació de temps entre nodes)
- Fer còpies de seguretat dels wallets és molt important. No és recomanable l'ús de wallets al núvol (cas MtGox.com)

Seguretat

- Per continuar la descentralització del sistema s'ha de mantenir que cap miner tingui més del 50% del poder de generació de blocks
- El 13 de Juny de 2014 GHash ha superat el 50% de la capacitat de computació de la xarxa bitcoin

Hacking, Distributed

It's Time For a Hard Bitcoin Fork

Ittay Eyal, and Emin Gün Sirer — Friday June 13, 2014 at 02:05 PM

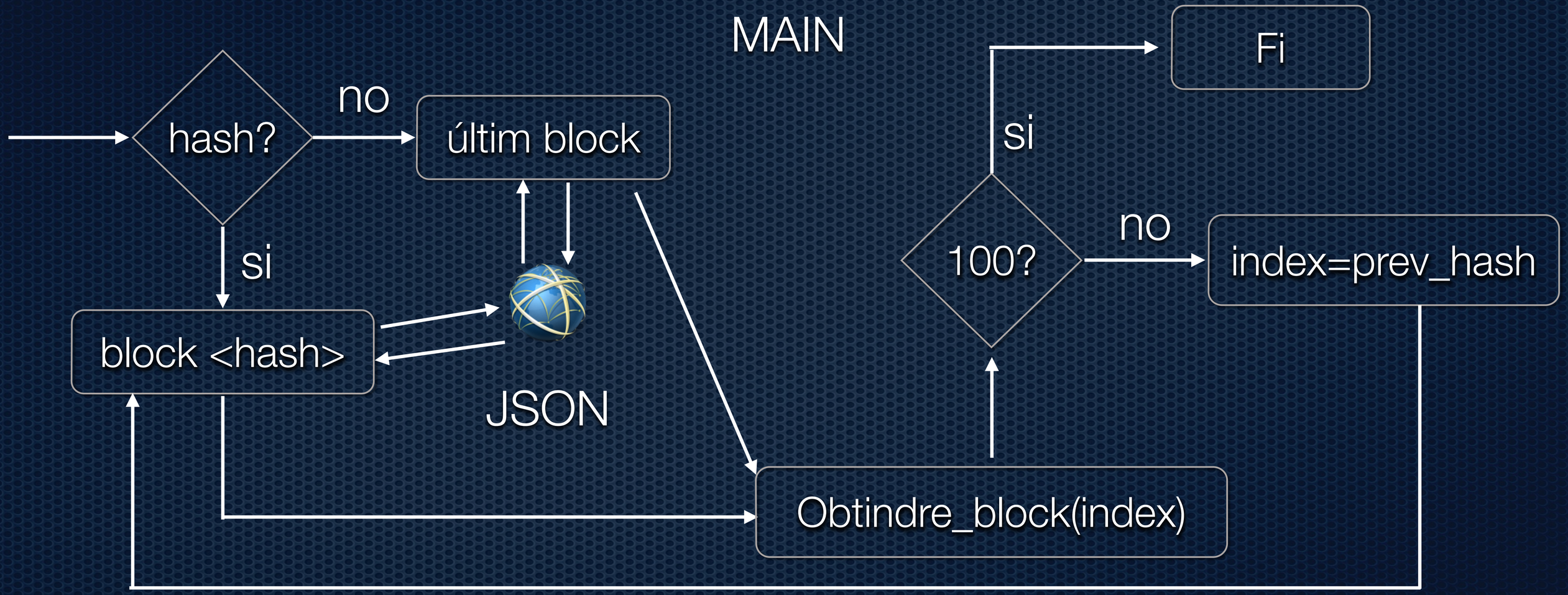
A Bitcoin mining pool, called GHash and operated by an anonymous entity called CEX.io, just reached 51% of total network mining power today. Bitcoin is no longer decentralized. GHash can control Bitcoin transactions.

