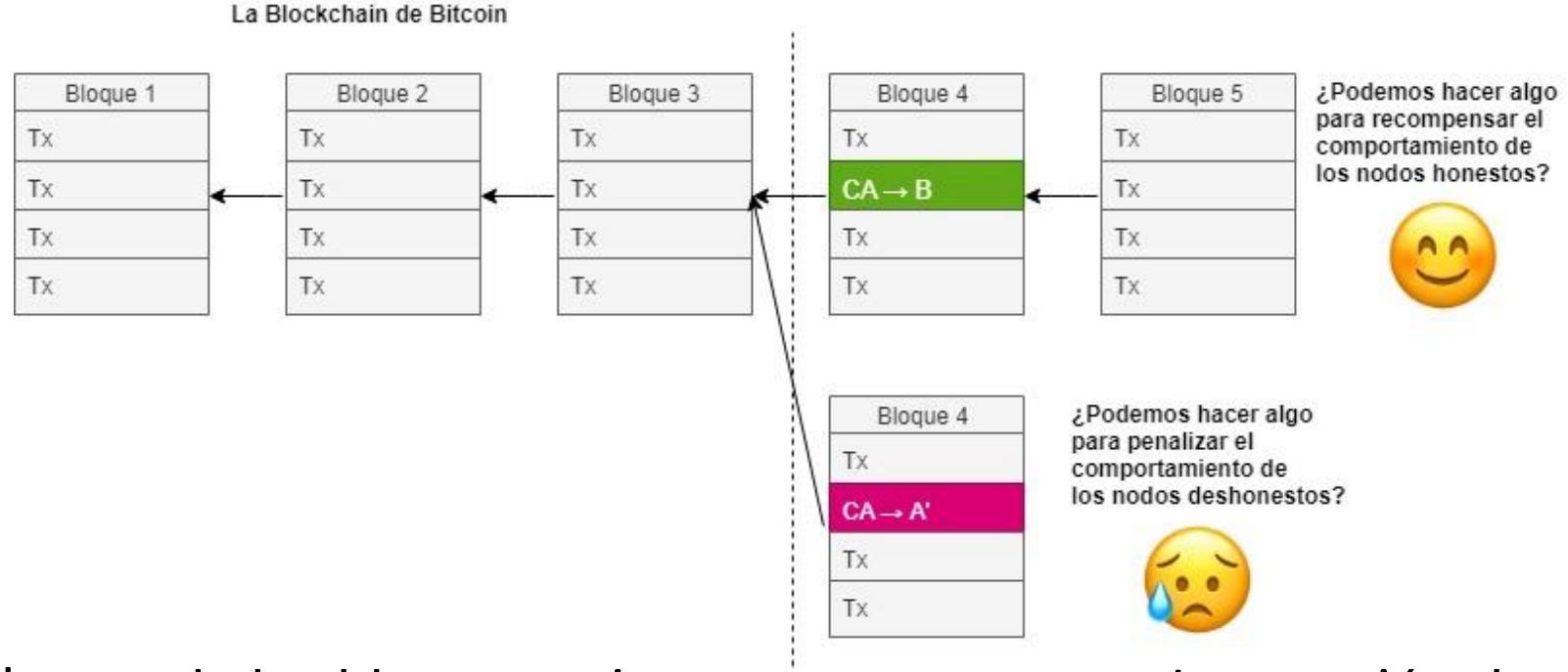
Consenso distribuido

2.3 Prueba de trabajo

Nunca hay que asumir honestidad de los nodos

¿Podemos darle **INCENTIVOS** a los nodos para que se comporten honestamente?

