UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

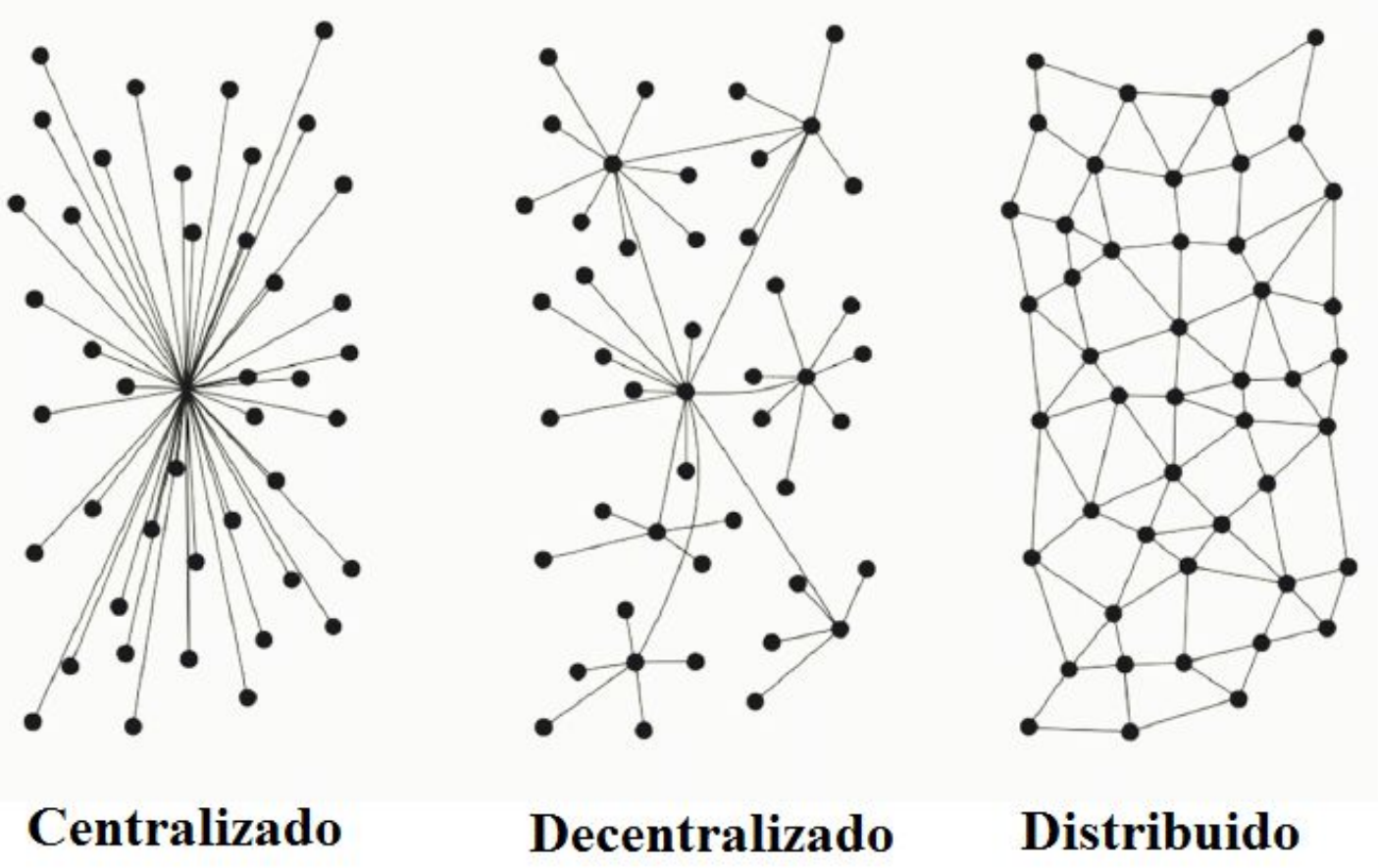
ciie
Centro de Investigación
e Innovación Educativa

Consenso distribuido

2.1 Consenso distribuido

Topología de redes:

Existen 3 topologías de redes



La descentralización es un continuo

Examinaremos 2 ejemplos de protocolos que seguramente ya conocen:

- El E-mail es un protocolo distribuido, sin embargo los proveedores de servicios como Gmail y Yahoo! son centralizados

- Torrent también es un ejemplo de protocolo distribuido para intercambio de archivos P2P, sin embargo hay distintos clientes de software que nos permiten utilizarlo

Aspectos de la descentralización de Bitcoin

Analizaremos 3 de estas 5 preguntas:

1. ¿Quién mantiene el registro?
2. ¿Quién tiene autoridad sobre qué transacciones son válidas?
3. ¿Quién crea nuevos Bitcoins?
4. ¿Quién determina cómo cambian las reglas del sistema?
5. ¿Cómo los Bitcoins adquieren valor de intercambio?

