El nonce o número d'un sòl ús.

A BitCoin

Una vegada més utilitzem la primera blockchain com a cas d'estudi. Un nonce és un número d'un sòl ús.

Quan els miners de Bitcoin construeixen el següent bloc que volen minar resolen un puzzle matemàtic. Aquest puzzle matemàtic consisteix en trobar una funció HASH que comence per un determinat número de zeros. Aquest número de zeros s'anomena la dificultat del bloc, i el augmenten i reduïxen els miners, en funció de la demanda.

Com que el bloc està format per transaccions, si un candidat a bloc conté unes transaccions determinades, li correspon un mateix HASH, de tal forma que el puzzle no és viable. Bitcoin afegeix al bloc un número d'un sol ún: el nonce, un número natural de 256 bits. El miner afegeix al candidat a bloc que pretén minar el camp *nonce*, amb un valor aleatori i prova de calcular-ne el HASH. Si compleix la condició, es considera que ha minat el bloc i s'emporta la recompensa.

Aquest funcionament de Bitcoin és la base del algorisme de consens PoW (*proof of work*, prova de treball). La majoria de blockchains amb algorisme de consens PoW utilitzen un nonce, diferint unes d'altres en la funció HASH utilitzada per minar el bloc.

Als Wallets d'Ethereum i blockchains EVM-compatibles

Ethereum és una xarxa que a vegades té problemes de congestió. Les transaccions enm Ethereum costen gas. El gas quie costa cada instrucció de la EVM és constant (excepte aquelles que criden altres contractes o accedixen al magatzem, que no son constants, però sí que són deterministes). El gas que costa una transacció simple és constant.
El que no és constant és el preu del gas, expresat en la moneda nativa (Eth si és Ethereum, MATIC si és Poligon, BNB si és BSC etc). Abans de The Merge Ethereum era PoW. Els miners s'emportaven el gas pagat pels wallets al executar transaccions. Despres del pas a PoS (*Proof of Stake*, prova de particiació) els blocs els construïxen els *validadors*, que són els qui s'emporten el gas.

De vegades es produïx una situació de competitivitat al accedir a la xarxa, que permet als usuaris pagar un valor més alt als constructors de blocs per tal de assegurar-se la inclusió de la transacció. El preu del gas que paga cada usuari el decidix el propi usuari. Si un usuari envia una transacció i veu que els constructors de blocs no la inclouen pot oferir la mateixa transacció per un preu major.

Si enviem la mateixa transacció dues vegades, ¿cóm sabem si és la mateixa o una diferent amb els mateixos origen, destí, quantitat però major preu de gas? Cada *wallet* té un número d'un sol ús per a cada xarxa. Quan s'envia una transacció el *nonce* s'inclou a la transacció i s'incrementa al Wallet.

Si es vol reenviar una mateixa transacció s'inclou el nonce de la transacció original. Si és una nova, portarà un nonce actualitzat.