



GLOSARIO DE TÉRMINOS

CUALIFICACIÓN PROFESIONAL: IFC789_3

Código: IFC789_3

NIVEL: 3

Antivirus: Tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus de un ordenador.

Backend: Sistema que ofrece un servicio remoto que puede ser accedido desde sistemas cliente o "frontend".

Blockchain: DLT que se implementa como una lista o cadena de bloques que se almacena en red de manera distribuida para registrar transacciones, eventos o sucesos de manera segura e irrefutable mediante el uso de la criptografía y de un algoritmo de consenso.

Cifrado: Encriptado. Conversión de información de un formato legible a un formato codificado. La información cifrada solo se puede comprender y procesar tras el descifrado (desencriptado).

Clave privada: Una de las dos claves que genera un procedimiento de criptografía asimétrica. La clave privada y la pública están matemáticamente relacionadas. La clave pública se genera siempre a partir de la clave privada. La clave pública puede ser difundida por su propietario para ser usada por terceros. Estos terceros pueden usar la clave pública del propietario para cifrar mensajes que solo el propietario de la clave pública podrá leer usando su clave privada.

Contrato inteligente: ("Smart Contract"). Contrato que se ejecuta por sí mismo sin que intermedien terceros y se escribe como un programa informático en lugar de utilizar un documento impreso con lenguaje legal.

Control de acceso: El control de acceso es una forma de limitar el acceso a un sistema o a recursos físicos o virtuales. En seguridad informática es el proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a los sistemas, recursos o información. En el contexto de los sistemas de seguridad físicos, el control de acceso lo constituyen son los mecanismos y dispositivos que permiten autorizar o denegar el acceso físicamente a personas o vehículos a un recinto.

Cortafuegos: (Firewall). Sistema que protege redes y terminales privadas de accesos no autorizados, especialmente durante la navegación por internet.

Criptomoneda: También criptodivisa. Es un tipo de moneda digital que utiliza la criptografía para proporcionar un sistema de pagos seguro.

Depuración (de software): Proceso de eliminar errores durante el desarrollo y mantenimiento de un "software" a partir de la corrección de su código fuente.

Despliegue (de software): Procesos utilizados para instalar paquetes de software o aplicaciones en dispositivos técnicos. Suele conllevar la instalación inicial, la configuración y el mantenimiento de múltiples aplicaciones de software en varios dispositivos de forma rápida, automatizada, cómoda y sin errores.

DLT: ("Distributed Ledger Technology". En español, Tecnología de Libro Mayor Distribuido). Base de datos que gestionan varios participantes y no está centralizada. En dicha base se registran activos y se graban en múltiples ubicaciones. Cada nodo procesa y verifica cada elemento y crea un consenso sobre su veracidad. Blockchain es un tipo de DLT.

Dominio (web): Nombre único y exclusivo que se le da a un sitio web en Internet para que cualquiera pueda visitarlo.

Entorno de desarrollo integrado: (IDE, "Integrated Development Environment"). Conjunto de procedimientos y herramientas que se utilizan para desarrollar un código fuente o programa. herramienta de desarrollo de software utilizado para escribir, generar, probar y depurar un programa.

Evento (software): Notificación automática que ha habido algún tipo de acción y que suele disparar una acción o conjunto de acciones que, a su vez, pueden dar como resultado un evento en particular o una serie de eventos.

Experiencia de usuario: (UX, User Experience). Factores y elementos relativos a la interacción del usuario, con un entorno o dispositivo concretos, cuyo resultado es la generación de una percepción positiva o negativa de dicho servicio, producto o dispositivo.

Fork (desarrollo de software): También Branch. En español, rama o bifurcación. En desarrollo de "software", sucede cuando los desarrolladores toman una copia del código fuente desde un paquete "software" e inician un desarrollo independiente sobre él, creando un trozo de "software" distinto y separado.

Framework: Marco o esquema de trabajo generalmente utilizado por programadores para realizar el desarrollo de "software". Utilizar un "framework" permite agilizar los procesos de desarrollo ya que evita tener que escribir código de forma repetitiva, asegura unas buenas prácticas y la consistencia del código.

Frontend: Parte de la página "web" o aplicación con la que interaccionan los usuarios de la misma. Comprende todo el código que se ejecuta en el equipo de un usuario, al que se le denomina cliente.

Grafo: Tipo abstracto de datos (TAD), que consiste en un conjunto de nodos (también llamados vértices) y un conjunto de arcos (aristas) que establecen relaciones entre los nodos.

Herramienta de depuración: Herramienta de desarrollo especializada que se asocia a la aplicación en ejecución y permite inspeccionar el código y detectar y corregir errores.

Host: (En español, anfitrión). Computadoras u otros dispositivos (tabletas, móviles, portátiles) conectados a una red que proveen y utilizan servicios de ella. Los servidores deben utilizar anfitriones para tener acceso a la red y pueden, a su vez, pedir los mismos servicios a otras máquinas conectadas a la red. Los anfitriones son, por tanto, dispositivos monousuario o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores web, etc.

Hosting: Servicio de alojamiento en línea que permite publicar un sitio o aplicación web en Internet y que sea accedida desde máquinas o dispositivos cliente.

IDE: (IDE, "Integrated Development Environment". En español, Entorno de Desarrollo Integrado). Conjunto de procedimientos y herramientas que se utilizan para

desarrollar un código fuente o programa. herramienta de desarrollo de software utilizado para escribir, generar, probar y depurar un programa.

Interfaz: Conexión física y funcional que se establece entre dos aparatos, programas, dispositivos o sistemas que funcionan independientemente uno del otro o entre persona y máquina (interfaz de usuario).