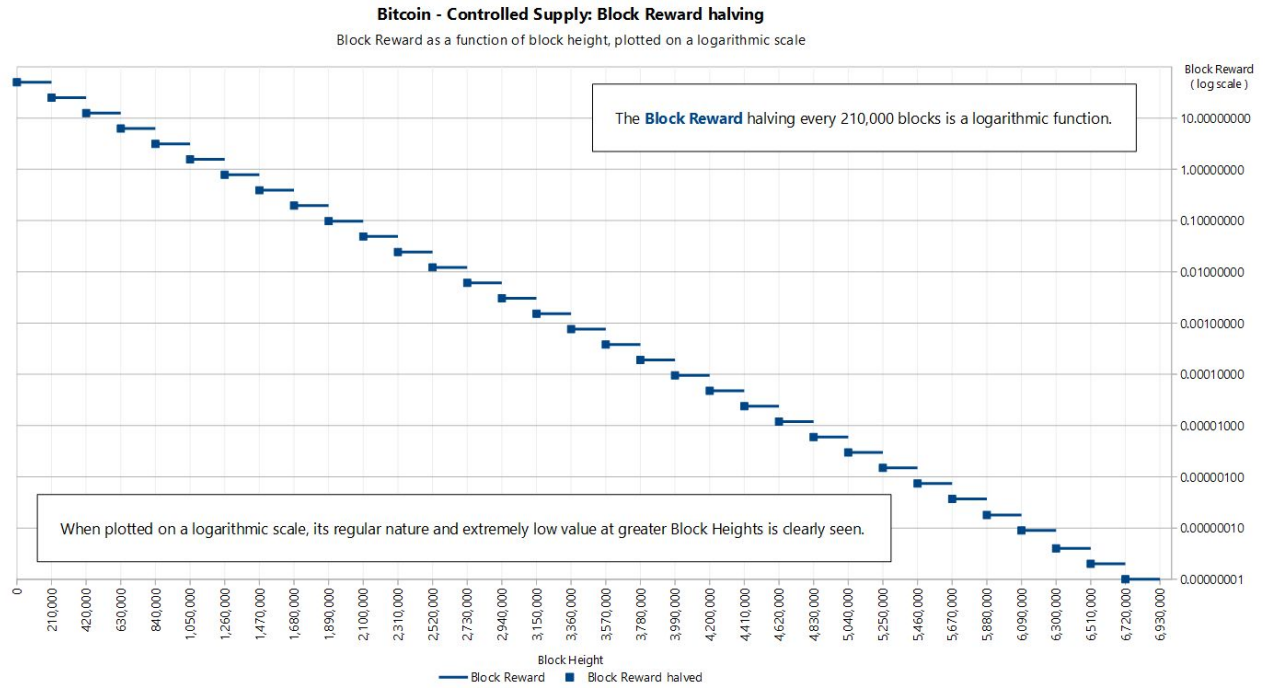


En cada uno de los bloques existe una recompensa: La creación de nuevas monedas (base monetaria) más las tarifas de uso de la red de cada una de las transacciones.

