

Módulo 2
Unidad 1

LECCIÓN 1
Generalidades de la
tecnología blockchain

Desarrollo de la sesión:

Blockchain es una tecnología que almacena datos inmutables y con registro de tiempo. Estas dos características la hacen útil en muchas aplicaciones en donde se requiere tener la trazabilidad de las operaciones y la confianza de que no hay posibilidad de fraudes de por medio.



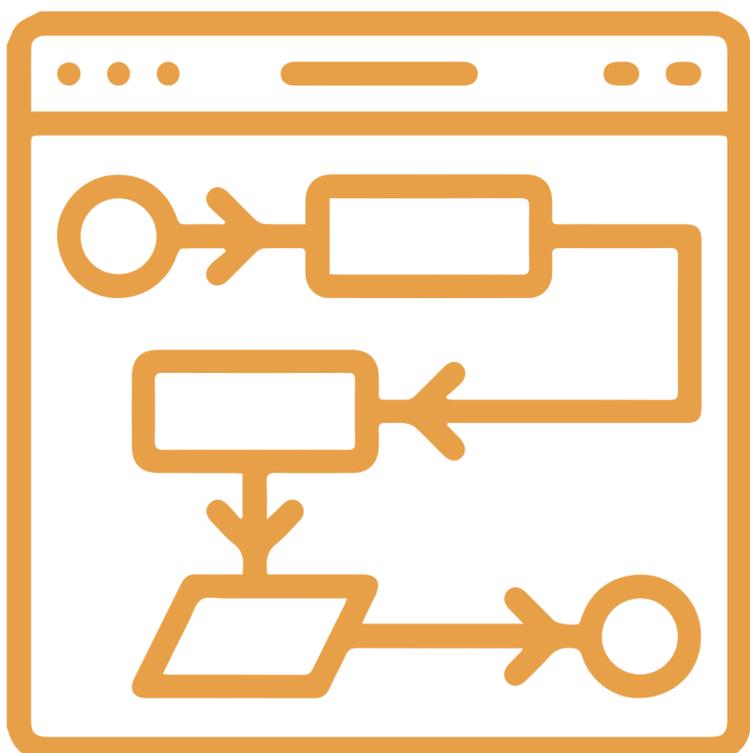
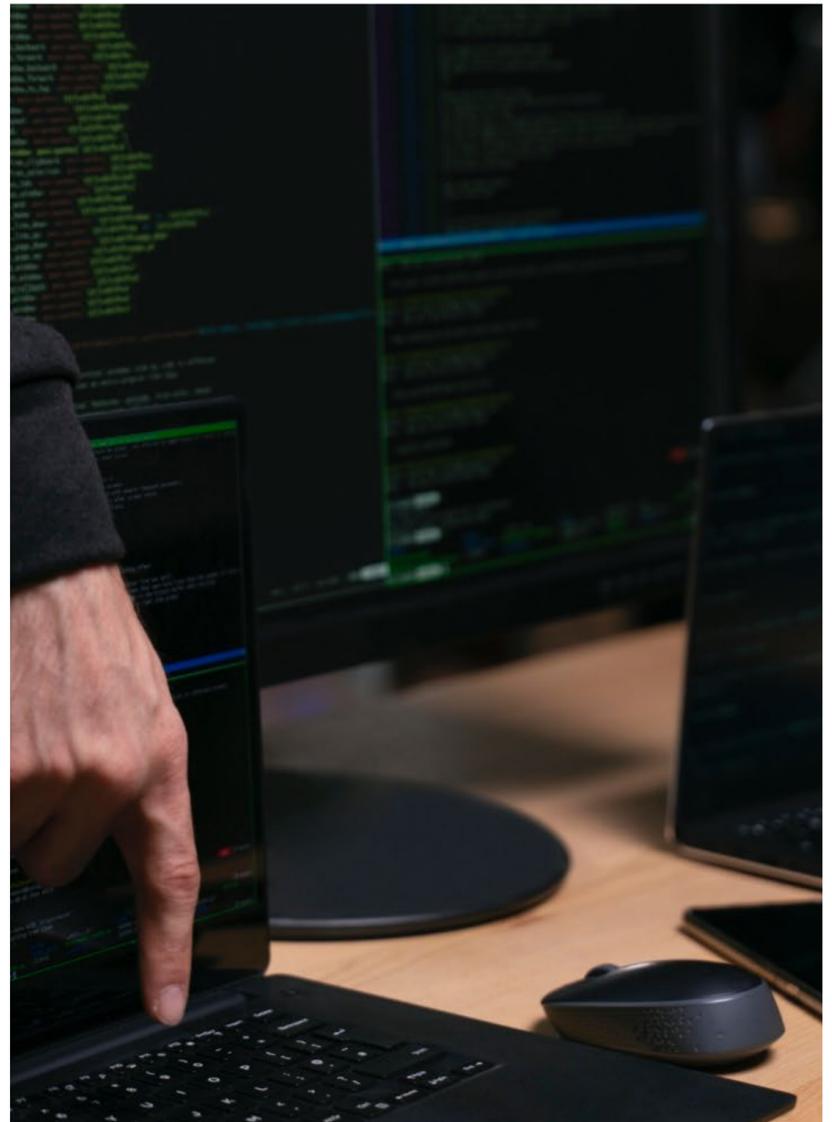
La propuesta permitía poner un sello digital a los documentos que evitaba los cambios y la falsificación en la fecha de firma. Para esto se empleaba una cadena de bloques que almacenaba los documentos con su sello de fecha y que era consultada cuando se necesitaba validar la autenticidad del documento. Si tenía modificaciones, la función de hash entregaba un número diferente, con lo que se validaba la originalidad.

Como se vio en la fase 1, para que blockChain pudiera existir, requería de técnicas de criptografía avanzadas, que salvaguardaran la identidad de los bloques en cadena y de las operaciones. Una de las primeras apariciones de la cadena de bloques fue en 1989 cuando científicos en Bellcore (Haber y Stornetta) emplearon criptografía de clave pública y funciones de hashing para garantizar la integridad de un documento, su autenticidad y la confidencialidad. Este sistema podía certificar que un documento original no se había modificado mediante la certificación de la fecha en que se generaba el documento, o en la última modificación que el documento tenía.