Elementos más allá del protocolo

- Las casas de intercambio, el software de las wallets, proveedores de servicios de pagos, etc.

Aspectos de la descentralización de Bitcoin

Una red persona a persona (P2P):

- Es una red pública, abierta y neutral a sus participantes, esto hace que tenga una baja barrera de entrada

Minería de Bitcoins:

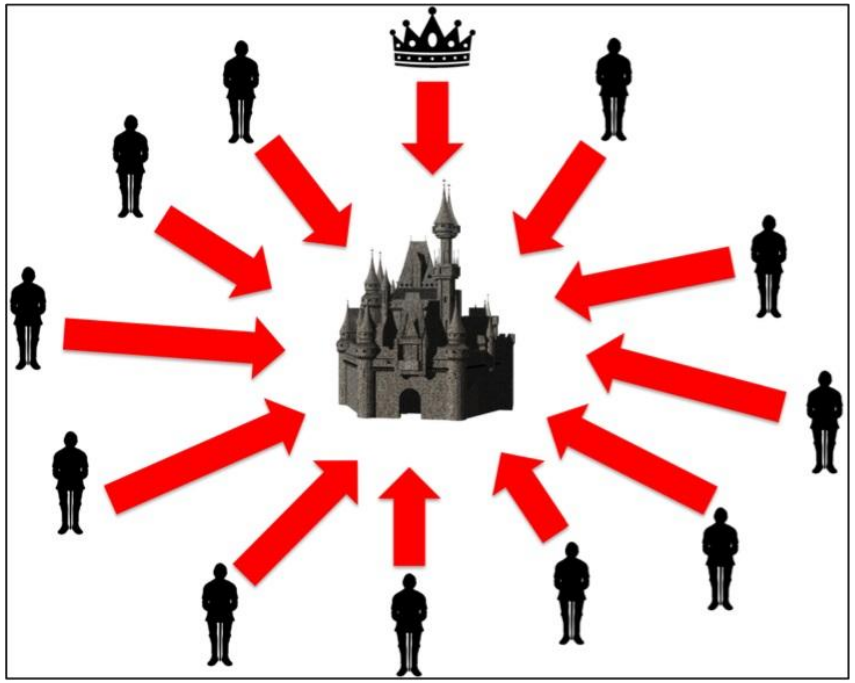
- Está abierta a cualquier participante, pero los incentivos y la carrera por el desarrollo del hardware hizo inevitable su centralización en algunos participantes. Esto no está bien visto por muchos de los usuarios.

Mejoras del software:

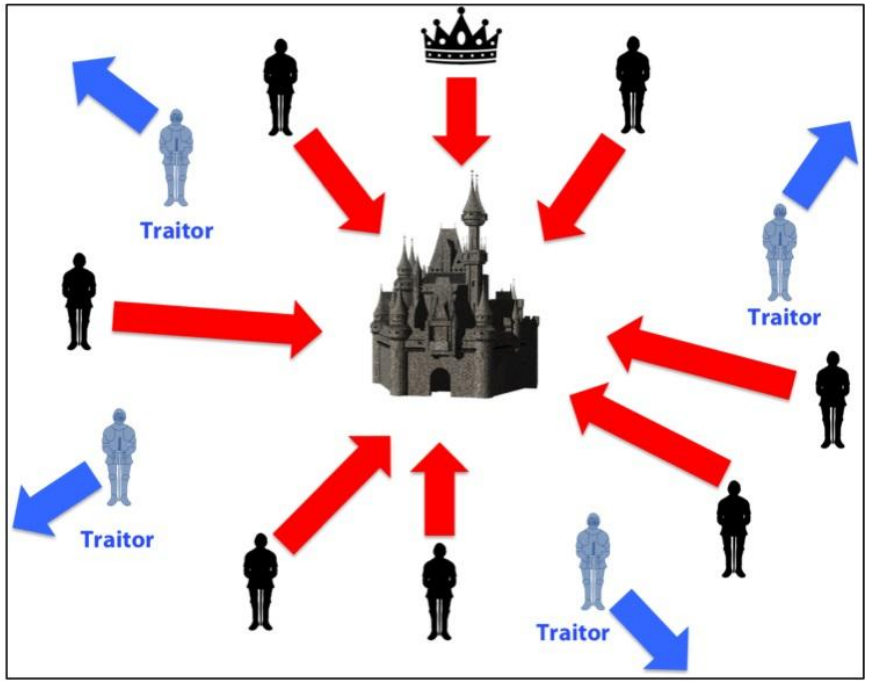
- Los desarrolladores más confiables por la comunidad también han centralizado la toma de decisiones y esa centralización tampoco está bien vista por muchos de los usuarios.