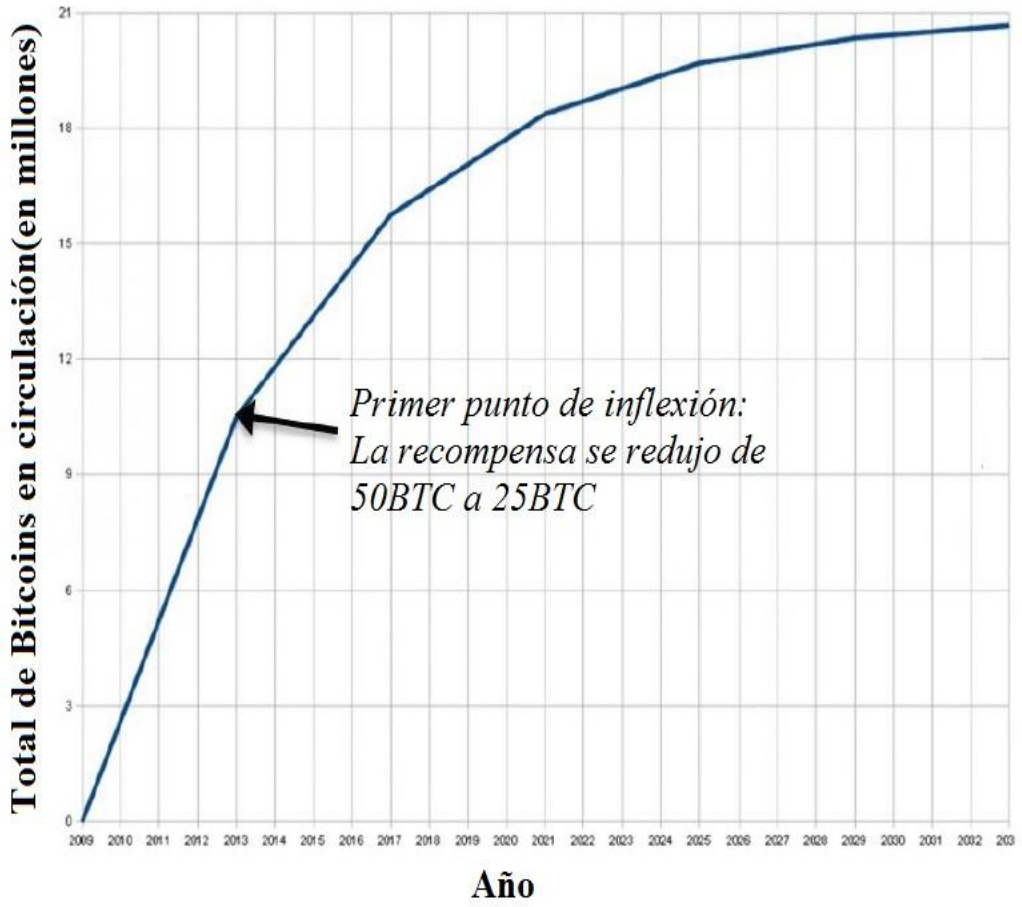
Incentivo 1: Creación de nuevos Bitcoins

El creador de un nuevo bloque puede:

- Incluir en el bloque la primera transacción, llamada transacción “coinbase” (base monetaria)
- Puede elegir quien va a recibir esa primera transacción.



Incentivo 1: Bitcoin es finito



- Suministro total: Ligeramente menos que 21 millones.
- La recompensa de creación de bloques nuevos es la única forma de creación de Bitcoin.
- Esta recompensa se termina en el año 2140. La recompensa por tarifas de transacciones continúa.

Incentivo 2: Tarifa de las transacciones

Las propinas por el uso de la red que se incluyen en las transacciones funcionan de la siguiente manera.

1. El creador de la transacción puede hacer que el valor de salida de la transacción sea menor que el valor de la entrada.
2. A la salida menos la entrada se la llama tarifa de la transacción, se suman todas las tarifas de las transacciones incluidas en un bloque y el creador del bloque las puede sumar a la transacción “coinbase”
3. Es puramente voluntario, como una propina. Muchas veces se la llama así también.

Algunos problemas persistentes en la Red Bitcoin

A pesar de estos problemas sigue funcionando Bitcoin:

1. ¿Cómo elegir un nodo aleatoriamente?
2. ¿Cómo hacemos para que no todas las personas quieran correr un nodo minero para obtener las recompensas?
3. ¿Cómo prevenimos los ataques Sybil?

Nota: En seguridad informática, un ataque Sybil ocurre cuando un sistema distribuido es corrompido por una misma entidad que controla distintas identidades de dicha red.

Distintos mecanismos de consenso descentralizado

1. Prueba de trabajo

2. Prueba de participación

3. Prueba de participación delegada

4. Prueba de Autoridad

Prueba de trabajo

1. Selecciona los nodos en proporción a su poder de cómputo (Hashing power).

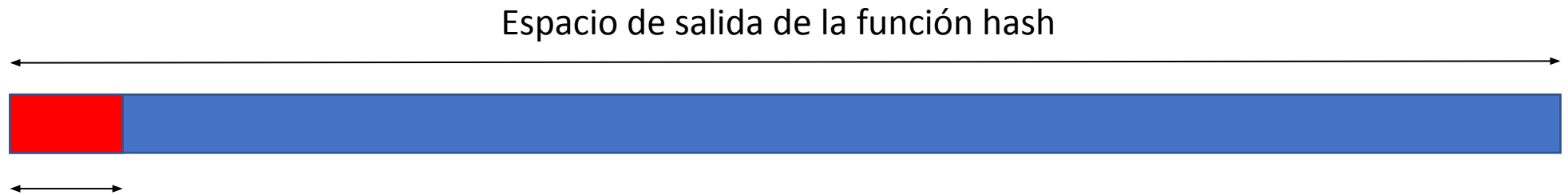
2. Los nodos compiten entre sí por su turno a crear un bloque nuevo.