En 1992 se incorporaron los árboles hash de Merkle al diseño del sistema de autenticidad de documentos. Con esta adición múltiples documentos se podían vincular en una única función de hash, haciendo el sistema de consulta mucho más eficiente. Una vez se guardaban todos los documentos que cupieran en un bloque, este se cerraba y se convertía en un bloque inmutable. Es decir, no se podía modificar.

En el año 1995 los científicos Haber y Stornetta fundaron la empresa Surety Technologies que puso en marcha una de las primeras plataformas de Bloch chain, la cual consistía en ofrecer servicios de sellado comercial de documentos.



Posteriormente, la NSA (agencia de seguridad de Estados Unidos) publicó una investigación en la que documentaba cómo era posible mantener una criptomoneda. En donde se aportó información sobre la descentralización y el sistema de protección del anonimato. A esta moneda se le llamó B-money, sin embargo, nunca se implementó debido a que no existían plataformas que cumplieran todos los requerimientos para su funcionamiento. Uno de los problemas de la implementación de B-money es que cualquier usuario podía realizar un doble gasto, es decir, con una misma unidad monetaria podía pagar varias veces.

En 2015 surgió una adición a las plataformas que empleaban criptomonedas, que permitía a programas basados en block chain extenderse a otras aplicaciones. Vitalik Buterin desarrolló y lanzó al mercado una plataforma que agregaba el concepto de contratos inteligentes, Ethereum.

En Ethereum un contrato inteligente es cualquier acción que puede programarse para ser ejecutada en la cadena de bloques. Ethereum también emplea algoritmos de consenso distintos a los que tiene bitcoin.



Gracias a la confianza que estas plataformas generaron y la masificación que tuvieron, creció el interés y el uso de algoritmos basados en cadenas de bloques, con lo que surgieron más plataformas que permiten realizar muchas tareas. La mayoría nacen con un enfoque de criptomonedas, pero pueden ser extendidas a otros ámbitos. Dentro de las plataformas se cuenta con

Stellar

Es una plataforma de código abierto, descentralizada, enfocada en transacciones transfronterizas. Uno de los problemas que stellar resuelve es la reducción de costos de operación en comparación con Ethereum.

Stellar mantiene una base de datos descentralizada y de código abierto, con lo que cualquier persona puede revisar las implementaciones y los algoritmos que se están ejecutando para garantizar transparencia en cómo funciona.

Otra ventaja de stellar es que tiene una velocidad de confirmación rápida, una transacción puede tardar entre 3 y 5 segundos gracias al mecanismo de consenso SCP (stellar consensus protocol). Su enfoque es la velocidad, ofrecer un bajo costo y ser eficiente energéticamente en comparación con otras plataformas de block chain. En stellar también es posible tener contratos inteligentes y firmas digitales.

Esta plataforma permite desarrollar aplicaciones sobre su ecosistema soroban, el cual tiene algunas experiencias de aprendizaje gamificadas como <https://quest.stellar.org/learn> que permiten a usuarios y desarrolladores entrar en contacto con la tecnología a través de juegos.



Al ser una plataforma orientada a las transacciones económicas, sus usos mas comunes son como base para empresas de pagos y giros internacionales. Sin embargo también hay usos para stellar como

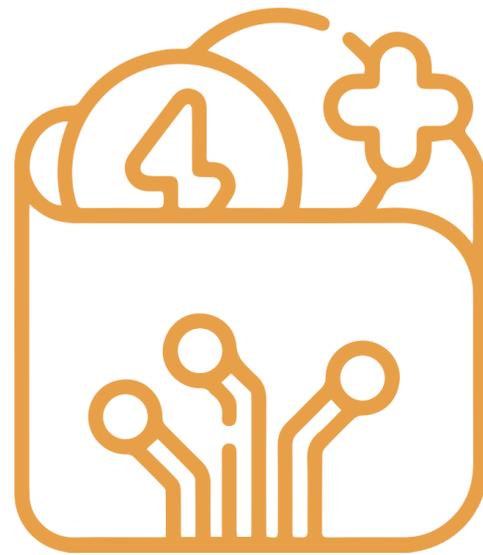
Tokanización de coleccionables: Stellar permite tokenizar elementos tanto físicos como virtuales. Esto permite que tales elementos se comercialicen con la premisa de que se conocen todos los movimientos de cada token desde su origen.

La tokenización no solamente sirve para coleccionables sino para bienes digitales como pueden ser documentos, lo que permite que un propietario asegure sus datos en blockchain, tenga trazabilidad de los cambios que estos tienen y pueda certificar su autenticidad.





Activos ancla: Uno de los componentes clave de stellar es que permite componentes que actúan como puentes entre diferentes monedas, permitiendo a los usuarios consignar y retirar dinero en su moneda local. Es decir, este componente permite manejar las tasas de cambio y que personas en diferentes países con diferentes monedas intercambien pagos.

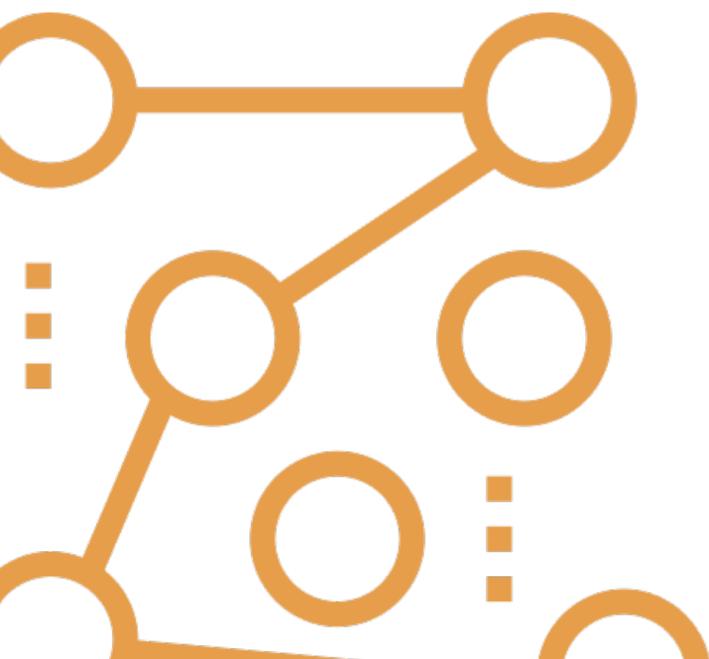


Servicios financieros

Billetera LOBSTR

La billetera LOBSTR es una billetera Stellar fácil de usar que facilita el envío, recepción y comercio de activos digitales. LOBSTR ofrece una forma segura y conveniente de gestionar tus activos Stellar.