El desafío clave de Bitcoin:

El problema de los generales Bizantinos es un experimento mental para plantear, el problema que se da entre un conjunto de sistemas informáticos que tienen un objetivo común.



Un ataque coordinado nos lleva hacia la victoria



Un ataque descordinado nos lleva hacia una derrota

Definición de consenso distribuido

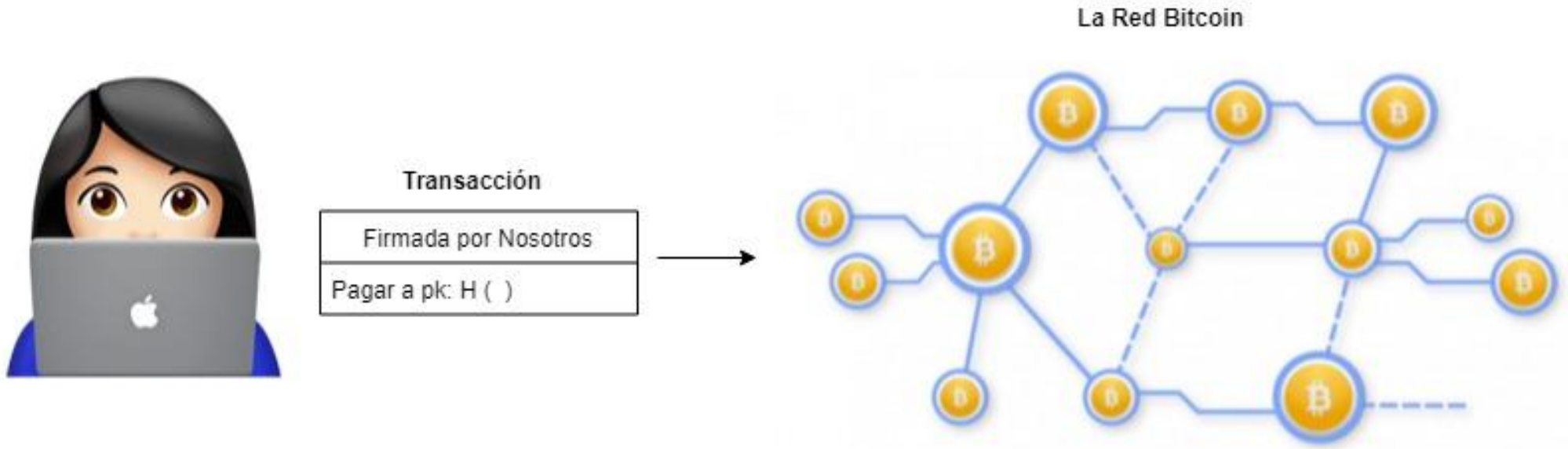
1. El protocolo corre una ronda y todos los nodos determinan el mismo valor.

2. Este valor tiene que haber sido propuesto por un nodo que se esté comportando honestamente

3. En un momento en el tiempo, puede que algunos nodos se encuentren des sincronizados. Pero a lo largo del tiempo se irán sincronizando y construyendo el consenso.

Bitcoin es un sistema persona a persona

Cuándo queremos realizar una transacción: tenemos que transmitir ese mensaje a todos los nodos de Bitcoin, utilizando lo que se llama un protocolo de susurros.



