

III Congrés de Sobirania Tecnològica

Blockchain:

Un univers contradictori

Abel - vdo@greyfaze.net PGP:0x4EE1184B

Pau - p4u@dabax.net PGP:0x5CF989CD

Index

1. Rerefons històric
2. Blockchain
3. Desmitificant Bitcoin i Blockchain
4. Reflexió i debat

1. Rerefons històric

Història (1)

- **Cypherpunk** (finals dels 80)

“ ... We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

”

Eric Hughes - Cypherpunk manifesto, 1993

Història (2)

- Criptografia **asimétrica**
(Phil Zimmermann, PGP, 1991)
- **Proof of Work** d'Adam Back (e-mail)
- Xarxes **p2p**
 - Napster 1999
 - e-Donkey, Torrent, etc...
- Nick Szabo, Hal Finney, Dai Wei, etc...

Història (3)

- Satoshi Nakamoto (**Blockchain**)

The Times 03/Jan/2009

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets". *The Times* has learnt.

The Bank of England revealed yester-

day that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus

on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels

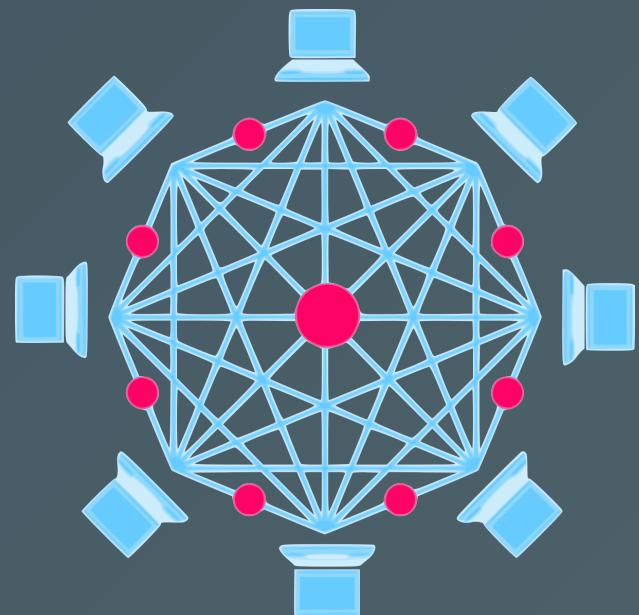
Business, page 47



2. Blockchain

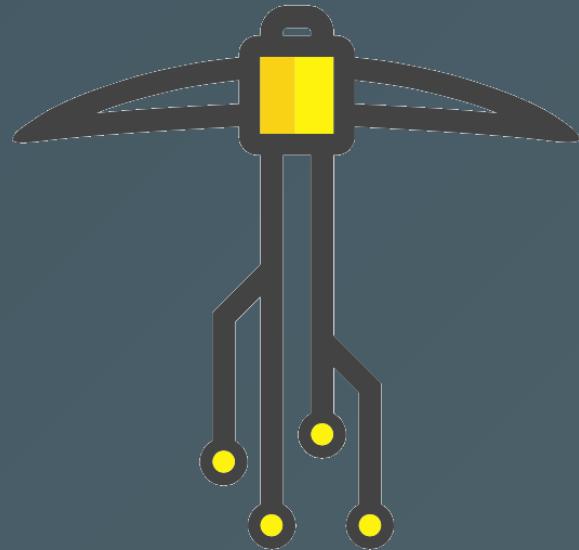
Blockchain [definició]

- Base de dades distribuïda
- Ordenada i inmutable (hashing)
- Verificada mitjançant criptografia
- Velocitat de creixement control·lada i estipulada



Blockchain [blocs i miners]

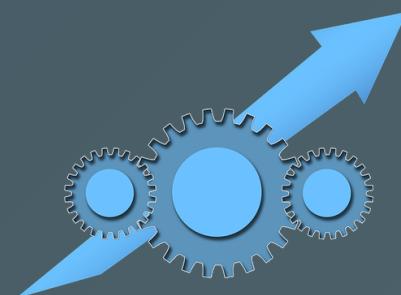
- Informació classificada en *blocs*
- Només els *miners* poden crear blocs
- Bitcoin: 1 bloc = 1 MByte (max)