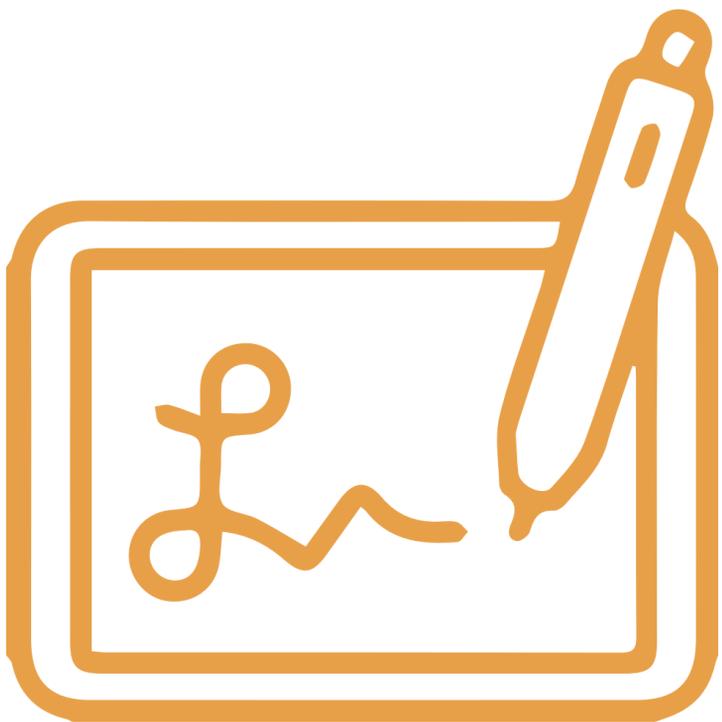
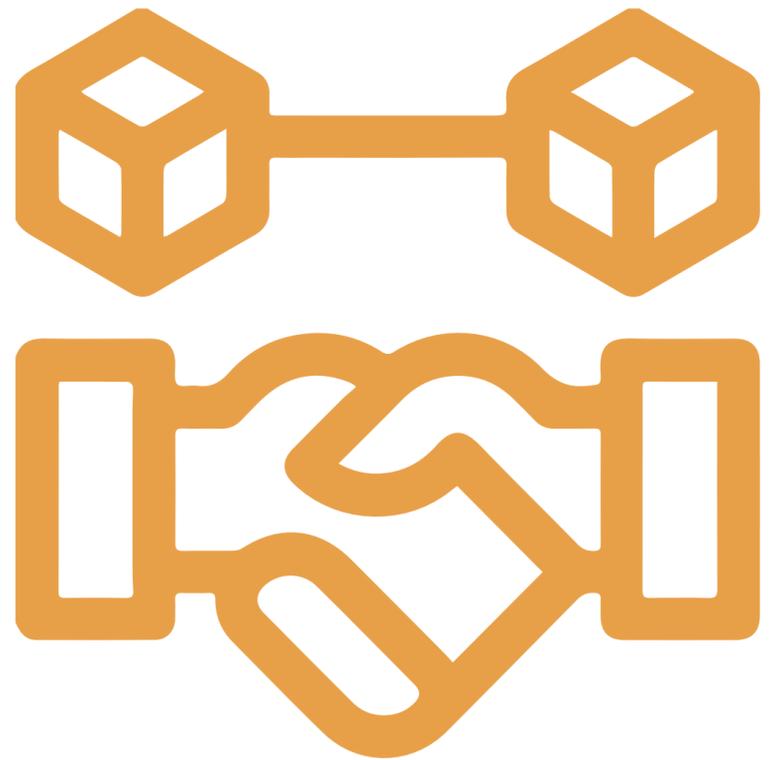
Ya seas un trader experimentado o un novato en blockchain, LOBSTR te cubre las espaldas. Soporta todos los tokens Stellar, permite transacciones rápidas y fáciles, y proporciona actualizaciones de saldo en tiempo real y un historial de transacciones.



Aplicación Bancaria Refuge

La red Stellar puede ser utilizada para construir aplicaciones bancarias para refugiados. Estas aplicaciones pueden proporcionar servicios financieros a quienes más los necesitan, ayudando a aliviar los desafíos que enfrentan las personas desplazadas.

Con una aplicación bancaria basada en Stellar, los refugiados pueden acceder a una plataforma segura y confiable para almacenar y gestionar su dinero. Pueden realizar y recibir pagos, acceder a créditos e incluso construir un historial financiero sin necesidad de una cuenta bancaria tradicional.



Contratos Inteligentes

El soporte de Stellar para contratos inteligentes simples abre posibilidades. Los contratos inteligentes son contratos autoejecutables con los términos de acuerdo escritos directamente en código.

Pueden automatizar diversos procesos, desde billeteras de múltiples firmas hasta pagos condicionales. Con los contratos inteligentes de Stellar, puedes crear transacciones seguras y automatizadas que se ejecutan cuando se cumplen ciertas condiciones.

Esto puede optimizar operaciones, reducir el riesgo de errores humanos y mejorar la transparencia y la responsabilidad.

Ethereum

Ethereum, lanzado en 2015 por Vitalik Buterin, es una plataforma blockchain que ha revolucionado la forma en que se desarrollan y ejecutan aplicaciones descentralizadas (DApps). Su innovación principal radica en la capacidad de ejecutar contratos inteligentes, código autónomo que ejecuta acciones cuando se cumplen ciertas condiciones predefinidas. Esto ha allanado el camino para una multitud de innovaciones en el mundo blockchain.

