DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

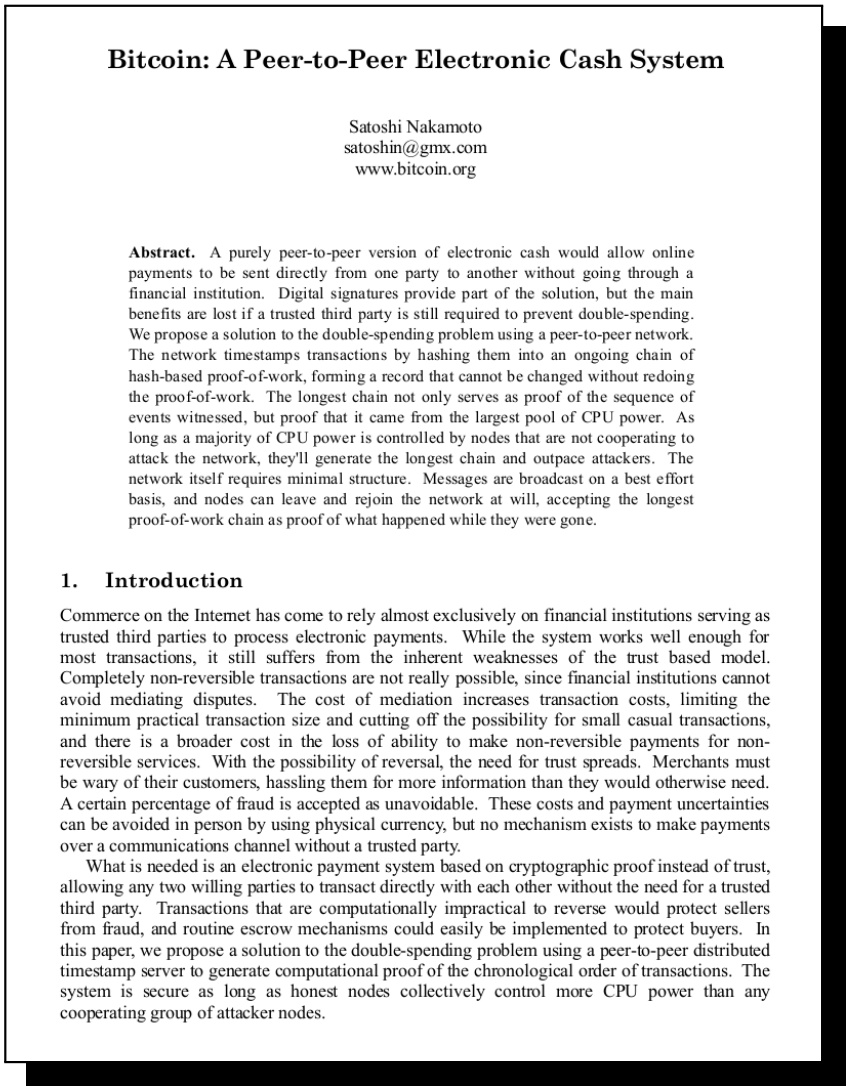
¿Puedo comprar un alfajor con Bitcoin?

David González Márquez

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

SdC 2017

¿Qué es un Bitcoin?, criptomonedas



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Satoshi Nakamoto - seudónimo

Creó y publicó en 2008 el protocolo Bitcoin

El primer Bitcoin se crea el 3 de enero de 2009, a las 18:15:05hs GMT

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

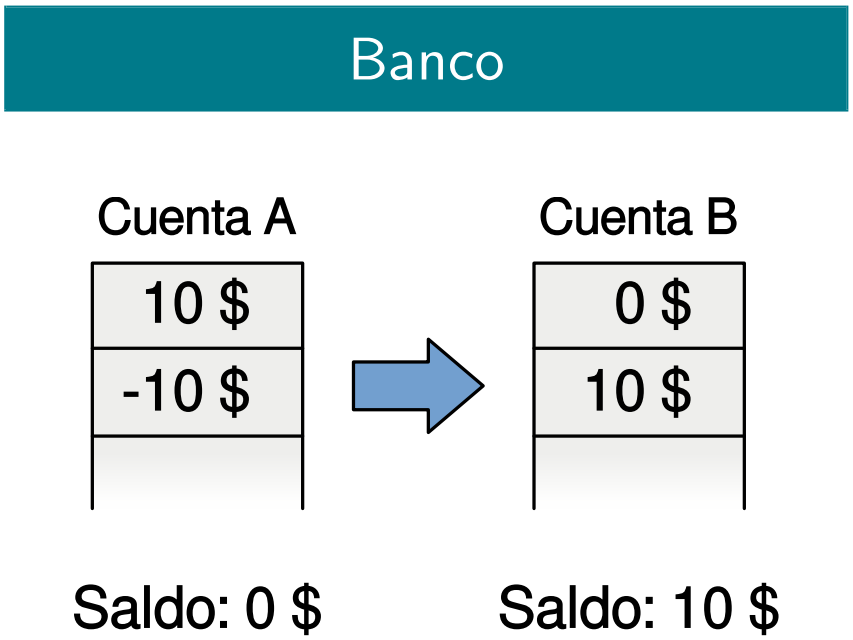
¿Qué es una transacción?

