

UN ENCUENTRO MÁGICO

BITCOIN Y HASKELL



A black and white engraving of a man with dark, wavy hair, wearing a high-collared coat and a striped cravat. He is looking slightly to his left with a neutral expression.

**LAS
PERSPECTIVAS
FUTURAS NO SON
AGRADABLES NI
MORALES**

Thomas Larkin

HACIENDOSE MILLONARIO

- ▶ Vendiendo equipamiento
- ▶ Alojamiento
- ▶ Comida
- ▶ Transporte



TEMARIO

- ▶ Que es bitcoin?
- ▶ Sistemas monetarios: problemas y soluciones
- ▶ Blockchain
- ▶ Minado
- ▶ Código

QUE ES BITCOIN?

- ▶ Un protocolo
- ▶ Una red de pagos
- ▶ Una moneda
- ▶ Descentralizado
- ▶ Basado en Blockchain

BITCOIN 101

EVERYTHING YOU NEED TO KNOW ABOUT THE DIGITAL CURRENCY AND HOW IT WILL SHAPE THE FUTURE

WHAT IS BITCOIN?

The infographic is titled "WHAT IS BITCOIN?" and features four blue banners connected by a vertical yellow line. The top banner says "BITCOIN STREET". The second banner from the top says "1st DECENTRALIZED DIGITAL CURRENCY". The third banner from the top says "OPEN-SOURCE SOFTWARE WHICH USES CRYPTOGRAPHY". The bottom banner says "PEER-TO-PEER SYSTEM". To the right of the banners is a stylized illustration of a peer-to-peer network where blue nodes connected by yellow lines represent Bitcoin coins.

Bitcoin is invented by pseudonymous developer **Satoshi Nakamoto**. According to speculations, he is either:

- a Japanese mathematician
- a professor in George Washington University
- a group of Dublin-based cryptography graduate students

TRIVIA

中本哲史
SATOSHI WHO?

EL LIBRO DE CUENTAS

- ▶ Problemas
 - ▶ Falsificación de monedas
 - ▶ Falta de fondos
 - ▶ Devaluación
- ▶ Solución
 - ▶ El libro de cuentas
 - ▶ Libro actual de bitcoin: ~ 170 GB

CUANTA CANTIDAD DE MONEDA HAY?

- ▶ Fija
 - ▶ Quien tiene el dinero al principio?
 - ▶ Como entran nuevos participantes?
 - ▶ Inflación
- ▶ Semi Variable
 - ▶ Basada en un bien físico?
- ▶ Variable
 - ▶ Inflación/Deflación
 - ▶ Quien lo controla?

COMO PREVENIR LA FALSIFICACIÓN?

- ▶ Haciendo difícil acuñar moneda
- ▶ Usando papel/tinta especial
- ▶ Firmas electrónicas

TRANSACCIONES

- ▶ Origen
- ▶ Destino
- ▶ Cantidad

MODELO DESCENTRALIZADO

- ▶ Todo el mundo tiene una copia del libro de cuentas
- ▶ Cualquiera puede verificar las entradas
- ▶ Como prevenimos un DoS?

EL MINADO

- ▶ Generación de nuevos bloques
- ▶ Puzzle: Proof of work
- ▶ Garantes del sistema
- ▶ Pago por sus servicios
- ▶ Generación de nueva moneda
- ▶ Dificultad variable

DIFICULTAD Y TIEMPO ENTRE BLOQUES

► El puzzle

```
difficulty :: String -> Integer -> Integer
difficulty someString nonce =
    os2ip $ pack . hashlazy (someString ++ show(nonce))
```

- 160 bits (SHA1)
- Número decimal de ~ 50 cifras
- Valor completamente aleatorio
- Tiempo entre bloques constante (10 minutos aprox)
- Ajuste cada 2016 bloques

EJEMPLOS DE CODIGO

- ▶ Implementación básica sin minado
- ▶ Minado básico
- ▶ Minado completo

AGRADECIMIENTOS

MICHAEL BURGE

- ▶ Blog: <http://www.michaelburge.us/>
- ▶ Ejemplos:
- ▶ <http://www.michaelburge.us/2017/08/17/rolling-your-own-blockchain.html>
- ▶ <http://www.michaelburge.us/2017/08/31/roll-your-own-bitcoin-exchange.html>