Grant Thornton

Blockchain

Glosario de Blockchain

Blockchain
Es un tipo de registro digital distribuido en el que se plasman datos de manera secuencial y permanente en forma de "bloques" (*blocks*). Cada bloque nuevo que se crea está conectado al bloque inmediatamente anterior a través de una firma criptográfica y forma una "cadena" (*chain*). De esta manera se consigue una autovalidación inviolable de los datos que permite procesar y registrar transacciones en la cadena sin necesidad de recurrir a un agente certificador externo. Este registro no está alojado en un único lugar ni es gestionado por un único propietario, sino que está compartido y pueden acceder a él aquellas personas que dispongan de los permisos oportunos; de ahí qu e sea "distribuido".

Bloque
Un paquete de datos que contiene múltiples transacciones que se han producido durante un periodo de tiempo determinado.

Cadena
El enlace criptográfico que mantiene los bloques unidos a través de una función criptográfica denominada «hash».

Minería de datos (*data mining*)
El proceso de resolución de problemas criptográficos que utiliza hardware informático para añadir bloques recién creados (y encriptados mediante la función hash) a una cadena de bloques pública, como puede ser bitcoin. Al realizar esta función, los *data miners* consiguen que la cadena de bloques siga registrando transacciones de forma activa y, como incentivo, son recompensados con bitcoins recién acuñadas por las molestias.

Ethereum
Un sistema de blockchain público desarrollado como proyecto de código abierto; su arquitectura funciona de forma remota en la Máquina Virtual Ethereum. Utiliza "ethers", una criptomoneda, como token y apoya el almacenamiento y la ejecución de los denominados smart contracts o "contratos inteligentes".

Hash
El resultado de aplicar una función algorítmica a los datos para convertirlos en una cadena aleatoria de cifras y letras. De este modo se crea una huella digital de dichos datos que permite bloquearlos en un sitio específico dentro de la cadena.

Hyperledger
Un proyecto paraguas creado por la Fundación Linux que incluye varias herramientas y sistemas para generar blockchains de código abierto.

Nodo
Una copia del registro que está manejado por un participante de la red blockchain.

Oráculo
Un puente desde una cadena de bloques a una fuente externa de datos que permite que un *smart contract* realice su actividad mediante el envío puntual de información. Un oráculo hace posible, por ejemplo, que un *smart contract* acceda a los consumos de energía de un consumidor, a horarios de trenes en tiempo real, a resultados electorales, etc.

Peer-to-peer (P2P)
El intercambio directo de datos entre nodos de una red, en contraposición al que se realiza a través de un servidor central.

Registro con permisos
Una red amplia y distribuida que utiliza un *token* nativo y que restringe el acceso únicamente a aquellos que tengan unas funciones específicas.

Blockchain privada
Una red controlada de forma privada, operada por un consorcio, en la que los datos son confidenciales y a la que únicamente acceden miembros de confianza. Las blockchains privadas no requieren un *token*.