UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

ciie
Centro de Investigación
e Innovación Educativa

Consenso distribuido

2.2 Blockchain

¿Por qué no se utilizan identidades en Bitcoin?

1. La identidad es algo difícil de lograr en un sistema persona a persona

2. La anonimidad es algo deseado en Bitcoin, por ahora es pseudo anónimo.

3. Siempre debemos asumir que existen un 50% de nodos deshonestos.

Idea clave: la prueba de trabajo en el consenso

1. En la construcción de cada bloque, proporcionalmente a la cantidad de poder de cómputo un nodo es elegido.
2. Este nodo propone el siguiente bloque en la cadena.

Otros nodos implícitamente aceptan/rechazan este bloque de acuerdo a las siguientes opciones:

- Si todas las “tx” contenidas y el bloque cumplen con todas las reglas, entonces un próximo bloque comenzará a construirse a partir de este.
- Si alguna regla no se cumple entonces ese bloque se ignorará y la cadena se extenderá a partir de un bloque anterior.

Simplificación del algoritmo de consenso Bitcoin

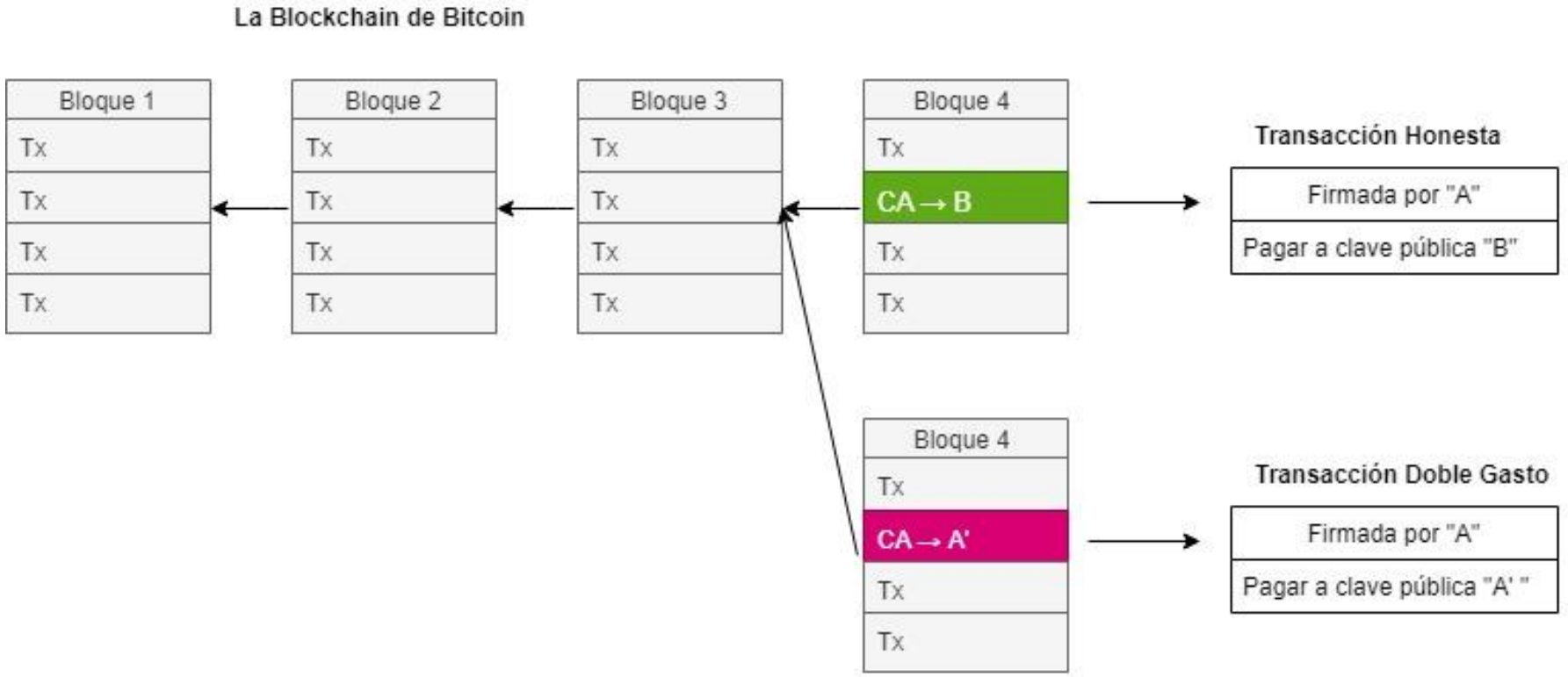
De esta forma funciona Bitcoin:

1. Las nuevas transacciones son transmitidas a todos los nodos.
2. Cada nodo escucha todas las transacciones y propone un orden en un bloque.
3. En cada ronda, a un nodo aleatorio le toca transmitir un bloque nuevo.
4. Los otros nodos lo aceptan solamente si todas las transacciones dentro de él son válidas (no han sido previamente gastadas y tienen firmas válidas)
5. Los nodos expresan la aceptación del bloque creando un próximo bloque en donde incluyen el hash de este.

