Glosario

Rocío Mena

June 18, 2024

1 Glosario

Blockchain es una estructura de datos distribuida que mantiene un registro inmutable de transacciones o eventos mediante técnicas criptográficas que protegen contra la manipulación. La información se organiza en transacciones que son validadas y agrupadas en bloques. Cada bloque, junto con un puntero al bloque anterior, forma una cadena de transacciones interconectadas. Una vez que una transacción se ha añadido a la cadena, generalmente no puede ser modificada ni eliminada porque requeriría cambiar todos los bloques posteriores en la cadena, lo cual es computacionalmente impracticable debido a la distribución y la seguridad criptográfica de la red blockchain [RCB18].

Distributed ledger technology (DLT) : un ledger es un libro mayor o registro contable que registra todas las transacciones realizadas dentro de un sistema. El término DLT se suele utilizar como sinónimo de Blockchain y se refiere a la base de datos distribuida donde se almacenan todas las transacciones [RCB18].

Mecanismo de Consenso es un protocolo utilizado en redes distribuidas, como una blockchain, que permite a los nodos de la red llegar a un acuerdo sobre el estado actual del sistema o sobre qué transacciones son válidas y deben ser agregadas al ledger. El objetivo principal de un mecanismo de consenso es asegurar que todos los participantes de la red lleguen a un consenso o acuerdo sobre la verdad de los datos, incluso cuando algunos participantes puedan ser deshonestos o intenten manipular la red. Un mecanismo de consenso eficaz debe ser seguro, resistente a la censura, tolerante a fallas y verificable en tiempo real [DTF22].

Proof of Work (PoW) es un mecanismo de consenso donde los participantes, conocidos como mineros, compiten entre sí para resolver problemas criptográficos complejos y validar transacciones. Este proceso requiere una gran cantidad de poder computacional y consume mucha energía para encontrar la solución correcta primero. Una vez que un minero encuentra la solución, la cadena de bloques la verifica y el bloque con su solución

se agrega a la cadena, lo que garantiza que el trabajo realizado sea genuino. El sistema de PoW es seguro debido a la dificultad computacional requerida para alterar la cadena de bloques, mientras que es verificable en tiempo real y no requiere confianza entre los participantes [RCB18].

Proof of Stake (PoS) es un mecanismo de consenso donde la cantidad de criptomonedas que un participante posee y decide "bloquear" o "apostar" determina sus posibilidades de ser elegido para validar transacciones y crear nuevos bloques. Este proceso elimina la necesidad de la competencia intensiva en recursos y el consumo de energía asociado con la PoW, ya que no se requiere resolver problemas criptográficos complejos. Los participantes con más monedas (stake) en juego tienen más probabilidades de ser seleccionados para validar transacciones, y si se descubre que están actuando de manera fraudulenta, pueden perder parte o la totalidad de sus criptomonedas apostadas [RCB18].

Proof of Authority (PoA) es un mecanismo de consenso donde la validez de las transacciones son validadas por un conjunto predeterminado de autoridades o validadores reconocidos dentro de la red. Estos validadores son elegidos por su reputación, credibilidad o posición dentro de un entorno permisionado o consorcio blockchain. PoA no requiere grandes recursos computacionales ni participación económica significativa. Las transacciones son confirmadas y agregadas al blockchain cuando son validadas por una mayoría o número predefinido de estas autoridades.

Token en el contexto de Blockchain, es una unidad de valor que representa un activo digital y está asociado a una plataforma blockchain en particular. Se suele utilizar como sinónimos de criptomoneda. Los tokens se pueden intercambiar, transferir, almacenar y utilizar en todas las aplicaciones construidas sobre una blockchain. Los tokens pueden ser fungibles o no fungibles, dependiendo de si son intercambiables o únicos.