Trato por el que **dos** partes, llegan a un **acuerdo comercial**

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

¿Qué es una transacción?

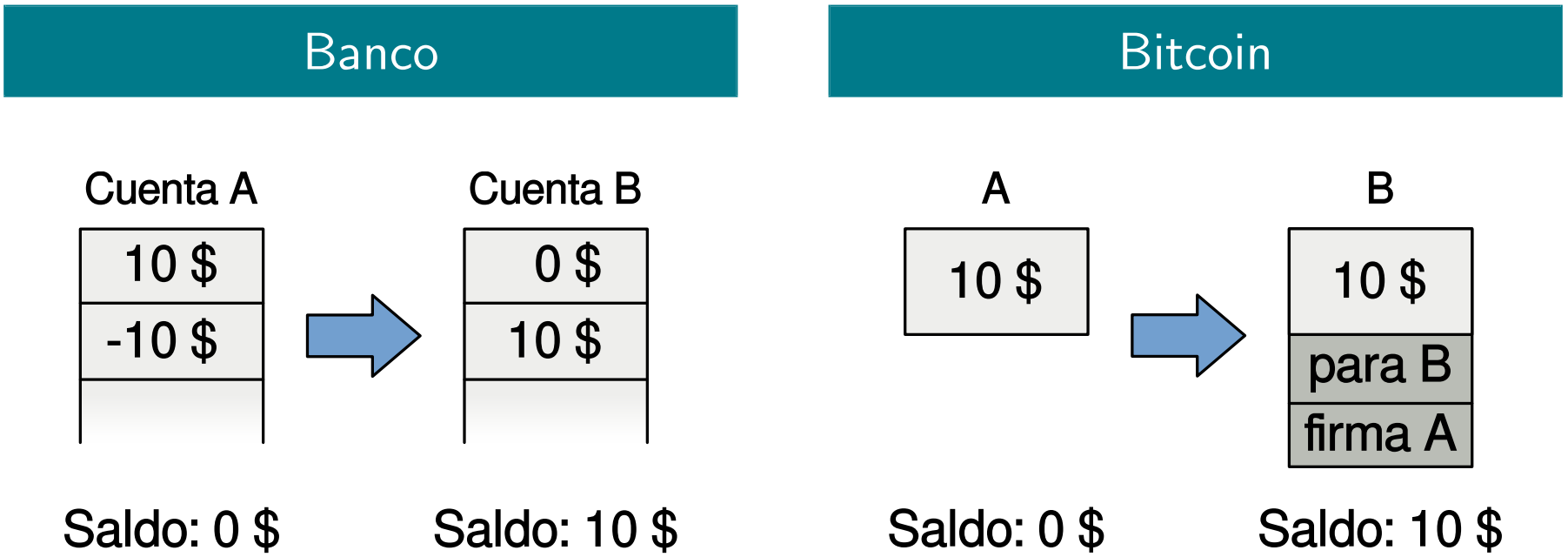
Trato por el que **dos** partes, llegan a un **acuerdo comercial**



DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

¿Qué es una transacción?