Nota: En este caso estamos hablando de “nodos mineros”, en otras lecciones se cubrirán los distintos tipos de nodos.

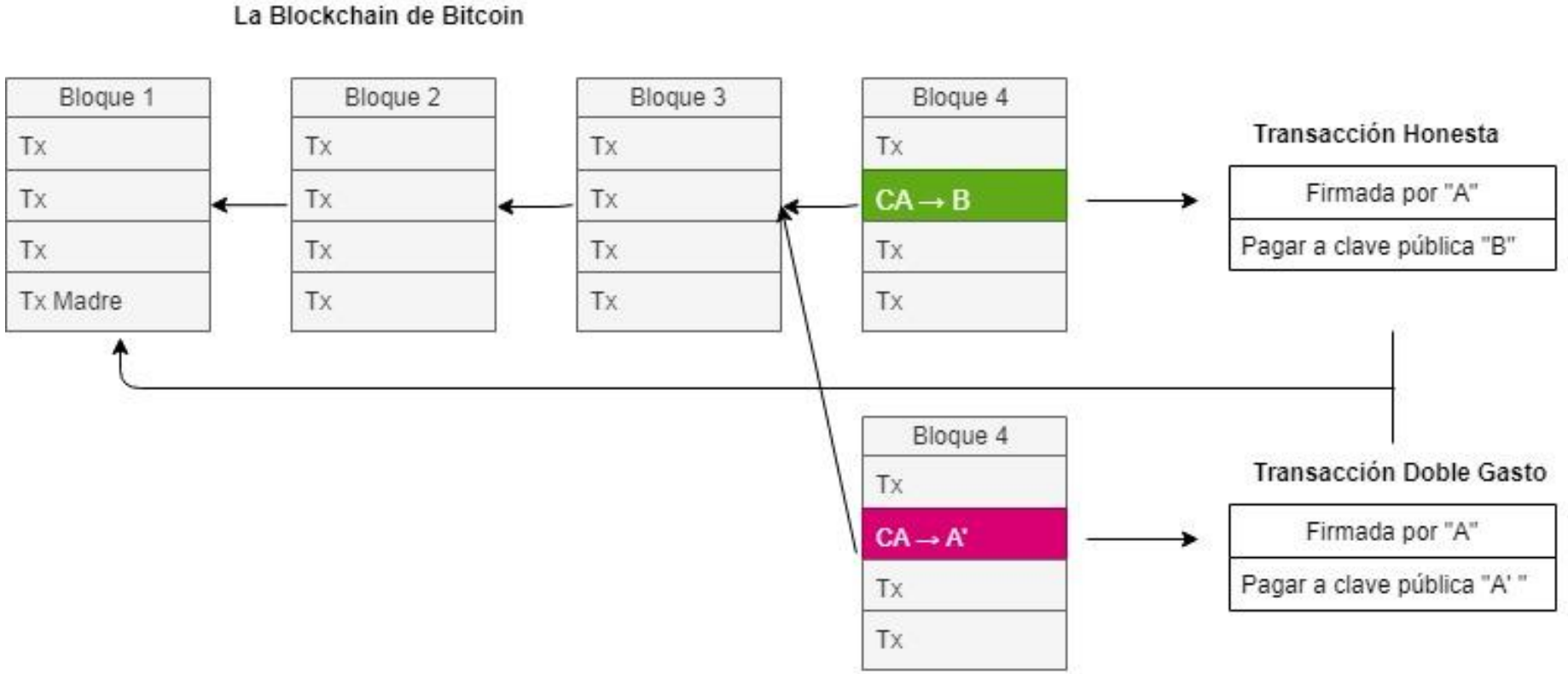
¿Cómo podría operar un nodo malicioso?

Ataque doble gasto: “A” crea dos transacciones, una en la que envía a “B” Bitcoin y otra en la que gasta esos mismos Bitcoin a una dirección que también controla, llamémosla “A’ ”.