Reglas del protocolo: Transacciones

1. Verificar que la sintaxis de la transacción sea correcta.
2. Asegurarse que ninguna de las listas de entradas o salidas esté vacía
3. Tamaño en bytes <= MAX_BLOCK_SIZE
4. Cada valor de salida, así como el total, debe estar dentro del rango de dinero legal
5. Asegurarse de que ninguna de las entradas tenga hash = 0, n = -1 (transacciones de base monetaria)
6. Comprobar que nLockTime <= INT_MAX , tamaño en bytes> = 100 y sig opcount <= 2
7. Rechazar transacciones "no estándar": scriptSig hace otra cosa que no sea empujar números en el stack, o scriptPubkey no coincide con los formatos permitidos
8. Rechazar una transacción si ya tenemos una que coincide en el grupo, o en un bloque en la rama principal
9. Para cada entrada, si la salida a la que se hace referencia existe en cualquier otra transacción en el grupo, rechazar esta transacción.
10. Para cada entrada, buscar en la rama principal y el grupo de transacciones para encontrar la transacción de salida a la que se hace referencia. Si la transacción de salida falta para alguna entrada, esta será una transacción huérfana. Agregar las transacciones huérfanas, si una transacción coincidente aún no está allí.

Reglas del protocolo: Transacciones

11. Para cada entrada, si la transacción de salida a la que se hace referencia es una transacción de base monetaria “coinbase” (es decir, solo 1 entrada, con hash = 0, n = -1), debe tener al menos 100 confirmaciones, COINBASE_MATURITY (100); sino rechazar esta transacción.
12. Para cada entrada, si la salida a la que se hace referencia no existe (por ejemplo, nunca existió o ya se gastó), rechazar esta transacción.
13. Usando las transacciones de salida a las que se hace referencia para obtener valores de entrada, verificar que cada valor de entrada, así como la suma, estén dentro del rango de dinero legal
14. Rechazar transacción si la suma de valores de entrada <suma de valores de salida
15. Rechazar transacción si la tarifa de transacción (definida como suma de valores de entrada menos suma de valores de salida) es demasiado baja para entrar en un bloque vacío
16. Verificar que scriptPubKey sea válido para cada entrada; rechazar si alguno no es válido
17. Agregar al grupo de transacciones
18. "Añadir a la billetera si es mía"
19. Transmitir la transacción a los nodos
20. Para cada transacción huérfana que use esta como una de sus entradas, ejecute todos estos pasos (incluido este) de forma recursiva