Trato por el que **dos** partes, llegan a un **acuerdo comercial**

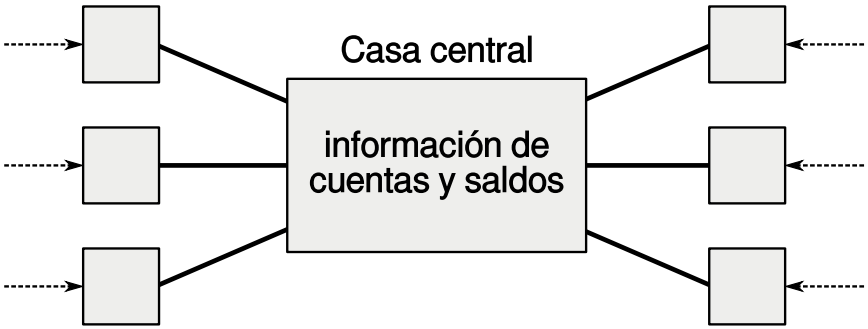


DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Red centralizada vs red descentralizada

Red centralizada vs red descentralizada

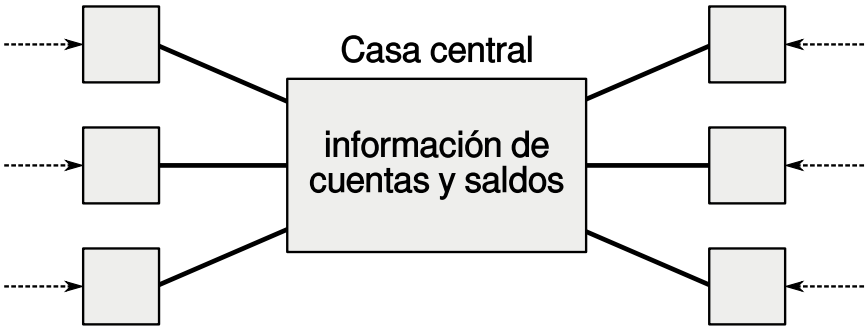
Banco



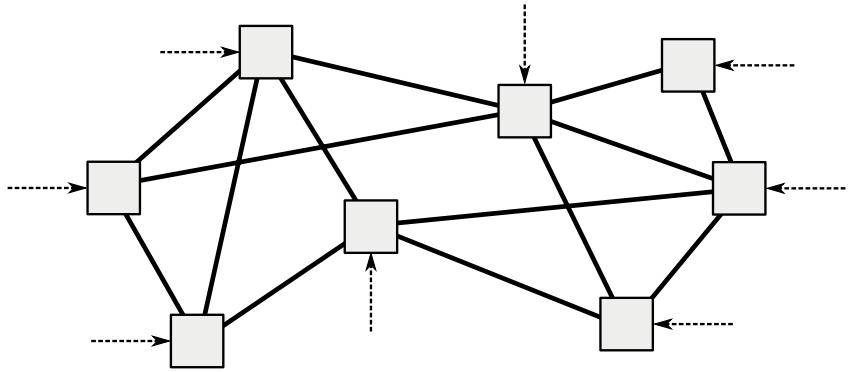
DEPARTAMENTO
DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Red centralizada vs red descentralizada

Banco



Bitcoin



En un banco la información esta **centralizada** en la casa central

En Bitcoin cada nodo de la red tiene **toda** la información sobre cuentas y saldos

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

¿Qué es una función de Hash?

Una función de HASH toma una secuencia de valores y genera un número de **tamaño fijo**.

Ejemplo:

HASH(0000 0000 0000 0000 0000 0000) → 2413

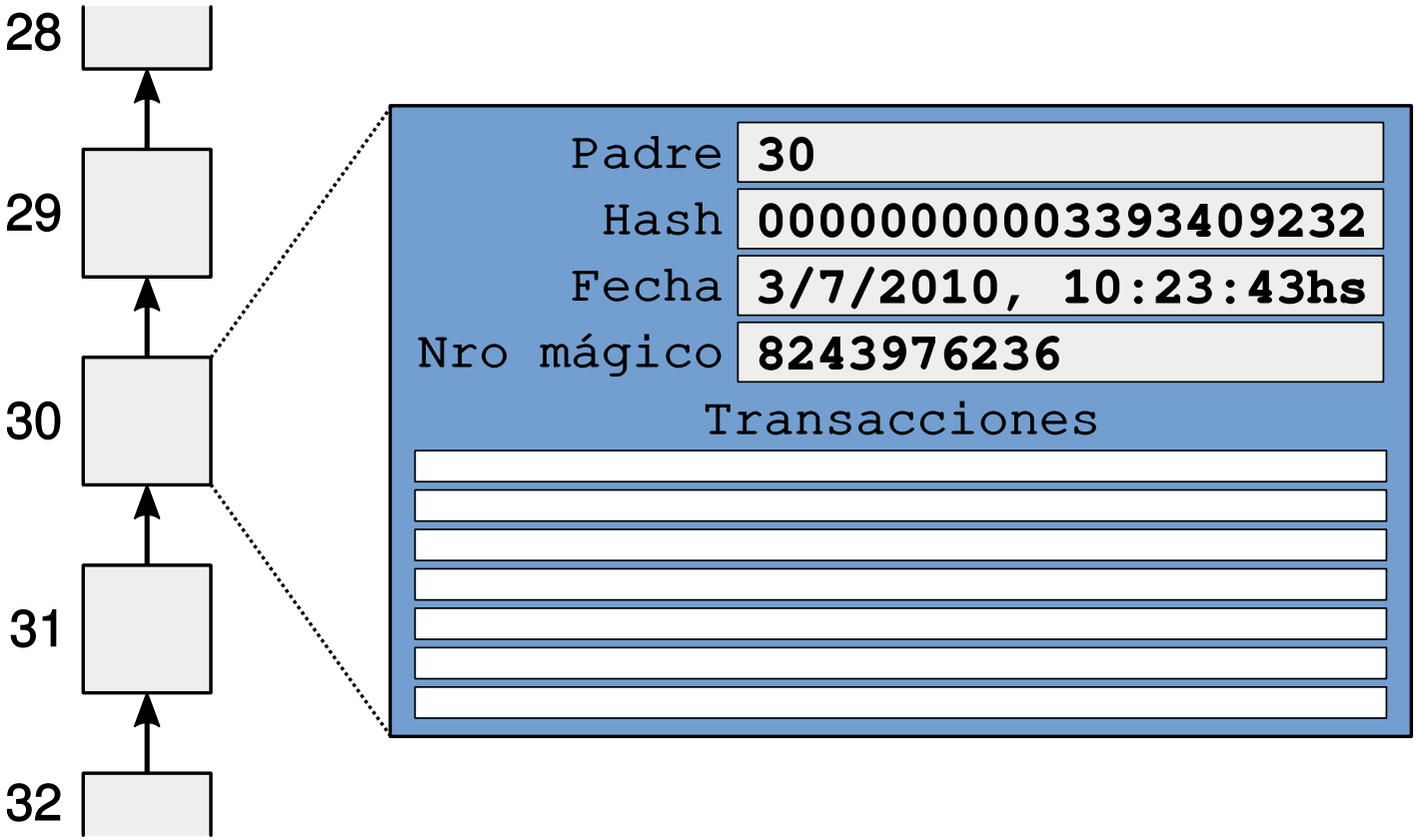
HASH(0000 0000 0000 0000 0000 0001) → 9402