3. A medida que pasa el tiempo, se hace más difícil realizar un ataque Sybil.

Rompecabezas Hash

Para crear un bloque válido, hay que encontrar un nonce (un numero de 32 Bits) que cumpla que:

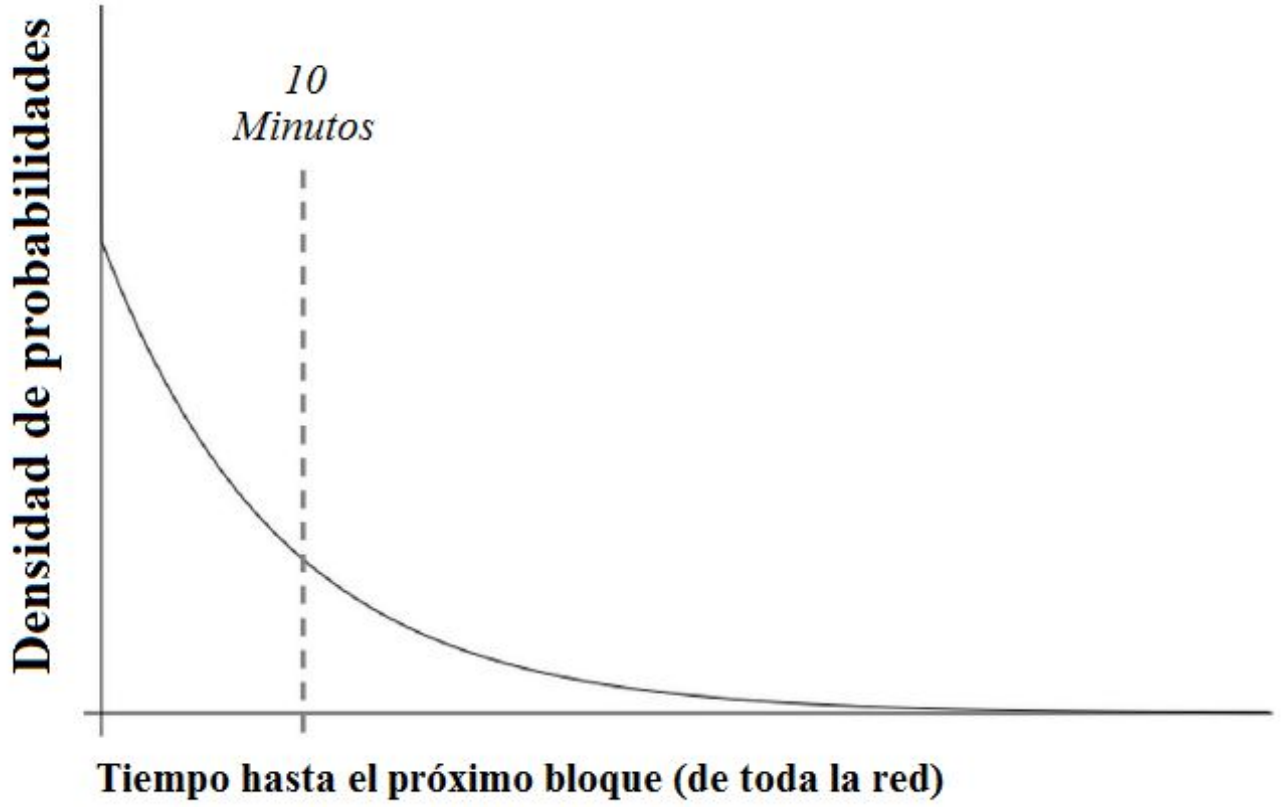
$$H\,(Nonce \,||\, prev\_hash \,||\, tx \,||\, \ldots \,||\, tx\,) < \text{Objetivo}$$