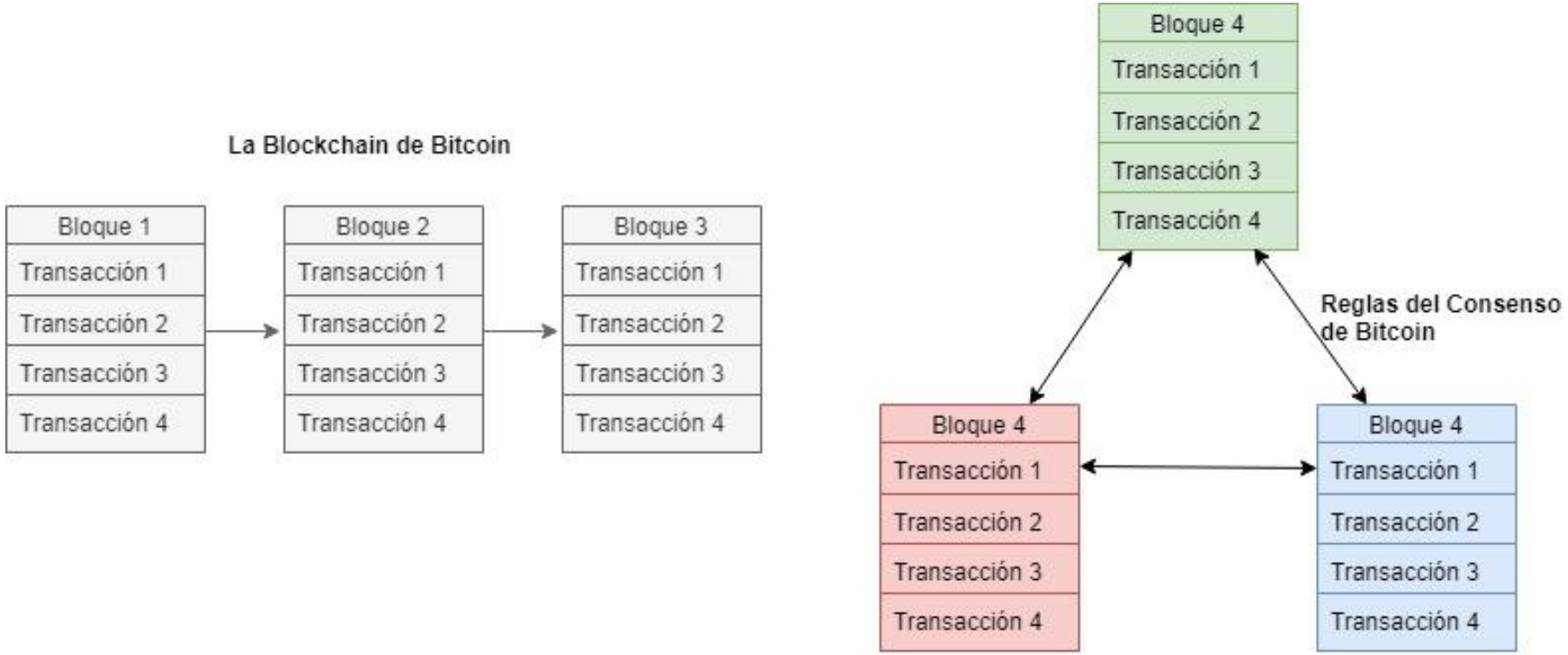
Consenso distribuido en la red Bitcoin

En un momento en particular:

1. Todos los nodos tienen una secuencia de bloques de transacciones que verificaron las reglas del protocolo y que ya hay un consenso que se realizaron, esto se conoce como la cadena de bloques o “blockchain”.

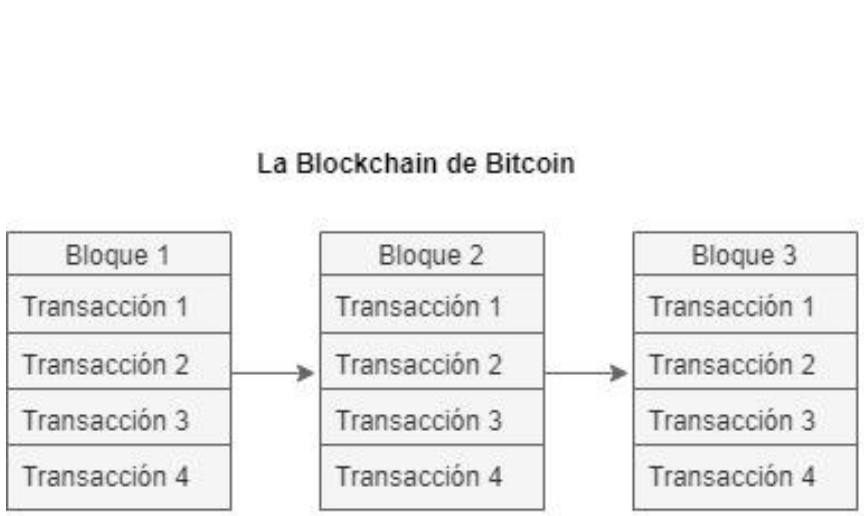
2. Cada uno de los nodos, tiene una lista de transacciones pendientes que ha escuchado.

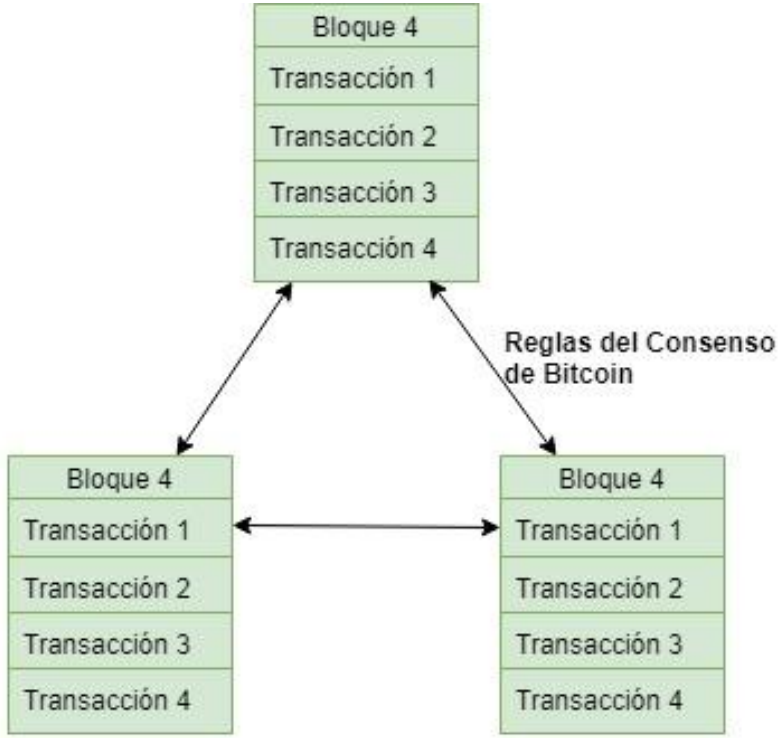
¿Cómo funciona el consenso en la red Bitcoin?