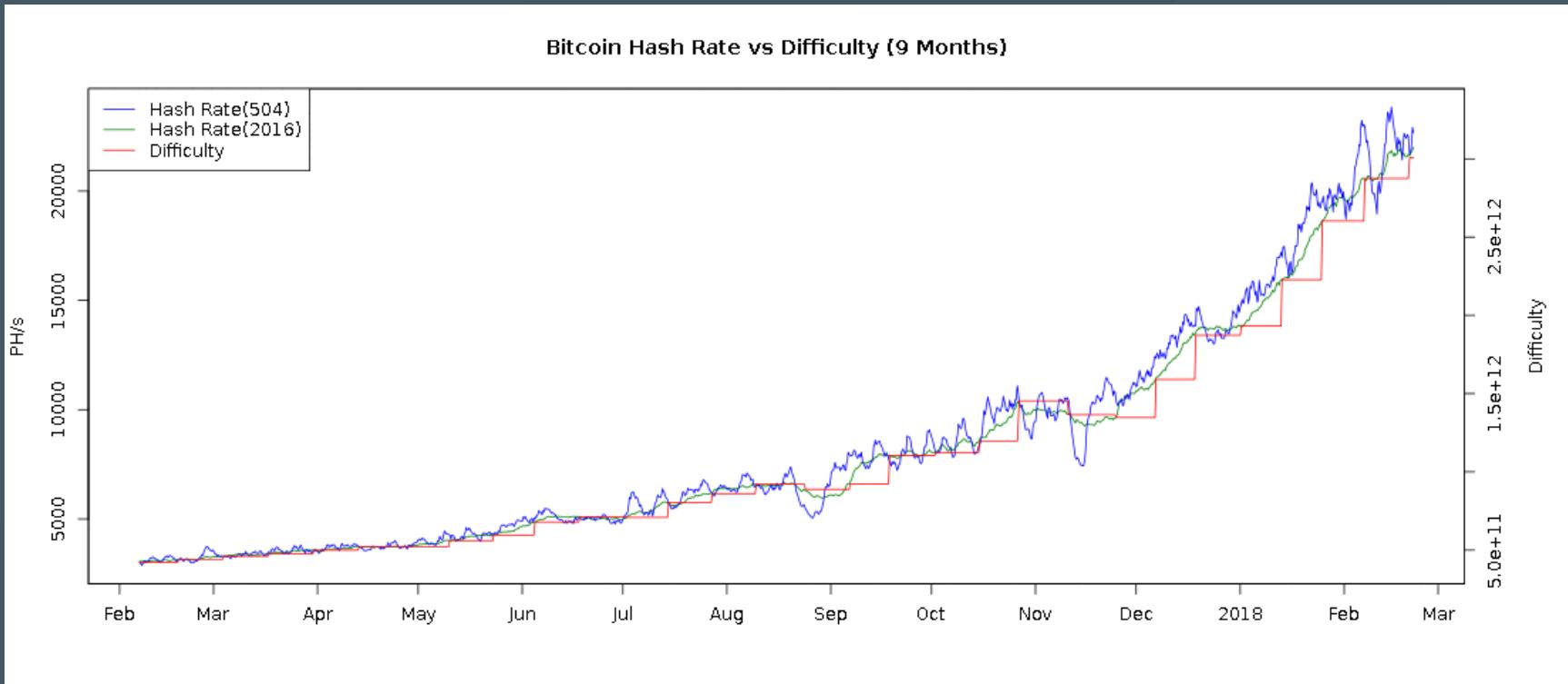
Blockchain [creixement (PoW)]

- Creixement control·lat amb problema matemàtic.
- Dificultat proporcional al poder de càlcul global.
- Cada N blocs es recalcula la dificultat.
- Bitcoin:

1 bloc cada 10 Minuts
reajust cada 2048 blocs (~14 dies)