http://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/

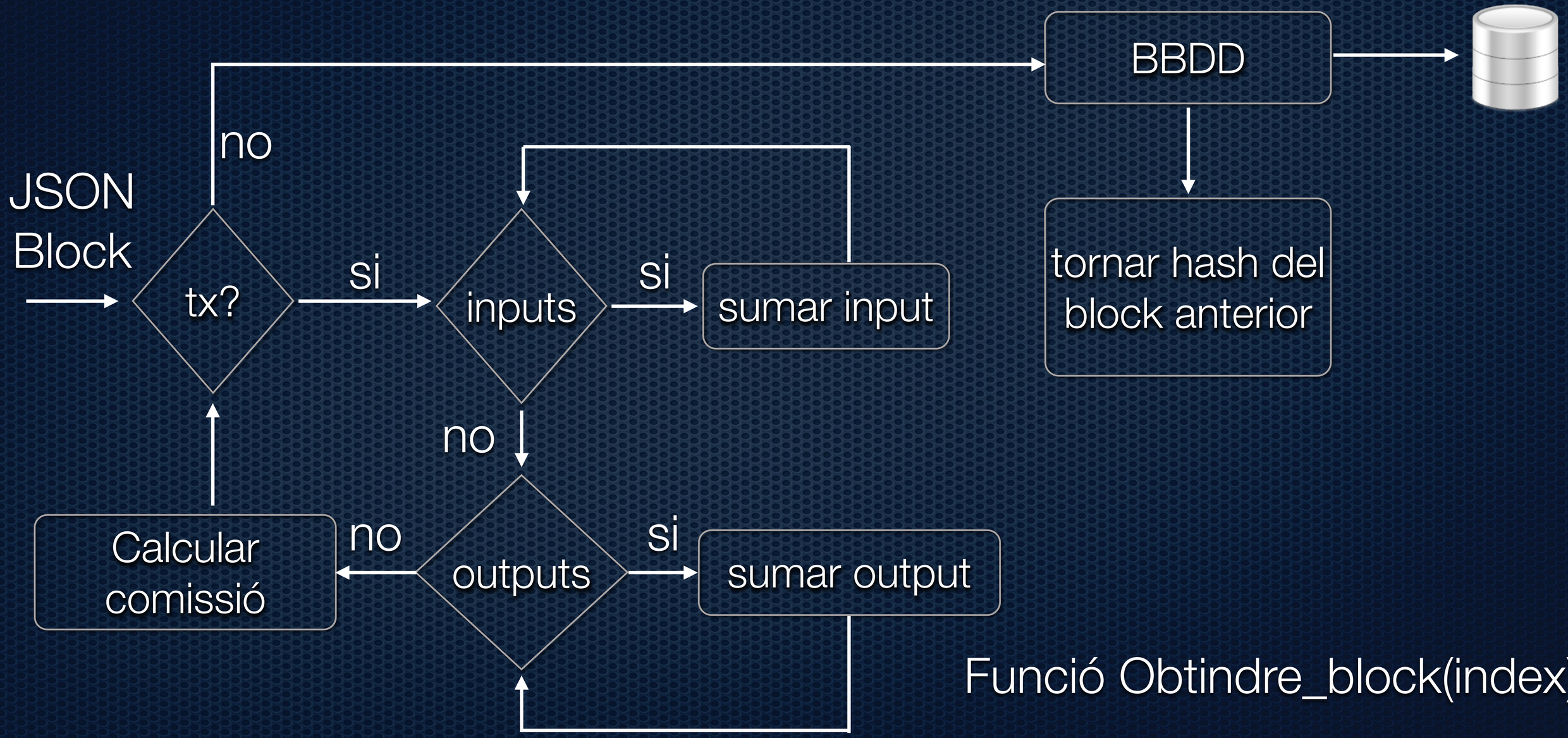
Segona Part

Anàlisi de dades

Script d'obtenció de dades



Script d'obtenció de dades



Funció Obtindre_block(index)

