COLOMBIA POTENCIA DE LA VIDA

TIC

Características de una blockchain, **descentralización y distribución**

Lección 3

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Tiempo de ejecución: 8 horas

PLANTEAMIENTO DE LA SESIÓN
En la tercera sesión se pondrá el foco en las principales características de blockchain y diferencias entre los sistemas centralizados y descentralizados, proponiendo un debate acerca de estos dos conceptos y desarrollando actividades grupales que permitan profundizar en sus diferencias.

Desarrollo teórico de la sesión: 4 horas

Características de una blockchain

La tecnología de blockchain o cadena de bloques se presenta como un sistema avanzado de bases de datos que facilita la transparencia en la compartición de información en entornos empresariales. En una base de datos de blockchain, la información se organiza en bloques interconectados formando una cadena. La consistencia cronológica de los datos se mantiene, ya que modificar o eliminar la cadena requiere consenso en la red. Este enfoque permite crear un registro inalterable para rastrear órdenes, pagos y otras transacciones, ofreciendo seguridad contra entradas no autorizadas y asegurando una visión coherente de las transacciones compartidas en la red.

Las bases de datos convencionales enfrentan desafíos al registrar transacciones financieras, como en la venta de una propiedad. En este escenario, la confiabilidad de las partes involucradas es incierta, generando riesgos legales. La presencia de una autoridad central para supervisar las transacciones complica el proceso y crea vulnerabilidades. La tecnología de blockchain aborda estos problemas al establecer un sistema descentralizado y seguro para registrar transacciones. En el caso de transacciones inmobiliarias, crea un libro mayor para comprador y vendedor, requiriendo aprobación de ambas partes y actualizándose en tiempo real. Cualquier alteración afecta todo el libro mayor, proporcionando seguridad. Estas características han impulsado su aplicación en diversos sectores, incluyendo la creación de criptomonedas como Bitcoin.

COLOMBIA POTENCIA DE LA VIDA

TIC

¿Cuáles son las características de la tecnología de blockchain?

Descentralización

Inmutabilidad

Consenso

Estas características definen la esencia de la tecnología de blockchain, asegurando transparencia, seguridad y participación consensuada en la red.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Consenso

Establece reglas para el consenso de los participantes en el registro de transacciones. Las nuevas transacciones solo se registran con el consentimiento mayoritario de los participantes de la red, es decir, con el voto del 51% o más para aprobar la transacción realizada.

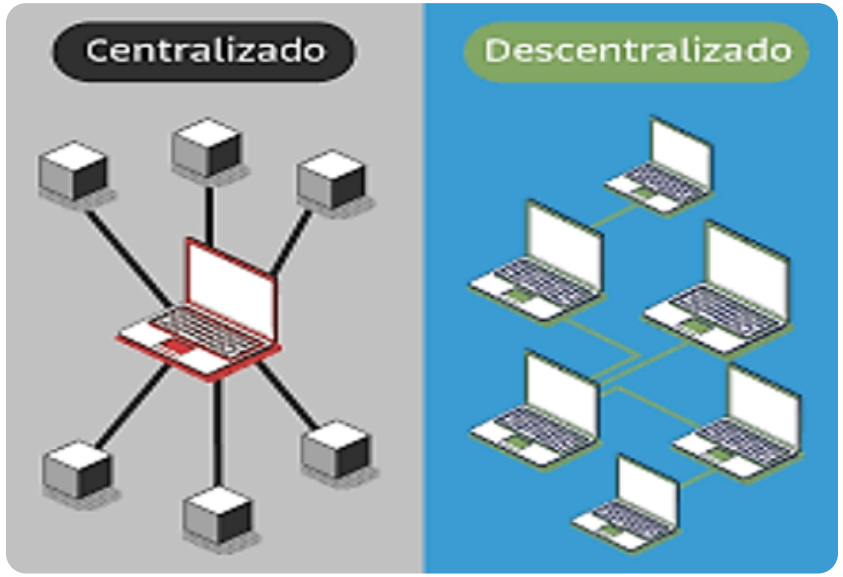
Estas características definen la esencia de la tecnología de blockchain, asegurando transparencia, seguridad y participación consensuada en la red.