- Como la función hash es resistente a colisiones, la única forma de tener éxito es probando una cantidad suficientes de “nonces” hasta que se tiene suerte.
- El tiempo de creación de bloques es 10 minutos en promedio
- La dificultad de la red se ajusta cada 2016 bloques (aproximadamente 14 días)
- El espacio objetivo es inversamente proporcional a la dificultad de la red.

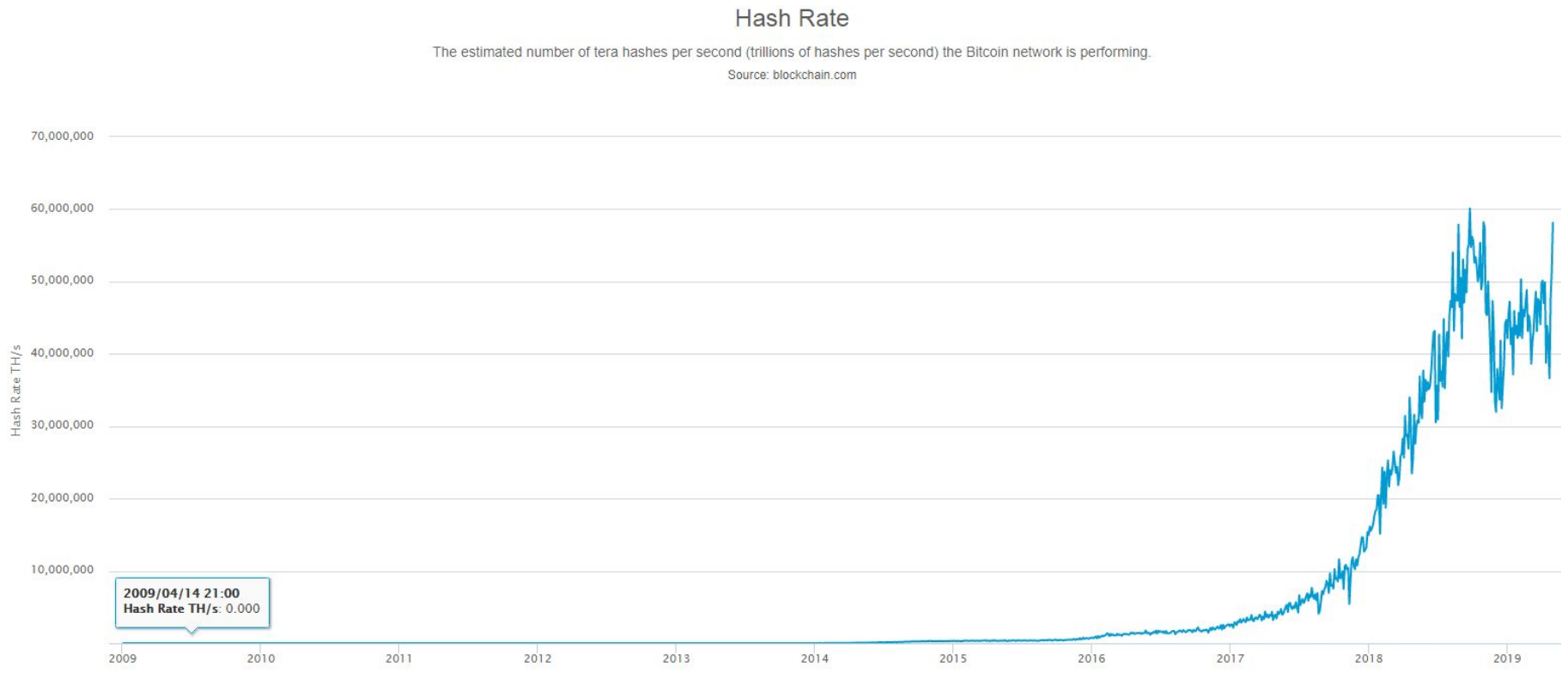
Rompecabezas Hash parametrizable

Resolver estos rompecabezas hash es probabilístico, cada 10 minutos un bloque nuevo es emitido en promedio.