Contratos Inteligentes y DApps

Los contratos inteligentes en Ethereum son piezas de código que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Estos contratos pueden representar acuerdos financieros, lógica de negocio compleja o cualquier otro tipo de transacción que desee automatizarse y ejecutarse de forma segura y confiable en la blockchain.

- **Ejemplo de Contrato Inteligente:** Un contrato inteligente para un préstamo podría establecer automáticamente los términos del préstamo, verificar la identidad del prestatario y el prestamista, y liberar los fondos una vez que se cumplan las condiciones acordadas.

Las DApps son aplicaciones descentralizadas que se ejecutan en la blockchain de Ethereum. Estas aplicaciones aprovechan los contratos inteligentes para realizar transacciones y ejecutar lógica de aplicación de forma transparente y segura.

- **Ejemplo de DApp:** Un intercambio descentralizado (DEX) permite a los usuarios intercambiar criptomonedas sin necesidad de una autoridad centralizada. Los contratos inteligentes en la DApp gestionan automáticamente el emparejamiento de órdenes y la liquidación de transacciones.

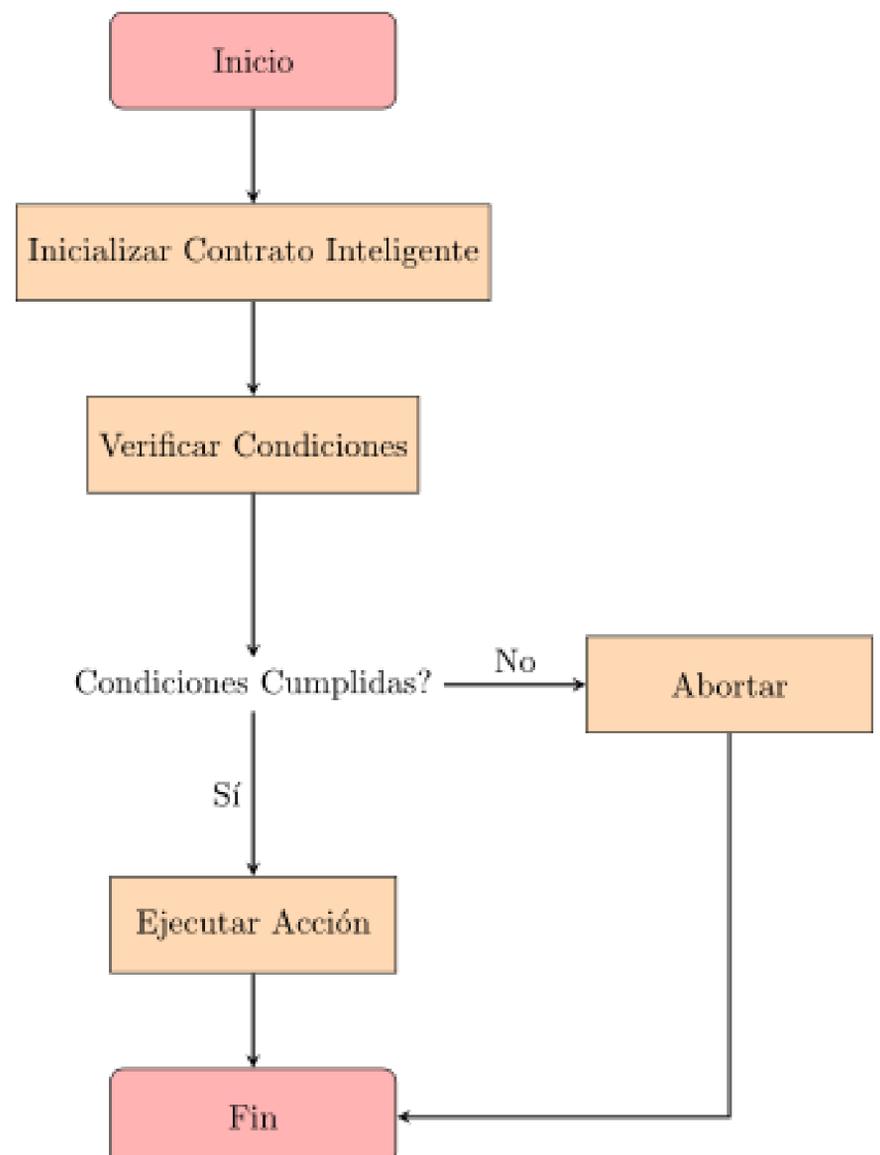
Impacto en el Sector Financiero

Ethereum ha tenido un profundo impacto en el sector financiero al permitir la creación de una amplia gama de servicios financieros descentralizados (DeFi). Estos incluyen préstamos, intercambios descentralizados (DEX), pools de liquidez, derivados financieros y más.

- **Ejemplo de DeFi:** Los protocolos de préstamos descentralizados como Compound o Aave permiten a los usuarios prestar y pedir prestado activos digitales sin la necesidad de intermediarios financieros tradicionales.

Además del sector financiero, Ethereum ha sido fundamental en el desarrollo de otras áreas, como

- **Juegos Descentralizados (DApps):** Los juegos basados en Ethereum permiten la propiedad descentralizada de activos virtuales y la interoperabilidad entre diferentes juegos.
- **Mercados Digitales:** Plataformas como OpenSea facilitan la compra, venta y intercambio de activos digitales únicos (NFTs) en la blockchain de Ethereum.



Algunos aspectos importantes se mencionan a continuación

Aspecto	Descripción
• Contratos Inteligentes	Automatización de acuerdos y transacciones mediante código autónomo.
• Aplicaciones Descentralizadas (DApps)	Aplicaciones que funcionan sin autoridad centralizada, ejecutadas en Ethereum.
• Finanzas Descentralizadas (DeFi)	Ecosistema financiero en Ethereum, sin intermediarios tradicionales.
• Interoperabilidad	Capacidad de Ethereum para comunicarse con otras blockchains.
• Escala y Rendimiento	Desafíos de crecimiento y eficiencia en el procesamiento de transacciones.
• Actualización a Ethereum 2.0	Transición a un protocolo más eficiente y escalable basado en la prueba de participación.