Dades analitzades

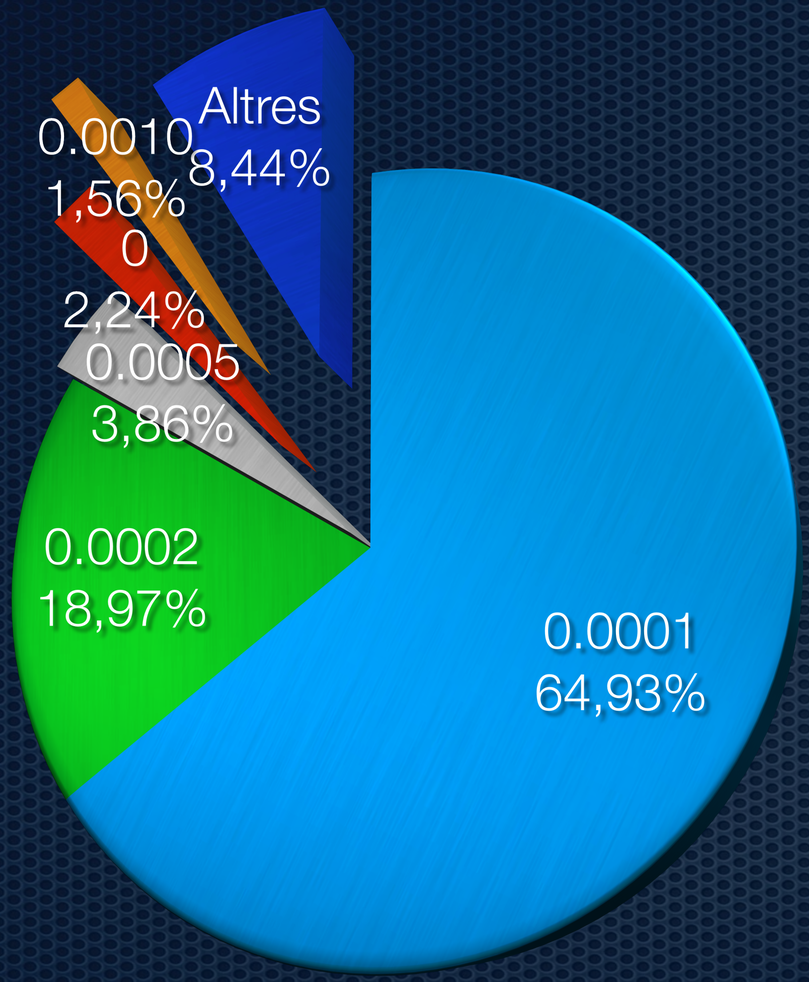
- Llenguatge d'script Python
- Base de dades MySQL

Taula	Nº de Entrades	Espai usat a la BD
transaccions	1415233	398,1MB
blocks	3669	1,5MB

- Splunk 6.1

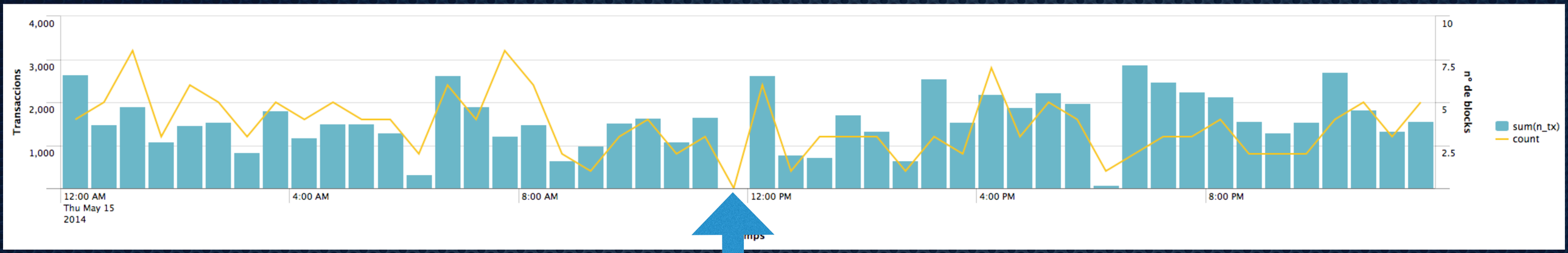
Font de dades	Transaccions/ blocks
transaccions_ip	971574 transaccions
blocks	3669 blocks

Comissions més comuns



Comissió BTC	Transaccions	Percentatge
0.0001	630921	64.93%
0.0002	184385	18.97%
0.0005	37540	3.86%
0	21842	2.24%
0.0010	15161	1.56%
0.0004	13724	1.41%