Monedero (virtual): Wallet. También monederos de criptomonedas (u otros activos). Pieza de "software" o de "hardware" con los que realizar las operaciones de recepción y envío a través de la red DLT de cada activo.

Monedero frío: ("Cold Wallet"). Son monederos o carteras digitales donde puedes almacenar y gestionar activos como criptomonedas y que utilizan claves generadas por una fuente que no está conectada a la blockchain y por tanto, tampoco a Internet.

Monitorización: Acción realizada por elementos físicos y software que registran la situación en que están cada uno de los aspectos que se desean controlar.

NFT: ("Non Fungible Token". En español, token no fungible). Activo que es único, no se puede modificar y no se puede intercambiar por otro de igual valor, porque no existiría uno igual. Estos activos son, además, digitales, es decir, que no tienen correlación en el mundo físico.

Nodo (de red): Punto de conexión que puede recibir, crear, almacenar o enviar datos a lo largo de rutas de red distribuidas. Cada nodo de la red, ya sea un punto final para la transmisión de datos o un punto de redistribución, tiene una capacidad programada o diseñada para reconocer, procesar y reenviar transmisiones a otros nodos de la red.

Non Fungible Token: (NFT. En español, token no fungible). Activo que es único, no se puede modificar y no se puede intercambiar por otro de igual valor, porque no existiría uno igual. Estos activos son, además, digitales, es decir, que no tienen correlación en el mundo físico.

Nube: Uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software.

Online: En español "en línea". Estado activo de conectividad en Internet.

Oráculo (blockchain): Servicio mediante el cual una "blockchain" o un "smart contract" se nutre de información externa a la "blockchain" sobre la que se ejecuta.

Proof of Authority: (PoA. En español, prueba de autoridad). Algoritmo de consenso en DLT en el que todos los participantes involucrados son entidades conocidas, lo que obliga a ser aceptado para participar en ellas (también llamadas "permisionadas"). Cada participante en la operación la firma con su certificado digital.

Proof of Stake: (PoS). Algoritmo de consenso en DLT en el que el validador de un bloque depende de la inversión de ese validador en la red. Se basa en la idea de que cuanto más se tiene invertido en la red (y por tanto más se puede perder) te vuelves más fiable validando transacciones.

Proof of Work: (PoW). Algoritmo de consenso en DLT en el que cualquier propuesta de estado del registro llega con el resultado de un cálculo complejo de que requiere

mucha potencia de cálculo. La verificación del cálculo es, sin embargo, bastante rápida y sencilla por lo que no resulta rentable enviar un estado falso. Típicamente usa hash para implementar esa operación. El estado (que se trabaja por bloques de transacciones) tiene una referencia al estado anterior y el resultado del cálculo de su hash, por lo que todo está enlazado y no es posible cambiar un bloque del pasado sin cambiar todos los siguientes.

Registro log: Archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

Remote Procedure Call: ("RPC, Remote Procedure Call". En español, Llamada a Procedimiento Remoto). Mecanismo síncrono que transfiere el flujo de control y los datos entre dos espacios de direcciones a través de una red. Tecnología que regula la comunicación entre procesos, es decir, el intercambio de información entre procesos de sistema y consta del envío de parámetros y el retorno de un valor de función.

RPC: ("Remote Procedure Call". En español, Llamada a Procedimiento Remoto). Mecanismo síncrono que transfiere el flujo de control y los datos entre dos espacios de direcciones a través de una red. Tecnología que regula la comunicación entre procesos, es decir, el intercambio de información entre procesos de sistema y consta del envío de parámetros y el retorno de un valor de función.

Simplified Payment Verification: (SPV. En español, Verificación de Pago Simple). Sistema reseñado en el Whitepaper original de Bitcoin que permite a clientes ligeros (monederos ejecutándose en sistemas "low-end") verificar que una transacción ha sido incluida en el sistema y, por tanto, que la transacción se ha producido.

Smart Contract: En español, Contrato Inteligente. Contrato que se ejecuta por sí mismo sin que intermedien terceros y se escribe como un programa informático en lugar de utilizar un documento impreso con lenguaje legal.

SPV: (Simplified Payment Verification. En español, Verificación de Pago Simple). Sistema reseñado en el Whitepaper original de Bitcoin que permite a clientes ligeros (monederos ejecutándose en sistemas "low-end") verificar que una transacción ha sido incluida en el sistema y, por tanto, que la transacción se ha producido.

Tipo (algoritmo) de consenso: Mecanismo digital que consigue asegurar que el registro de una transacción en una DLT sea válido de manera irrefutable. Tipos de consenso son Proof of Work (PoW), Proof of Authority (PoA) y Proof of Stake (PoS), entre otros.

Transacción (informática): Interacción con una estructura de datos compleja, compuesta por varios procesos que se han de aplicar uno después del otro.

URL: (Uniform Resource Locator. En español, Localizador de Recursos Uniforme). En la www, identificador de un recurso específico disponible mediante un nombre de dominio y/o subdominios y un tipo de dominio a los que se puede añadir una ruta al recurso dentro del servidor.



UX: (User Experience. En español, experiencia de usuario). Factores y elementos relativos a la interacción del usuario, con un entorno o dispositivo concretos, cuyo resultado es la generación de una percepción positiva o negativa de dicho servicio, producto o dispositivo.

Wallet (blockchain): Monederos de criptomonedas u otros activos. Pieza de "software" o de "hardware" con los que realizar las operaciones de recepción y envío a través de la red DLT de cada activo.