Binance Smart Chain

Binance Smart Chain (BSC) ha emergido como una opción destacada en el ecosistema blockchain, impulsada por su estrecha integración con la reconocida plataforma de intercambio de criptomonedas, Binance. Esta asociación estratégica ha sido fundamental para su rápida adopción y popularidad entre desarrolladores y usuarios por igual.



Integración con Binance y Acceso al Ecosistema

La estrecha integración con Binance ha sido un factor clave en la popularidad de Binance Smart Chain. Los usuarios de Binance pueden acceder fácilmente a BSC y viceversa, lo que facilita la transferencia de activos entre ambas plataformas. Además, la reputación y el respaldo de Binance han brindado una capa adicional de confianza y legitimidad a BSC, lo que ha atraído a una amplia audiencia de usuarios e inversores.

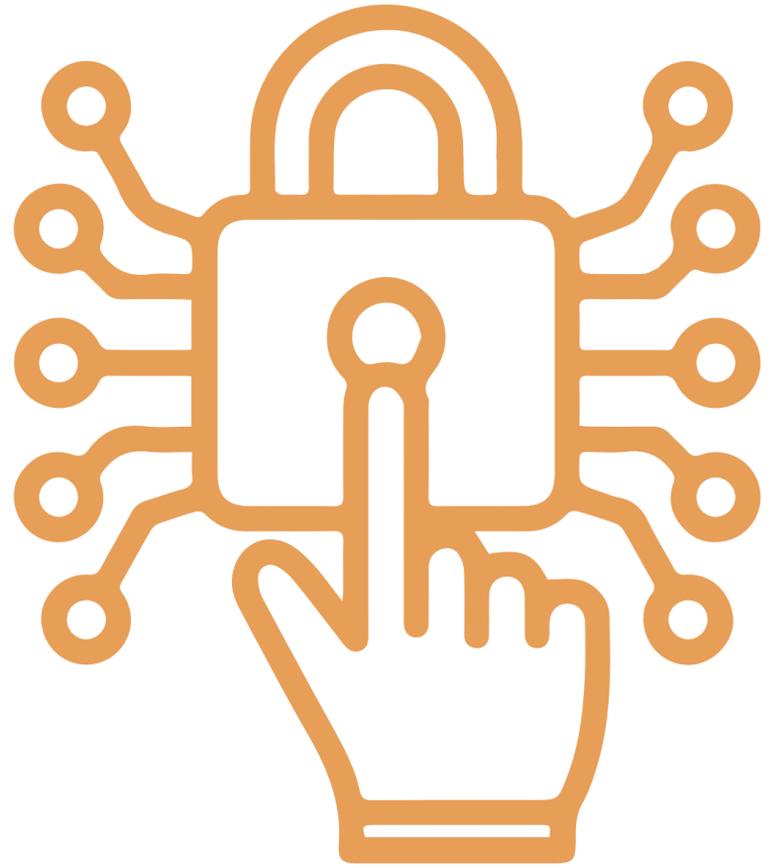
Enfoque en Transacciones Rápidas y Económicas

Una de las principales características que distingue a Binance Smart Chain es su enfoque en transacciones rápidas y económicas. Con tarifas de transacción significativamente más bajas en comparación con otras blockchains, BSC se ha convertido en una opción atractiva para aquellos que buscan minimizar los costos operativos y maximizar la eficiencia de sus transacciones. Además, la capacidad de BSC para manejar un gran volumen de transacciones por segundo garantiza una experiencia fluida y sin demoras para los usuarios.



Migración de DApps y Crecimiento del Ecosistema

La búsqueda de una escalabilidad mejorada y tarifas más económicas ha llevado a muchas aplicaciones descentralizadas (DApps) a migrar a Binance Smart Chain. Este éxodo de DApps ha sido un factor clave en el crecimiento explosivo del ecosistema de BSC. Ahora, BSC alberga una amplia variedad de aplicaciones, que van desde finanzas descentralizadas (DeFi) hasta juegos y tokens no fungibles (NFTs). Esta diversidad de aplicaciones ha contribuido a hacer de BSC un ecosistema vibrante y dinámico, con un potencial de desarrollo y crecimiento continuo.



Polkadot

Polkadot se destaca en el panorama blockchain por su enfoque en la interoperabilidad, una característica que revoluciona la forma en que las blockchains se comunican entre sí. Esta capacidad única de Polkadot permite una comunicación fluida y eficiente entre diferentes cadenas de bloques, lo que abre un abanico de posibilidades para una amplia variedad de aplicaciones en diversos sectores.