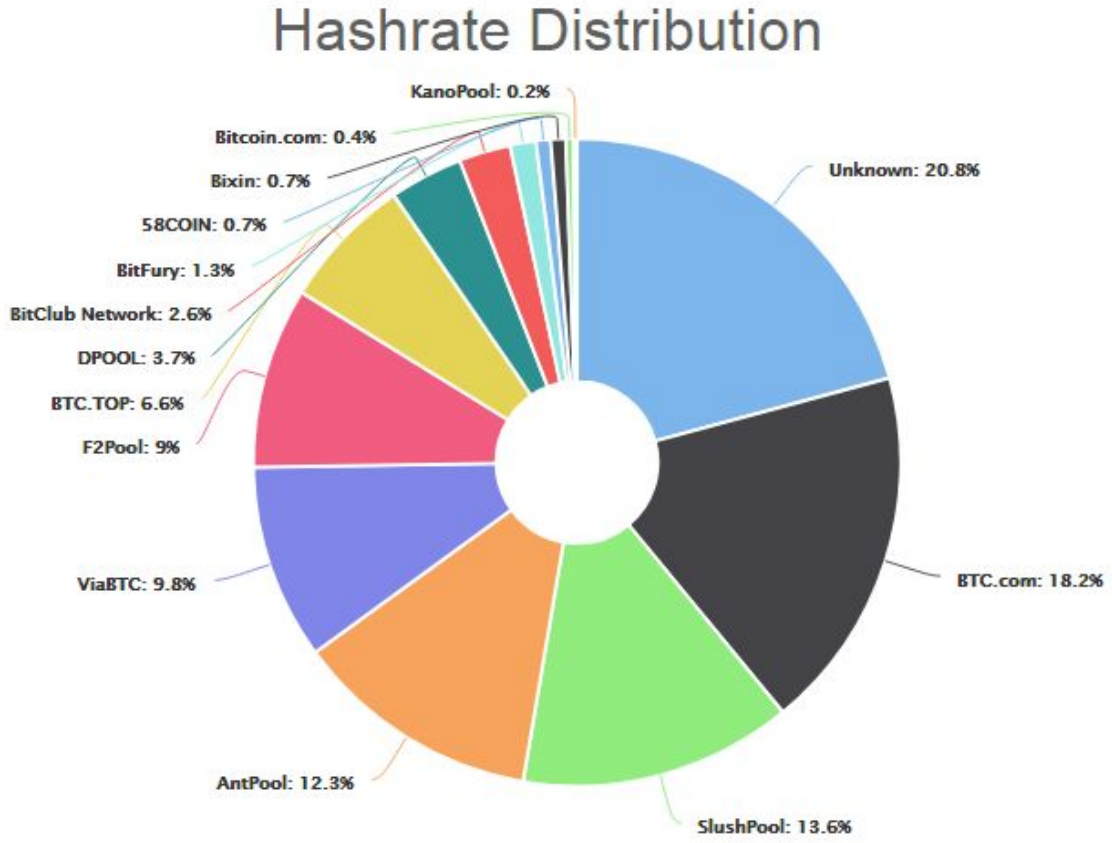
Prueba de trabajo: Hashing power

Mayo 2019: 60.000.000 TH/s



Prueba de trabajo: Distribución de Hashing power

Mayo 2019: Los tres pooles de minería que más poseen aportan el 45% del hashing power de la red de Bitcoin.



Prueba de trabajo: Es fácil de verificar

Los nonces tienen que ser publicados como parte del bloque. Los otros nodos mineros o nodos completos verifican que se haya cumplido:

$$H\,(Nonce \,||\, prev\_hash \,||\, tx \,||\, \ldots \,||\, tx\,) < \text{Objetivo}$$