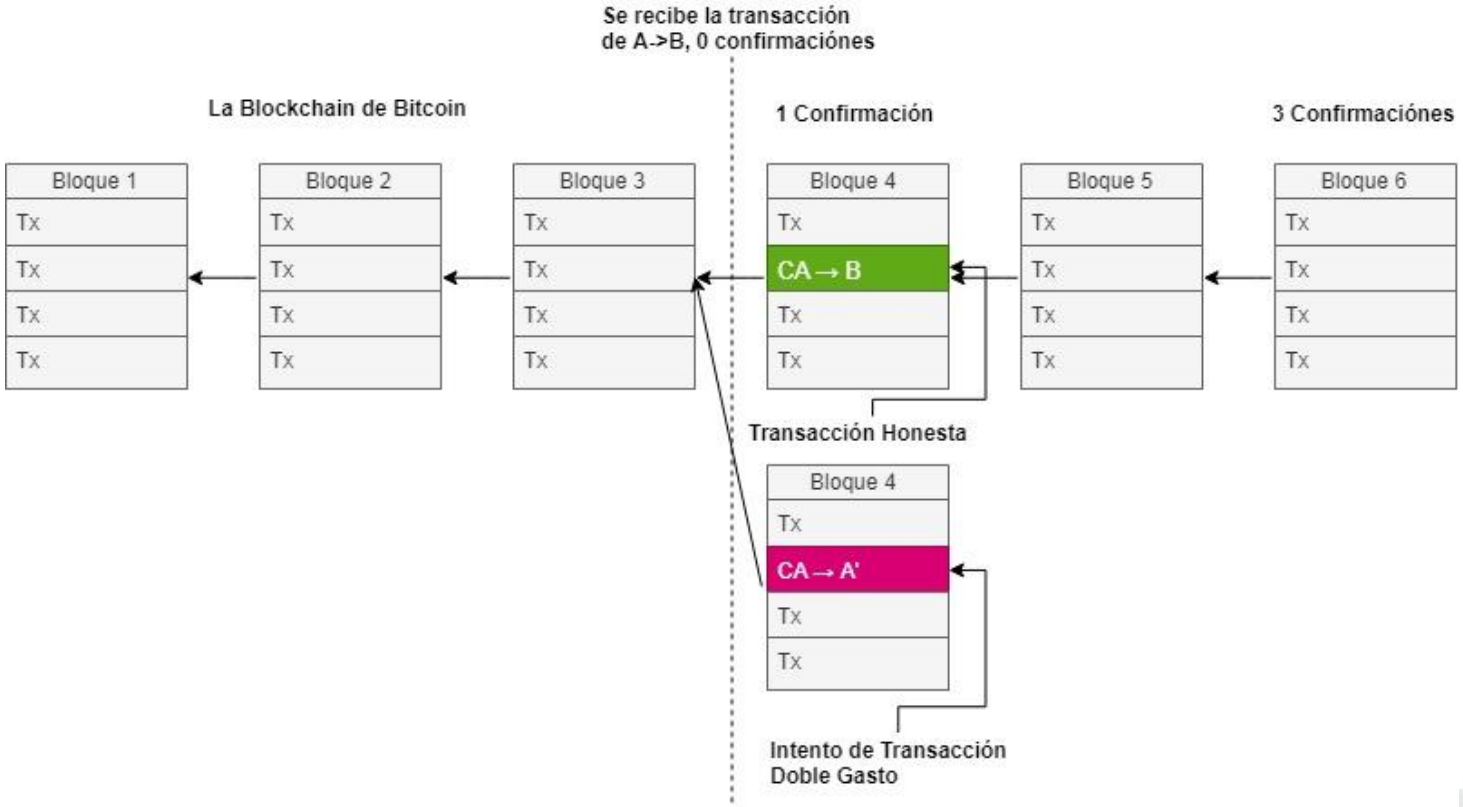
¿Cómo podría operar un nodo malicioso?

Cómo se gastan los mismos Bitcoin, solo una de estas transacciones puede incluirse en la cadena de bloques. Las flechas son punteros de un bloque al bloque anterior en donde “A” tenia sus monedas.



Forma de prevenir un doble gasto

Para prevenir este doble gasto, “B” debe esperar hasta que la transacción se incluya en la cadena de bloqueo y tenga algunas confirmaciones.



Cálculos de ataque en el Whitepaper de Bitcoin

p = probabilidad de que un nodo honesto encuentre el próximo bloque
q = probabilidad de que el atacante encuentre el próximo bloque
q_z = probabilidad de que el atacante llegue a alcanzar desde z bloques atrás.

$$\sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012
```

Nota: La probabilidad de que un atacante produzca “Z” bloques consecutivos se reduce exponencialmente. Con 3 confirmaciones está en el orden de 1%.

Recapitulando

1. La protección contra transacciones inválidas es criptográfica, pero es forzada a través del mecanismo de consenso descentralizado.

2. La protección contra doble gastos se realiza puramente por el consenso a través del tiempo. Mientras más antigua es la transacción, más confiable es.

3. Nunca se está 100% seguro que una transacción esta en la blockchain con mayor trabajo acumulado. La garantía es probabilística.