Inmutabilidad

La inmutabilidad implica la incapacidad de cambiar o alterar registros una vez registrados en el libro mayor compartido. Cualquier error en una transacción requiere una nueva transacción para corregirlo, ambas siendo visibles para la red. Como se había comentado en lecciones anteriores, blockchain aplica métodos y tecnologías como el hash para identificar de manera única los registros que se realizan, este sistema permite detectar discrepancias en un archivo fácilmente y se puede negar la transacción o el registro en cuestión.

Descentralización

La descentralización traslada el control de una entidad central a una red distribuida. Reduce la necesidad de confianza entre participantes y evita la concentración de autoridad en la red. En este caso, los usuarios o participantes están al tanto de todos los bloques de registros en tiempo real para validar su veracidad y dar aprobación.



En el caso de los sistemas centralizados, la autoridad, la responsabilidad o el poder suelen caer en manos de una sola entidad, lo que da pie a varios inconvenientes, por ejemplo, la modificación de registros en una votación, una aplicación o plataforma que queda fuera de servicio porque su servidor central tuvo un fallo, etc.

Ahora que conocemos sus características más importantes, podemos hablar de sus componentes y arquitectura. La arquitectura de la cadena de bloques integra los siguientes componentes fundamentales:

Libro mayor distribuido

Criptografía de clave pública

Contratos inteligentes

Criptografía de clave pública

Proporciona seguridad e identificación única de participantes en la red de blockchain. Cada miembro posee una clave pública común y una clave privada única; estas claves se combinan para desbloquear los datos del libro mayor, solamente se pueden desbloquear con dicha llave privada, intentarlo con fuerza bruta de cómputo es una tarea altamente demandante y que no daría un resultado satisfactorio.

Veamos un ejemplo de uso de la criptografía de clave pública: Carlos cifra una transacción con su clave privada, y Sara, utilizando su clave pública, puede verificar la transacción, asegurando la integridad de la información, de esta forma se valida que la cadena es auténtica y queda grabada en el registro, si Carlos luego intenta modificar el valor de su transacción, se podrá ver en el libro de registros.

Contratos inteligentes

Permiten la autoadministración de contratos comerciales sin intermediarios, siendo programas ejecutados automáticamente en la blockchain. Por ejemplo, imaginemos un contrato inteligente en el sector inmobiliario que libera automáticamente el pago del depósito de alquiler a los propietarios una vez que los inquilinos confirman la recepción de las llaves y la condición satisfactoria del inmueble.

Libro mayor distribuido

Es la base de datos compartida que almacena transacciones, similar a un archivo editable por todos los participantes. Impone reglas estrictas sobre edición y previene la eliminación de entradas una vez registradas. No es posible alterar o eliminar un registro con un hash que ya ha sido ingresado en el libro, en el caso de que alguno de los participantes altere o borre uno de los registros, basta con que los demás participantes comparen para notar las discrepancias en la cantidad total de registros del libro o en las diferencias de los hashes.

Estos componentes son esenciales para la operatividad y seguridad de la tecnología de blockchain, facilitando transparencia y confianza en las transacciones, ya que los participantes votan y verifican por sí mismos los registros en el libro mayor de distribución y no dependen de una entidad externa con el poder de modificar o alterar las transacciones que ya se han realizado.

En conclusión, el funcionamiento general de una blockchain se puede definir en cuatro pasos ordenados: Registrar la transacción realizada, conseguir el consenso de la mayoría de los participantes, vincular el bloque con los registros en el libro mayor con su respectiva función hash, y por último se comparte el libro mayor con el nuevo registro a los demás participantes para que todos tengan una copia.