H (Hash del bloque previo + Árbol de merkle de transacciones en el bloque + nonce) => ca978112ca1bb……

¿Cómo funciona el consenso en la red Bitcoin?





H (Hash del bloque previo + Árbol de merkle de transacciones en el bloque + nonce) => 000000000000000000gp1Ca143 ……

Reglas del protocolo: Bloques

1. Verificar que la sintaxis del bloque sea correcta.
2. Rechazar si hay bloque duplicado que tengamos en cualquiera de las tres categorías.
3. La lista de transacciones no debe estar vacía.
4. Bloque de hash debe satisfacer nBits, en la prueba de trabajo
5. La marca de tiempo del bloque no debe ser más de dos horas en el futuro
6. La primera transacción debe ser coinbase (es decir, solo 1 entrada, con hash = 0, n = -1)
7. Para cada transacción, hay que verificar "tx" reglas 2-4
8. Para la transacción de coinbase (primera), la longitud de scriptSig debe ser 2-100
9. Rechazar si la suma de transacciones sig_opcounts > MAX_BLOCK_SIGOPS
10. Verificar el hash del árbol Merkle con todas las transacciones

Reglas del protocolo: Bloques

11. Verificar si el bloque prev (que corresponde al hash anterior) está en la rama principal o en las ramas laterales. Si no es así, agregue esto a los bloques huérfanos, luego haga una consulta entre pares para obtener el primer bloque huérfano perdido en la cadena anterior;
12. Comprobar que el valor de nBits coincide con las reglas de dificultad
13. Rechazar si la marca de tiempo es el tiempo medio de los últimos 11 bloques o antes
14. Para ciertos bloques antiguos (es decir, en la descarga del bloque inicial) verifique que el hash coincida con los valores conocidos
15. Para añadir bloque en el árbol. Hay tres casos: 1. el bloque extiende aún más la rama principal; 2. el bloque extiende una rama lateral pero no agrega suficiente dificultad para que se convierta en la nueva rama principal; 3. El bloque extiende una rama lateral y la convierte en la nueva rama principal.
16. Para cada bloque huérfano en el cual este bloque es su anterior, ejecutar todos estos pasos (incluido este) recursivamente

¿Por qué el consenso distribuido es difícil de lograr?

1. Los nodos pueden crashear
2. Los nodos pueden actuar maliciosamente
3. Los nodos pueden apagarse/encenderse en diferentes momentos

La red es imperfecta entonces:

- No todos los nodos están conectados entre sí
- Fallas en la red
- Latencia en la red