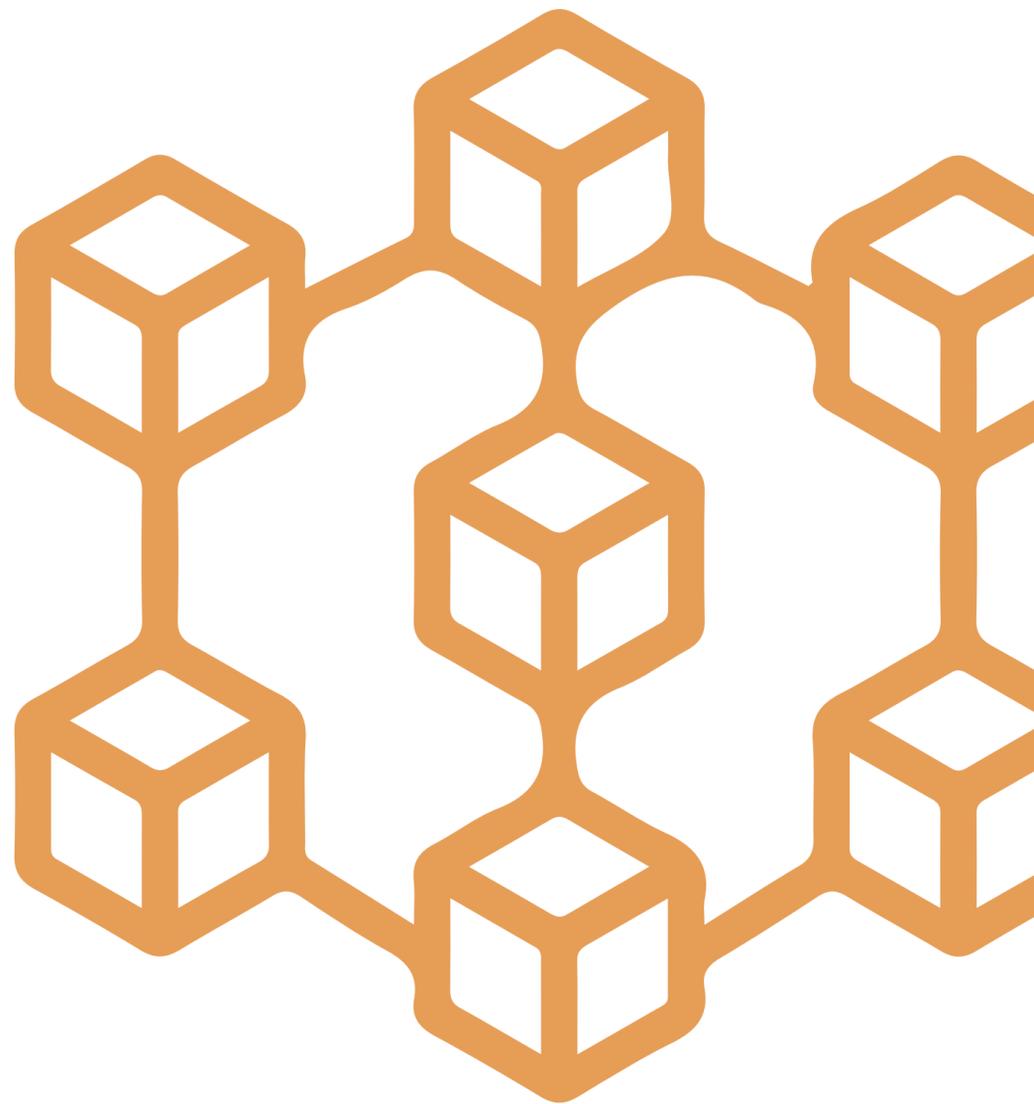


Interoperabilidad para la Comunicación entre Blockchains

La interoperabilidad es el corazón de Polkadot. Esta capacidad permite que las diferentes blockchains conectadas a la red de Polkadot se comuniquen entre sí de manera eficiente, compartiendo datos y activos de forma segura y transparente. Esta comunicación fluida abre nuevas oportunidades en sectores como la cadena de suministro, la gestión de activos digitales y la Internet descentralizada, donde la integración de múltiples fuentes de datos es esencial.

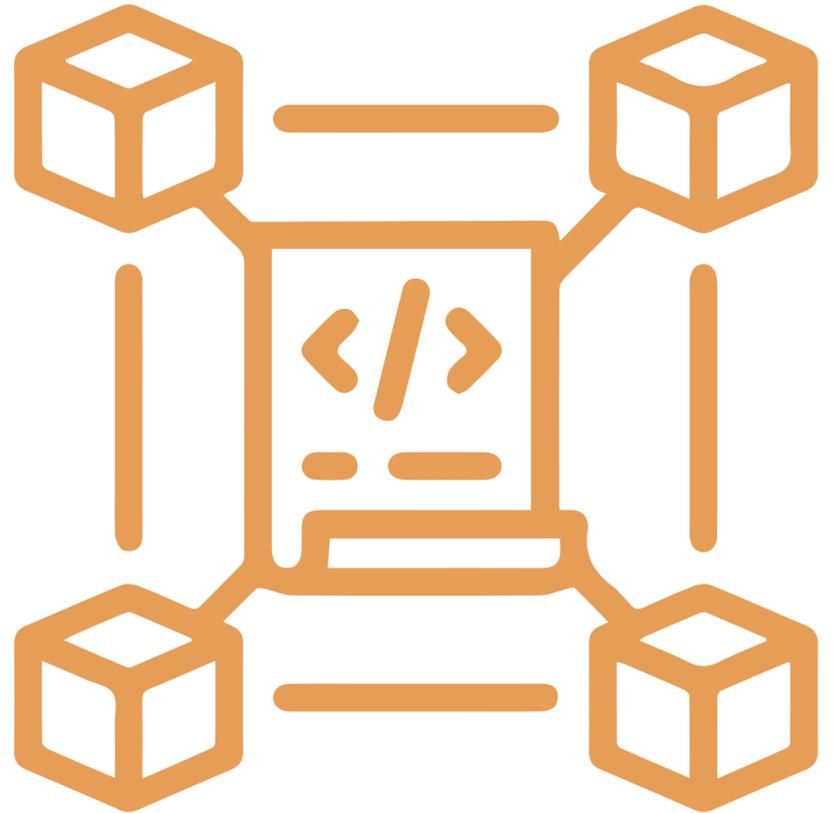
Arquitectura Modular para Flexibilidad y Adaptabilidad

La arquitectura modular de Polkadot es otro aspecto destacado de su diseño. Esto permite a los desarrolladores construir blockchains personalizadas que se ajusten a las necesidades específicas de sus aplicaciones, utilizando módulos predefinidos que se pueden ensamblar de acuerdo a los requisitos del proyecto. Esta flexibilidad y adaptabilidad hacen que Polkadot sea una opción atractiva para una amplia variedad de casos de uso, desde aplicaciones empresariales hasta proyectos de Internet descentralizada.



Conexión de Cadenas de Bloques Públicas y Privadas

Polkadot no solo conecta blockchains públicas entre sí, sino que también facilita la conexión con blockchains privadas. Esta capacidad promueve la colaboración y la interoperabilidad en todo el ecosistema blockchain, permitiendo que las organizaciones mantengan la privacidad y el control sobre sus datos mientras se benefician de la comunicación fluida con otras blockchains en la red de Polkadot. Esta combinación única de interoperabilidad pública y privada hace que Polkadot sea una plataforma versátil y poderosa para una amplia gama de aplicaciones y casos de uso.