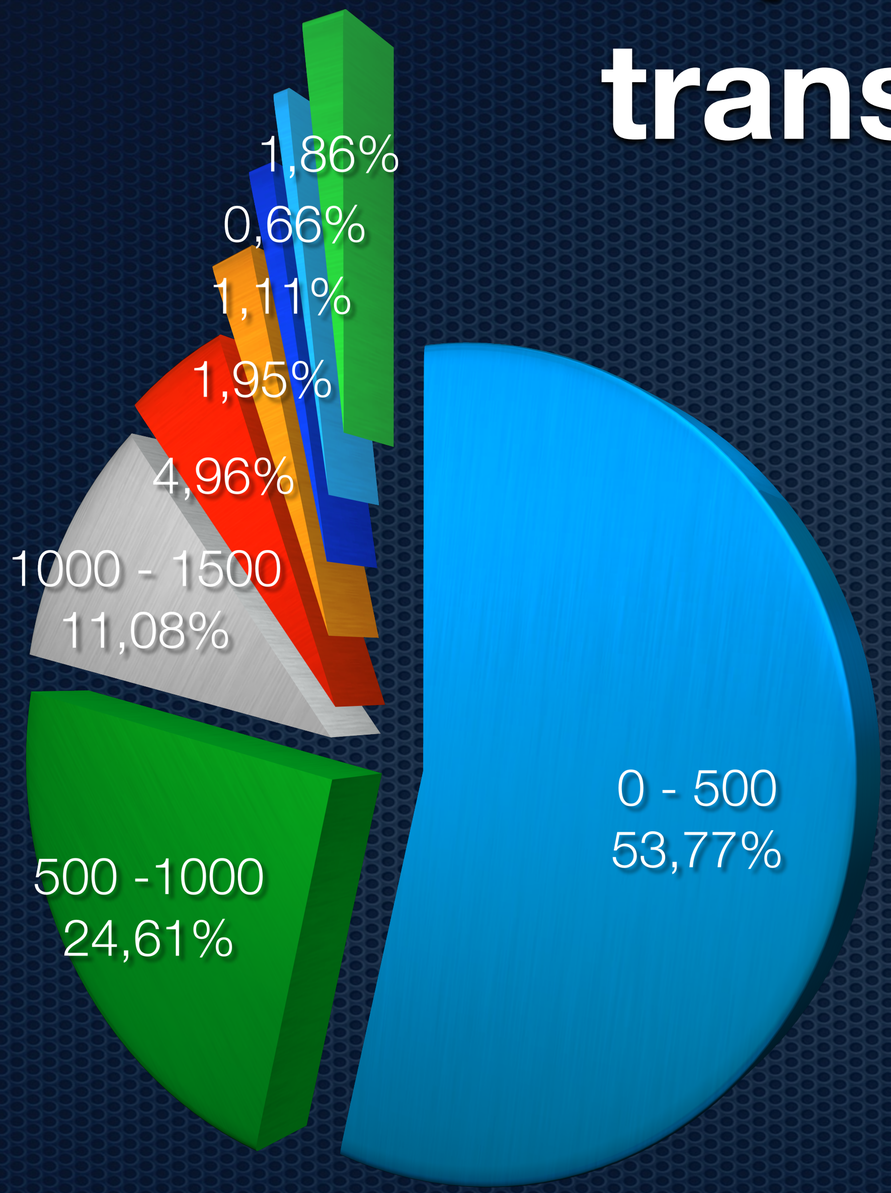
Transaccions/blocks de un dia



Període de mitja hora sense blocks

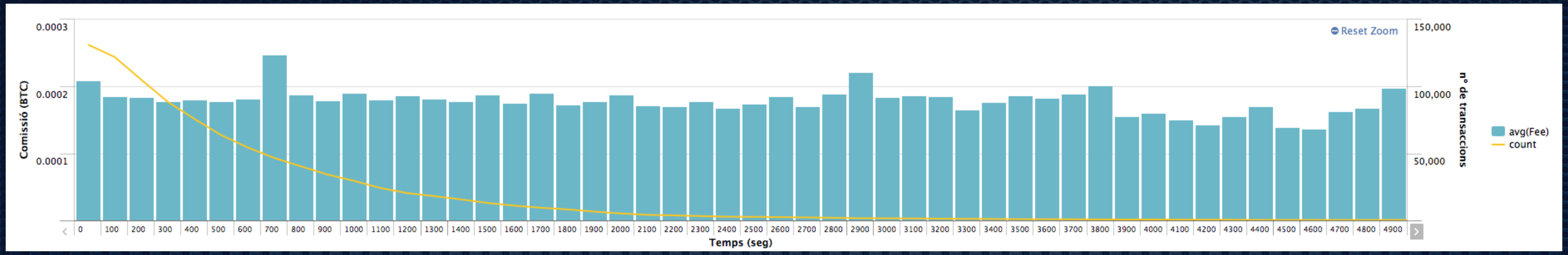
La generació de blocks és irregular
Normalment esperaríem un block cada 10 minuts
Aquestes desviacions sobre l'estimació faran que la dificultat del hash objectiu s'ajusti en un futur