Dificultat i hashrate: últims 12 mesos

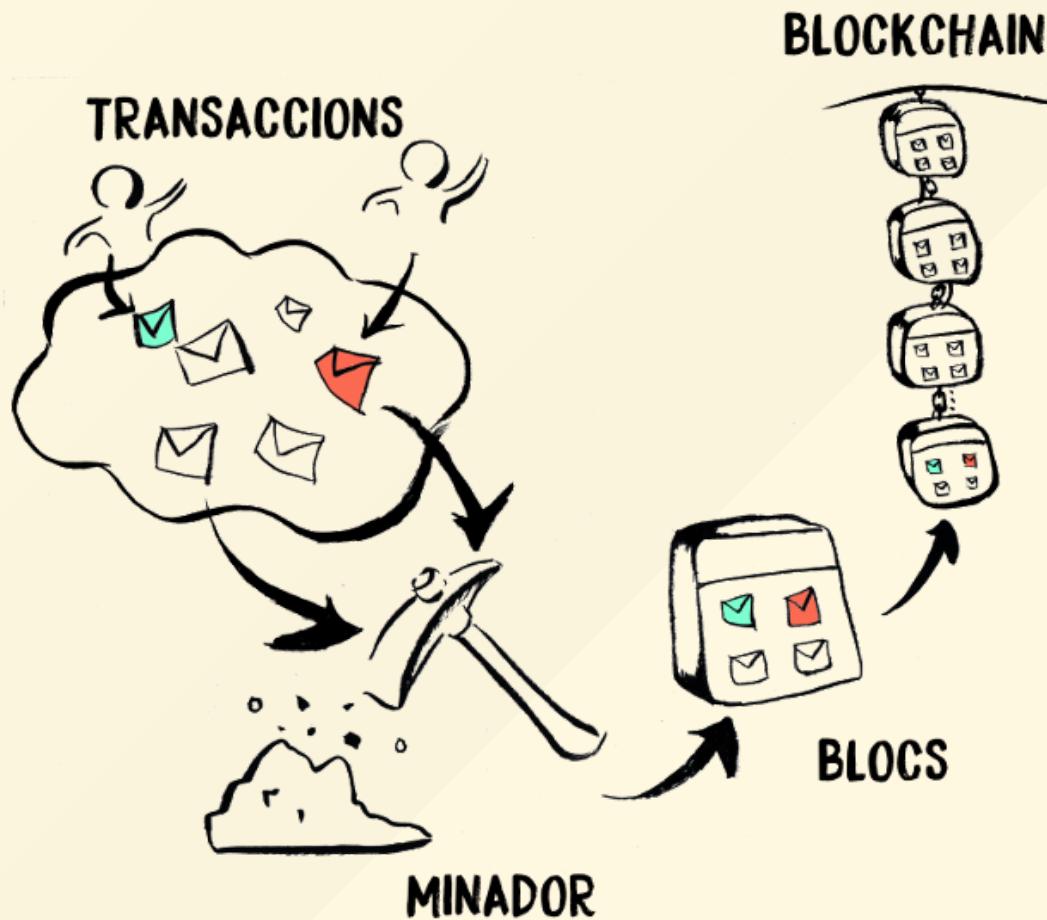


Blockchain [recompensa]

- Per incentivar la mineria hi ha una **recompensa**
- En Bitcoin inicialment 50 BTC. Actualment 12.5
- Cada 4 anys (210k blocs) es redueix a la meitat.



Blockchain [diagrama]



Blockchain [sobirania]

- **Base de dades disitribuïda** on els actors no necessiten ser de confiança.
- **Registre inmutable** i ordenat de dades amb marca de temps (timestamp).
- Dissenyada per a evitar centralització i/o censura.

Ens allibera de la necessitat de dependència cap a tercers *intermediaris*

Exemples: Sistema monetari, notaria, vot electrònic, Crowdfundings, identitat digital, etc...

3. Desmitificant Bitcoin

Bitcoin i Capitalisme

- El sistema es basa en un creixement infinit.

Satoshi és respalda amb la llei de Moore per justificar la seva escalabilitat.

- Fomenta la competència i economies d'escala.

Els miners han de competir entre ells per generar nous blocs d'informació. Qui més recursos té, més en guanya.

- Fomenta les "grans empreses" de miners per reduïr la variança i assegurar la recompensa

Ús i abús de la blockchain

- Nova 'criptoeconomia' no regulada i volàtil.
- Manipulació de mercats constant (JP Morgan, etc.)
- Especulació i (re)valorització independent de la seva utilitat real.
- Hiper-tokenització.
- Nous incentius per a infectar màquines i aprofitar-ne els recursos per a minar.
- Spam i Phishing més avançat i rentable.