Solana

Solana se ha posicionado como una de las blockchains líderes en velocidad y escalabilidad dentro del ecosistema blockchain. Su infraestructura única permite una capacidad excepcionalmente alta de procesamiento de transacciones por segundo, superando a muchas otras blockchains en este aspecto. Esta capacidad técnica ha llevado a Solana a ser reconocida como una opción ideal para una amplia gama de aplicaciones que requieren un alto rendimiento y velocidad.

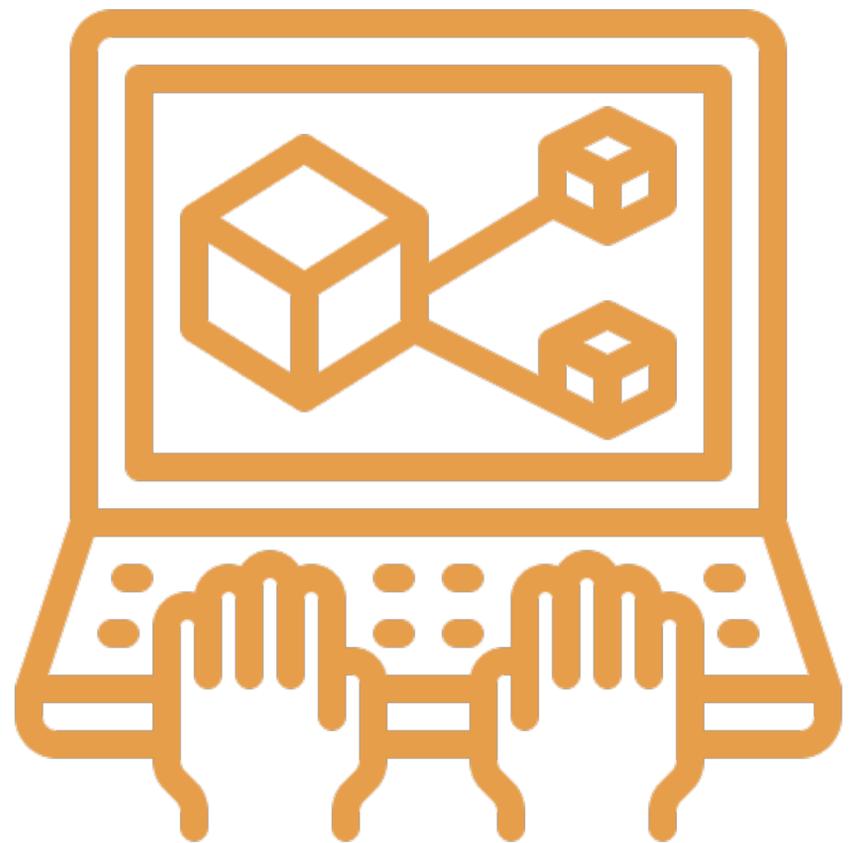


Infraestructura de Alta Velocidad

La infraestructura de Solana se destaca por su capacidad para manejar una mayor cantidad de transacciones por segundo en comparación con otras blockchains. Esta alta velocidad de procesamiento de transacciones la hace ideal para aplicaciones que necesitan respuestas rápidas y eficientes, como los mercados financieros de alta frecuencia, donde cada milisegundo cuenta, así como para juegos en línea y redes sociales descentralizadas que requieren interacciones instantáneas.

Enfoque en la Comunidad y Desarrollo

Además de su impresionante capacidad técnica, Solana ha demostrado un compromiso firme con la construcción de una comunidad activa y diversa de desarrolladores y usuarios. Este enfoque en la comunidad ha contribuido significativamente a su crecimiento y adopción en el espacio blockchain. Solana ha establecido programas de subvenciones, hackatones y otras iniciativas para fomentar la innovación y el desarrollo en su plataforma, atrayendo talento y proyectos de alta calidad.



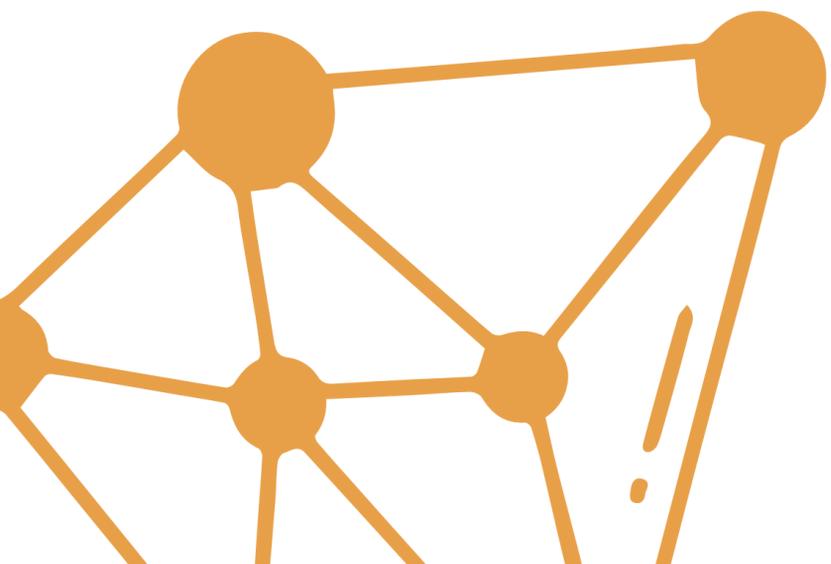
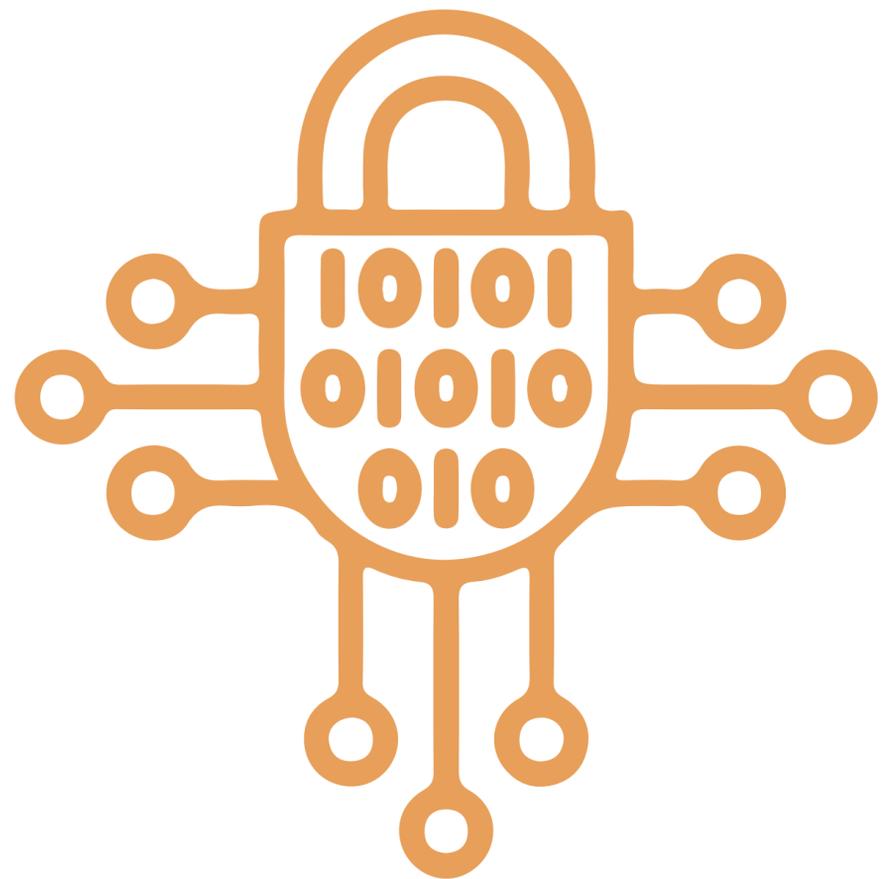