HASH(0000 0000 0000 0000 0000 0002) → 1465

- Es **fácil** de calcular
- No se puede **predecir** el resultado

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

¿Dónde se guarda la información?, Blockchain

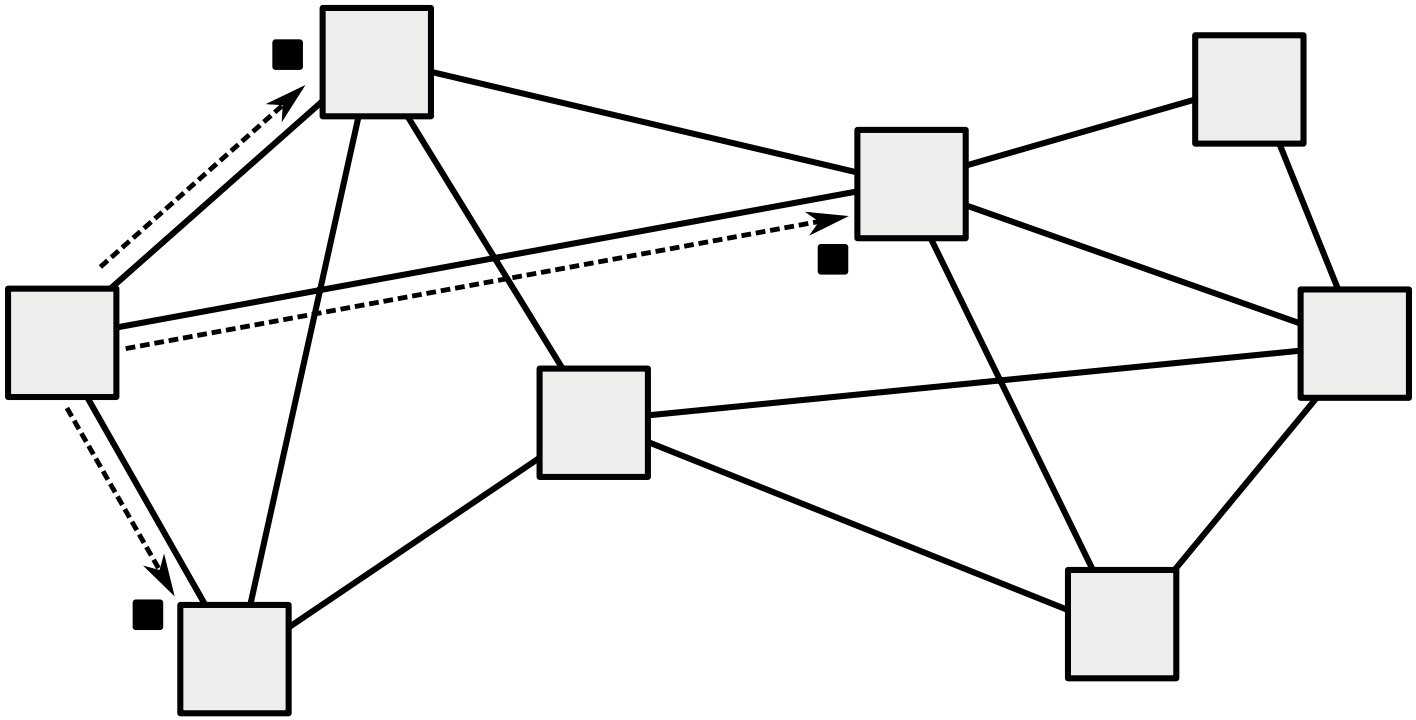


- Cada bloque se relaciona con el anterior
- Contiene una lista de transacciones

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

¿Cómo se crean Bitcoins?, Minado

- Algunos nodos (mineros) de la red crean Bloques nuevos
- Los nuevos bloques aparecen cada 10 minutos



- Los nuevos bloques son enviados a toda la red

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Algunas preguntas

Algunas preguntas

- **¿Y dónde se gana dinero?**

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Algunas preguntas

- **¿Y dónde se gana dinero?**
  - Por cada bloque que se crea (se **ganan**) 12.5 Bitcoin
  - Por cada transacción que entra en la blockchain se **cobra** un monto variable

- **¿Qué pasa si dos mineros crean un bloque al mismo tiempo?**

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Algunas preguntas

- **¿Y dónde se gana dinero?**
  - Por cada bloque que se crea (se **ganan**) 12.5 Bitcoin
  - Por cada transacción que entra en la blockchain se **cobra** un monto variable

- **¿Qué pasa si dos mineros crean un bloque al mismo tiempo?**
  - Se produce un **conflicto** y todos en la red deciden cual bloque queda en la blockchain

- **¿Cómo sé si mi transacción es válida?**

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Algunas preguntas

- **¿Y dónde se gana dinero?**
  - Por cada bloque que se crea (se **ganan**) 12.5 Bitcoin
  - Por cada transacción que entra en la blockchain se **cobra** un monto variable

- **¿Qué pasa si dos mineros crean un bloque al mismo tiempo?**
  - Se produce un **conflicto** y todos en la red deciden cual bloque queda en la blockchain

- **¿Cómo sé si mi transacción es válida?**
  - Nunca se sabe, solo tenés una probabilidad muy alta que no sea **revertida**

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Y respondiendo la pregunta importante...

¿Puedo comprar un alfajor con Bitcoin?

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Y respondiendo la pregunta importante...

¿Puedo comprar un alfajor con Bitcoin?

Sí

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Y respondiendo la pregunta importante...

¿Puedo comprar un alfajor con Bitcoin?

Sí, siempre que:

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Y respondiendo la pregunta importante...

¿Puedo comprar un alfajor con Bitcoin?

Sí, siempre que:

- el vendedor acepte Bitcoin

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Y respondiendo la pregunta importante...

¿Puedo comprar un alfajor con Bitcoin?

Sí, siempre que:

- el vendedor acepte Bitcoin
- estés dispuesto a pagar 70 dólares por la transacción

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Y respondiendo la pregunta importante...

¿Puedo comprar un alfajor con Bitcoin?

Sí, siempre que:

- el vendedor acepte Bitcoin
- estés dispuesto a pagar 70 dólares por la transacción
- y esperar una hora para asegurarte que la transacción sea válida

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

DEPARTAMENTO
DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

¡Gracias!

¿Preguntas?