Consenso en Bitcoin: Práctica vs Teoría

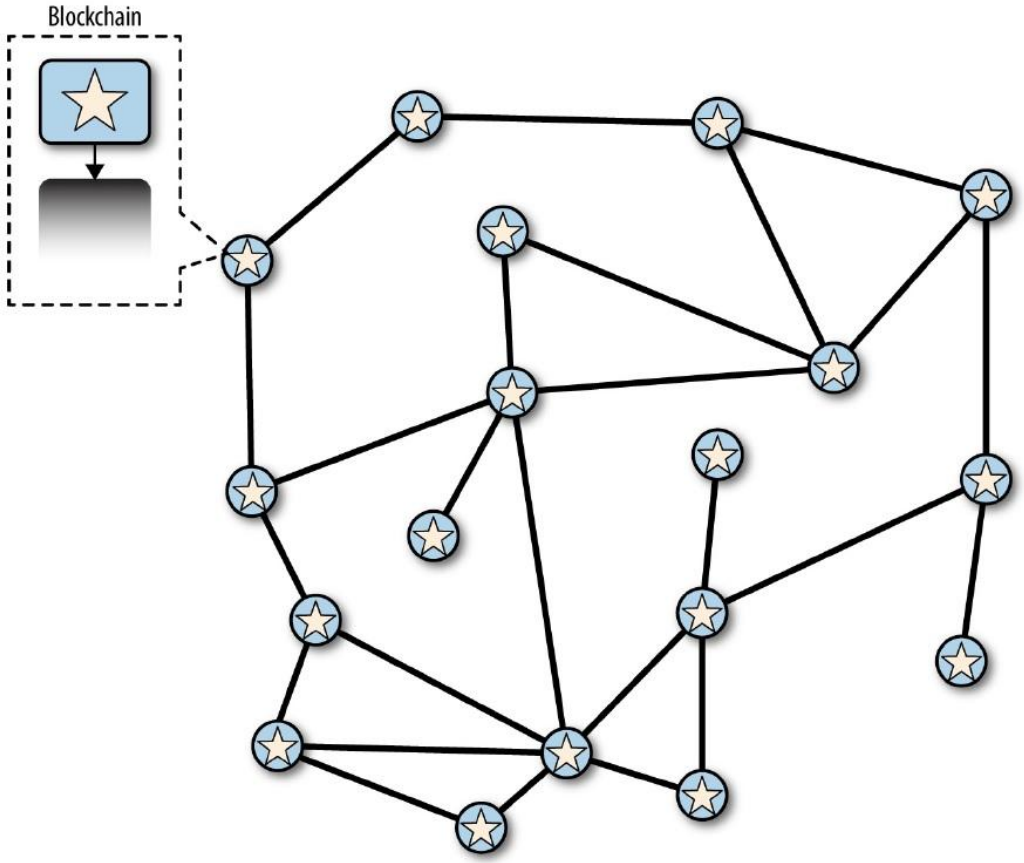
1. El consenso en Bitcoin funciona mejor en la práctica que lo que predice la teoría.

2. La teoría todavía está en desarrollo, recordemos que Bitcoin recién está en su infancia dado que recién cumplió 10 años.

3. La teoría es importante dado que nos ayuda a predecir nuevos comportamientos y ataques a la red.

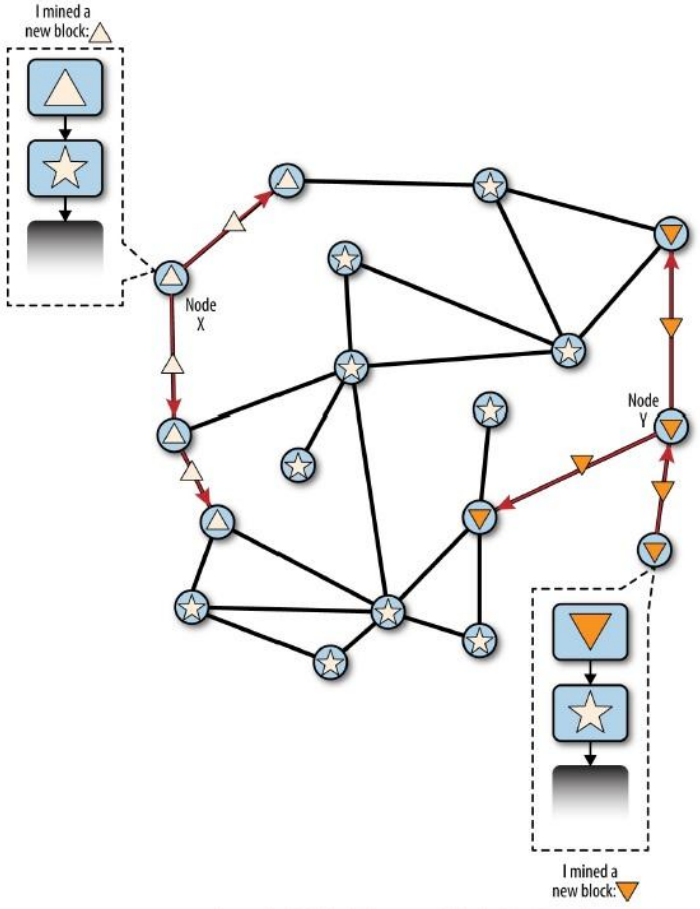
Bifurcación en la cadena de bloques

Antes de la bifurcación, todos los nodos tienen la misma historia y se encuentran sincronizados.



