Sh#Bit coin

matefest @ 2018

$> David Martínez

$> Enric Florit

$> Taras Yarema

?> Què és Bitcoin

$> El bitcoin (BTC) és una criptomoneda descentralitzada proposada inicialment per Satoshi Nakamoto. És la criptomoneda més utilitzada actualment amb un mercat total actual de més de 110B d'euros.

01110011011010000110100101110100011000110110111101100100101101110

$> El primer cop en que es parla de Bitcoin és en un paper anomenat "Bitcoin: A Peer-to-Peer Electronic Cash System" per Satoshi Nakamoto. És un document de 9 pàgines que explica detalladament com ha de ser la construcció de una moneda virtual anònima i decentralitzada.

fig[0] = Paper de Satoshi Nakamoto

?> Com funciona Bitcoin

>> Adreces

$> Tot participant de la xarxa Bitcoin té una cartera electrònica que conté un nombre arbitrari de claus criptogràfiques. La clau pública, o les adreces Bitcoin, funcionen com els punts remitent o receptor per a tots els pagaments. Les seves claus privades corresponents autoritzen el pagament només per a aquest cert usuari. Les adreces no tenen cap informació sobre el seu amo i són generalment anònimes.

01110011011010000110100101110100011000110110111101100100101101110

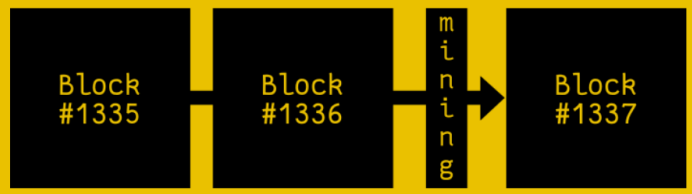
>> Transaccions

$> Els bitcoins contenen la direcció pública del seu amo actual. Quan un usuari **A** transfereix alguna cosa a un usuari **B**, **A** lliura la propietat agregant la clau pública de **B** i després signant amb la seva clau privada. **A** llavors inclou aquests bitcoins en una transacció, i la difón als nodes de la xarxa P2P als quals està connectat.

>> Aquests nodes validen les signatures criptogràfiques i el valor de la transacció abans d'acceptar-la retransmetre.

>> Blockchain

$> Tots els nodes que formen part de la xarxa Bitcoin mantenen una llista col·lectiva de totes les transaccions conegudes, la cadena de blocs. Els nodes generadors (miners) creen els nous blocs, així com les noves transaccions publicades a la xarxa.



fig[1] = Mining de un nou bloc

>> Quan un miner mina un nou bloc, ho transmet a la resta dels nodes als quals està connectat. En el cas que resulti un bloc vàlid, aquests nodes s'afegeixen a la cadena i el tornen a retransmetre. Aquest procés es repeteix indefinidament fins que el bloc ha assolit tots els nodes de la xarxa. Eventualment, la cadena de blocs conté l'historial de possessió de totes les monedes des de la direcció-creadora a la direcció de l'actual propietari. Per tant, si un usuari intenta reutilitzar monedes que ja va usar, la xarxa rebutjarà la transacció.

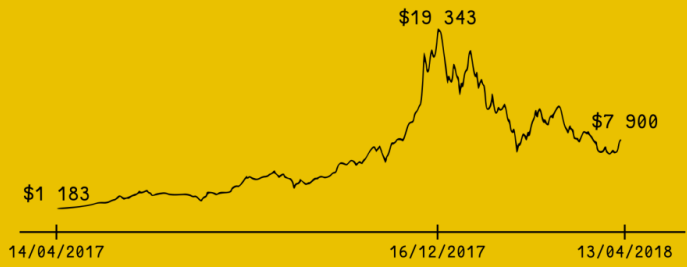
#> Privacitat

$> Les transaccions se signen digitalment (amb l'algoritme ECDSA) pel propietari de la direcció Bitcoin que conté originalment els fons. Aquest missatge signat es propaga per tota la xarxa i s'acaba emmagatzemant en la cadena de blocs. La xarxa no encripta cap tipus d'informació, totes les transaccions són públiques a internet.
>> Qualsevol persona pot analitzar el contingut, l'origen i la destinació de les transaccions. És a dir, expossar una adreça pública és expossar tot l'historial de transaccions d'aquesta.

01110011011010000110100101110100011000110110111101101001011011 10

€> Especulació

$> L'auge de BTC i la facilitat per comprar ha portat a un especulació massiva aquest darrer any. Portant a fluctuaccions de més de 1000% durant l'any 2017.



fig[2] = Preu BTC @ coindesk.com

HACKING LLIURE

fig[3] = hackinglliure.org