Integración con Binance y Acceso al Ecosistema

Solana ha visto una amplia variedad de casos de uso y aplicaciones desarrolladas en su plataforma. Además de los mercados financieros de alta frecuencia, los juegos en línea y las redes sociales descentralizadas mencionadas anteriormente, Solana se ha utilizado para aplicaciones como el comercio de activos digitales, finanzas descentralizadas (DeFi), almacenamiento de datos descentralizado y mucho más. Su capacidad para manejar un alto volumen de transacciones con baja latencia ha abierto nuevas posibilidades para la innovación en el espacio blockchain.

Cardano

Cardano se ha establecido como una blockchain que prioriza la seguridad, la sostenibilidad y la escalabilidad desde sus cimientos. Su enfoque en la investigación científica ha sentado las bases para altos estándares en términos de seguridad y eficiencia energética, lo que la distingue en el panorama blockchain.



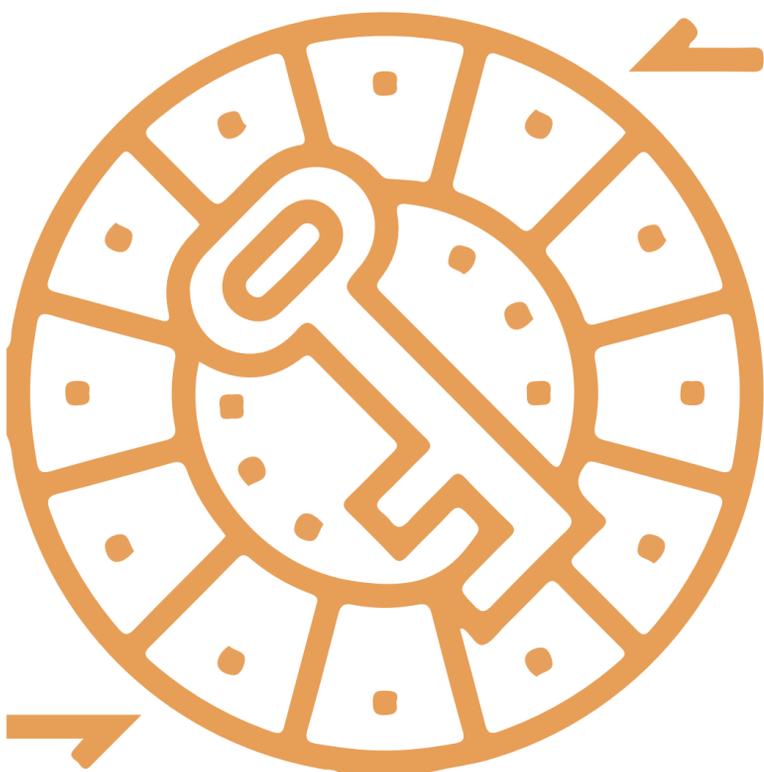
Enfoque en la Seguridad y la Eficiencia Energética

El diseño de Cardano se basa en un enfoque de investigación científica, lo que garantiza una arquitectura sólida y segura. Su protocolo de consenso basado en pruebas de participación (PoS) y su diseño modular se han desarrollado con la seguridad como prioridad, prometiendo una mayor resistencia a ataques maliciosos y una operación más confiable. Además, la eficiencia energética de Cardano la hace más sostenible y respetuosa con el medio ambiente en comparación con otras blockchains que utilizan métodos de consenso más intensivos en energía.



Promesa de Estabilidad y Confianza

Cardano se destaca por su protocolo de consenso basado en pruebas de participación, que ofrece una mayor seguridad y estabilidad en comparación con otras blockchains. Su diseño modular permite una mayor flexibilidad y adaptabilidad, lo que la hace adecuada para una variedad de aplicaciones, desde servicios financieros hasta sistemas de votación y gestión de activos digitales. Esta promesa de estabilidad y confianza la convierte en una opción atractiva para desarrolladores y usuarios que buscan una plataforma segura y confiable.



Sostenibilidad

El enfoque en la sostenibilidad es una característica distintiva de Cardano. Su diseño y protocolo están diseñados para garantizar que la red pueda crecer y evolucionar de manera sostenible a lo largo del tiempo. Esto asegura que Cardano pueda seguir siendo relevante y funcional en el futuro, adaptándose a las necesidades cambiantes del panorama blockchain y manteniendo su compromiso con la seguridad y la eficiencia energética.