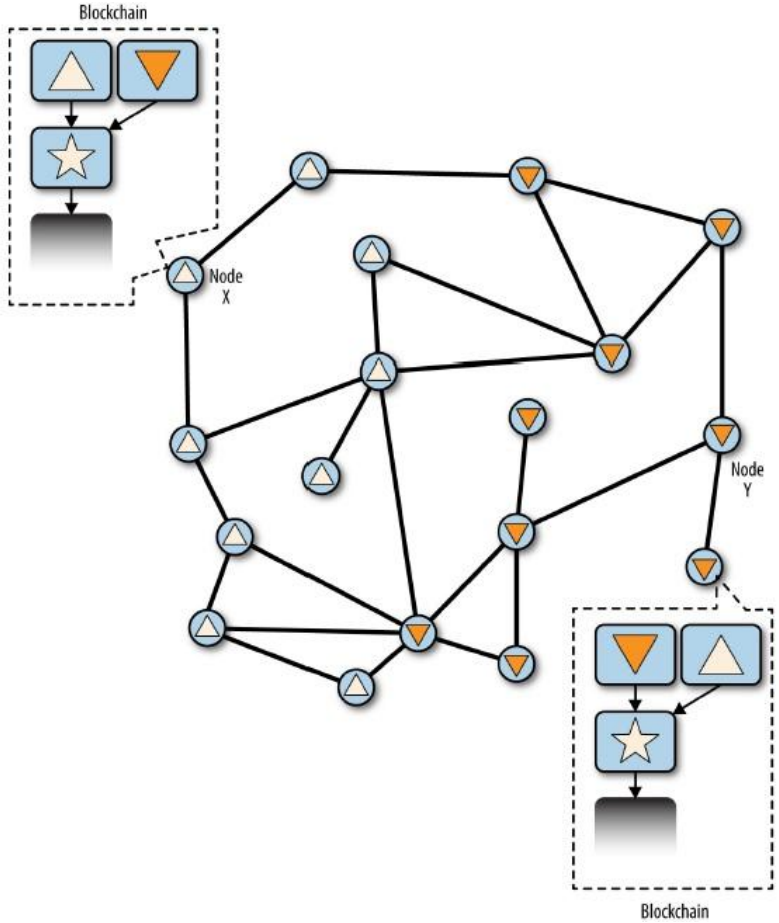
Bifurcación en la cadena de bloques

Dos bloques son hallados simultáneamente y la blockchain se bifurca.



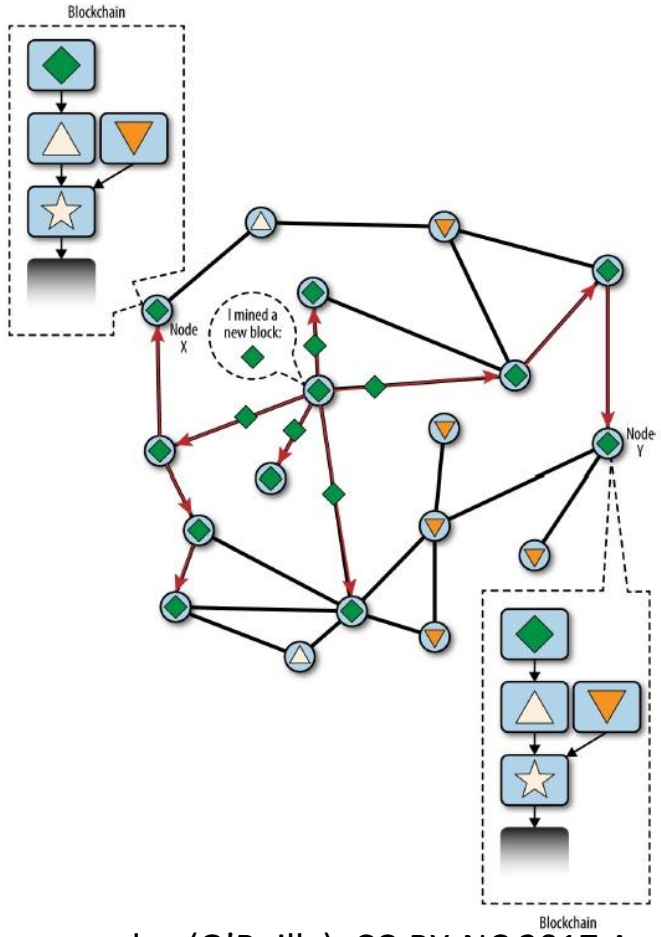
Bifurcación en la cadena de bloques

Ambos bloques son propagados por la red hasta llegar a todos los nodos



Bifurcación en la cadena de bloques

Un bloque nuevo extiende una de las ramas de la cadena y la red re converge



Bifurcación en la cadena de bloques

El bloque nuevo se propaga a toda la red. Los mineros empiezan a construir sobre la cadena más larga.