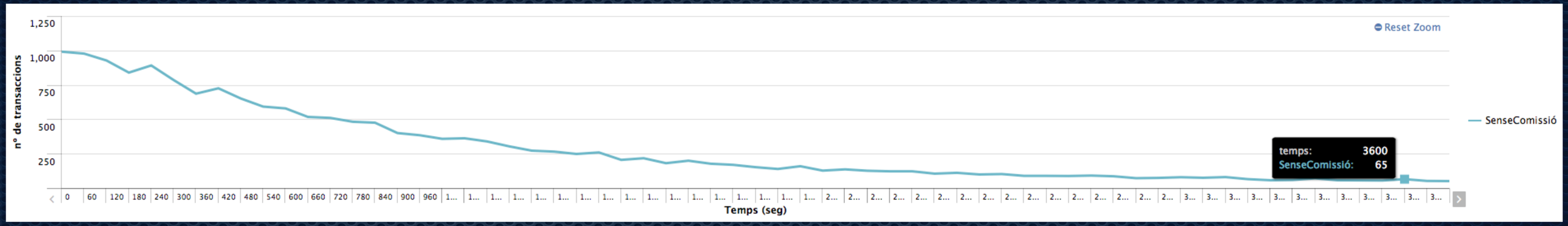
Temps en incloure una transacció al block

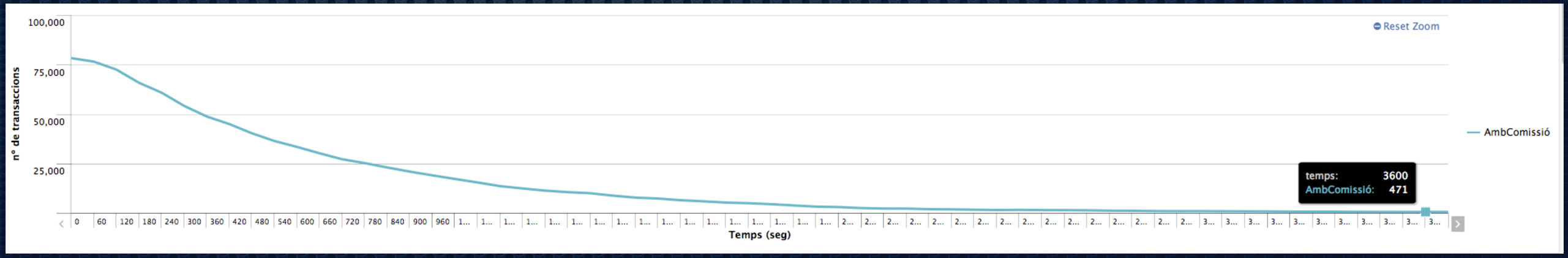


Temps	Transaccions	Percentatge
0	522418	53,77%
500	239123	24,61%
1000	107621	11,08%
1500	48198	4,96%
2000	18984	1,95%
2500	10800	1,11%
3000	6463	0,66%

Transaccions i comissions al temps







Tercera part

Conclusions i treball futur

Conclusions

- Bitcoin te ja 6 anys de vida
- El protocol s'autoajusta amb els mecanismes de dificultat dels blocks
- L'anonimat està bé però potser afavoreix intercanvis fora de llei (diners negres)
- El seu valor és molt volàtil i fluctuant, el que dificulta el comerç
- Bitcoin està limitat a generar com a màxim 21 milions de BTC, les comissions de generació s'acabaran i el sistema haurà de mantenir-se només amb les comissions per transacció.

Conclusions

- L'anàlisi de dades reflecteix la teoria dels bitcoins
- No pareix haver una relació directa entre les comissions pagades i el temps que triga una transacció en incloure's a un block
- Tampoc pareix que les transaccions sense comissió triguen més en incloure's als blocs
- Els pools de miners donen prioritat a les transaccions que ells originen

Treball futur

- Estudiar quina quantitat de bitcoins s'han perdut (pèrdues de wallets)
- Quin es l'efecte de que un pool tingui el 51% del poder total de computació de la xarxa (GHash)

Gràcies

Isidro Pastor Jordà

València, 16 Juny de 2014