L'estafa dels darrers anys (1)

Scam Coins (2013): *monedes 'brossa'*

Crear noves criptomonedes (normalment copiant altres), fer que entrin en algun mercat (normalment partíceps) i esperar el *pump&sell*

“ DogeCoin, PotCoin, TrumpCoin, SexCoin, etc. ”



L'estafa dels darrers anys (2)

ICO (2016): *initial coin offering*

- Crowdfundings amb recompensa ¿Model startup?
- Normalment la ICO reparteix un token o moneda entre els seus inversors.
- Casos on l'inversió és multiplica per x1000.
- Un cop tancada la ICO no hi ha control sobre el projecte per part dels inversors.

Arribat un punt dóna igual l'objectiu del projecte a finançar, només si en algun moment es revaloritzarà.

L'estafa dels darrers anys (3)

Hard Forks (2017)

- Divisions de la cadena en un punt que generen una nova cadena i per tant una nova moneda.
- A tothom se li dupliquen les unitats de moneda.
Generem valor sense fonament!



L'estafa dels darrers anys (4)



Hiper-tokenització

- El "hype" del terme Blockchain atreu a inversors i especuladors. Qualsevol idea, per absurda que sigui, pot aconseguir fons monetaris a cost zero.
- Venezuela (Petro), Iran, Canon, Nostrum, Facebook, Telegram...

Empresa

Una compañía de té helado triplica su valor en bolsa tras añadir blockchain a su nombre

21 diciembre, 2017 • 0 Comentarios

Privacitat

- Bitcoin i la majoria de blockchains no són anònimes, mes aviat totalment *transparents*.
- Permeten l'anàlisi i traçabilitat per part d'Estats, empreses privades, agéncies com l'FBI, etc.



Eina d'anàlisi de Blockchain

BLOCKSEER Search for a bitcoin address, block, or transaction Bitcoin Ethereum (Beta) Sign Out

Cluster Addresses Public Labels Identifier Overlay
OFF ON OFF ON OFF ON

?

FROM WANNACRY 1219YDPg...
First Tx Time: 08/03/2017 04:41
Last Tx Time: 08/03/2017 15:56

2022df650...
35ed59e8...
1HG7gdBAY...
1P2SbNvSz...
557b6869b...
95d36a6926639ba...
SHAPESHIFT...
SHAPESHIFT...
SHAPESHIFT...
SHAPESHIFT...
SHAPESHIFT...
1K9yMfU17...
14MuJkmk6...
1J7qjSnNQ...
1F7Z2W82h...
36e488e5...
24a8528e5...
SHAPESHIFT...
POLONIEX 1BvTQTPSP...
HITBTC.COM 1ETWkyQUY...
1AvG3JwEb...

Transaction

Tx Hash	95d36a6926639ba...
Block Height	478837
Total Value	9.02424717 BTC
Fee	0.00021107 BTC
Balance	BTC
Time	08/03/2017 09:37

