

¿Qué es?

Es la necesidad de que los nodos(mineros) que pertenecen a la blockchain lleguen a un acuerdo sobre el estado que tiene la cadena de bloques de las criptomonedas, que contiene los registros de todas las transacciones validadas que se realizan por dichos nodos.Consiguiendo que los nodos defectuosos o malignos no agreguen a la cadena de bloques transacciones inválidas.Para ello se usa el Proof of work para llegar a dicho consenso sobre qué bloques son o no válidos de agregar a la cadena.

¿Cómo funciona?

Los nodos(mineros) compiten por realizar problemas criptográficos y agregar un nuevo bloque a la cadena de bloques.Una vez que un nodo resuelve un problema lo distribuye por la red junto con el bloque que quiere agregar y sirve de prueba para que se sepa que el minero trabaja correctamente(no es maligno). El resto de nodos verifican y aceptan si hay que agregar o no dicho bloque.En caso de serlo y verificar que es un bloque válido se agrega a la cadena de bloques.

¿Cuándo se aplica?

Cuando se quiere verificar una transacción de criptomonedas entre dos direcciones de la red y agregarla a la cadena de bloques pública.