Descriptions

Wanna Cry exchange of BTC -> XMR

Shapeshift.io

Add Transaction Description

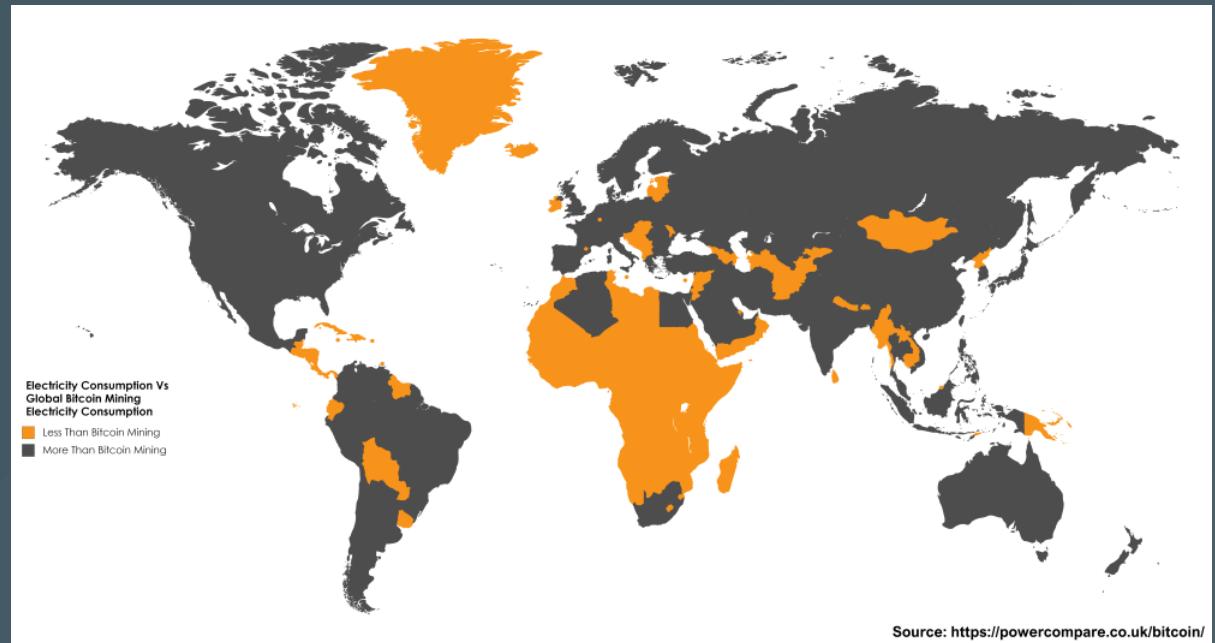
Description of Transaction

Save Description

```
graph TD; A[WANNACRY] -- 9.04 --> B[35ed59e8...]; B -- 9.03 --> C["FROM WANNACRY 1219YDPg..."]; C -- 9.03 --> D[2022df650...]; D -- 0.00329 --> E[1HG7gdBAY...]; D -- 9.02 --> F[1P2SbNvSz...]; E -- 9.02 --> G[95d36a6926639ba...]; F -- 7.22 --> G; G -- 1.8 --> H[SHAPESHIFT...]; G -- 7.22 --> I[SHAPESHIFT...]; G -- 5.19 --> J[SHAPESHIFT...]; H -- 5.06 --> K[SHAPESHIFT...]; H -- 9.42 --> L[SHAPESHIFT...]; H -- 1.8 --> M[36e488e5...]; I -- 0.729 --> N[SHAPESHIFT...]; I -- 0.00233 --> O[SHAPESHIFT...]; I -- 10 --> P[24a8528e5...]; J -- 8.38 --> P; J -- 3 --> Q[SHAPESHIFT...]; J -- 2.23 --> R[SHAPESHIFT...]; M -- 0.0112 --> S[SHAPESHIFT...]; M -- 17 --> T[POLONIEX 1BvTQTPSP...]; N -- 0.0109 --> U[1AvG3JwEb...]; P -- 7.14 --> U; P -- 30.7 --> V[HITBTC.COM 1ETWkyQUY...]
```

Consum d'energia (2017)

- 18.4 TWh / any. (aprox)
- Consum anual comparable a Islàndia.



Alternatives al consum d'energia?

- Proof-of-Stake
 - Seguretat no probada.
 - Incentiva l'acumulació de capital en els validadors.
- Proof of Authority i Proof of Cooperation
 - Recentralitzen la descentralització.
 - Requereixen confiança.

No hi ha una sol.lució segura, probada i energèticament sostenible a hores d'ara.

4. Reflexió

- Blockchain és una tecnologia que permet l'autogestió i soberania de les dades digitals.
- Avui dia està sobre explotada i en la majoria dels casos només hi ha un interès econòmic darrera.
- Els objectius de privacitat i anonimat s'estan difuminant, cal que siguin pilars centrals.
- La seguretat i resiliència de la tecnologia ve donada per la decentralització, però la tendència es centralitzadora.
- Cal fer recerca per trobar sol·lucions sostenibles energèticament.

Satoshi

“ Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.

”

“ Yes, we will not find a solution to political problems in cryptography, but we can win a major battle in the arms race and gain a new territory of freedom for several years.

”

Debat

El potencial ambivalent d'una tecnologia disruptiva:

- Autogestió econòmica VS Increment de desigualtats
- Intel.ligència artificial, Big data...: Al.liat o defensa?
- Privacitat VS transparència

Preguntes i debat