COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 1
Oráculos

Módulo 2 - Unidad 1

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

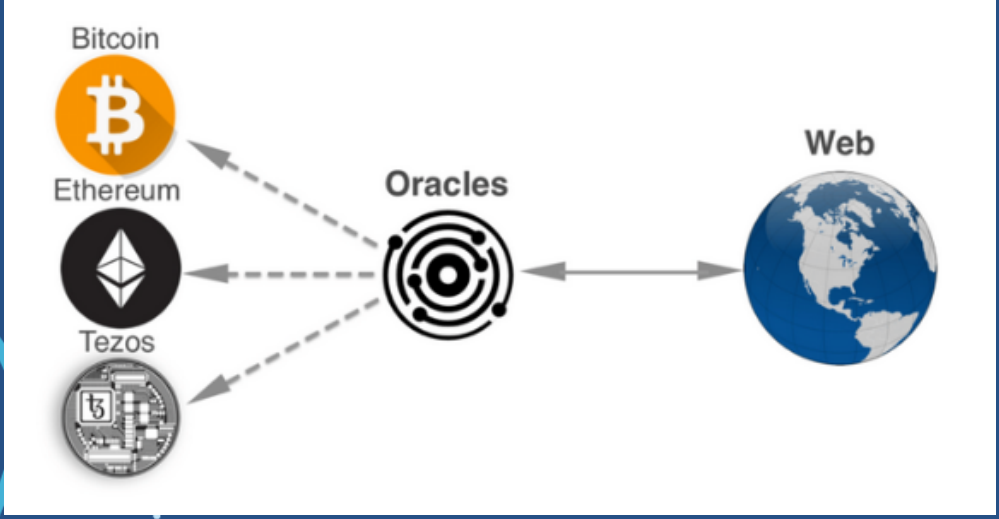
Universidad Tecnológica de Pereira

Desarrollo de la sesión:

Los oráculos desempeñan un papel crucial en el ecosistema de blockChain y las aplicaciones descentralizadas (dApps). Blockchain, como mencionaste, es una tecnología que almacena datos de manera inmutable y con registro de tiempo, proporcionando así transparencia y seguridad en las operaciones. Sin embargo, a pesar de su robustez, la cadena de bloques tiene limitaciones en cuanto a su capacidad para acceder a datos externos del mundo real.

En el contexto de blockChain, un oráculo actúa como un intermediario que permite a los contratos inteligentes, ejecutados en la cadena de bloques, interactuar con fuentes de datos externas, como información meteorológica, precios de acciones, resultados deportivos, entre otros. Esto es esencial para muchas aplicaciones que requieren datos actualizados y verificables para su funcionamiento, como los contratos financieros, los seguros basados en eventos, las apuestas y mucho más.

Históricamente, el concepto de oráculos ha evolucionado junto con el desarrollo de la tecnología blockChain. Desde los primeros días de la criptografía y las cadenas de bloques, como el trabajo pionero de Haber y Stornetta en la certificación de documentos, hasta la creación de Bitcoin por Satoshi Nakamoto en 2008, que introdujo la primera criptomoneda descentralizada y su infraestructura basada en blockChain, hemos visto cómo los oráculos se han convertido en una pieza fundamental para ampliar las capacidades de las dApps.

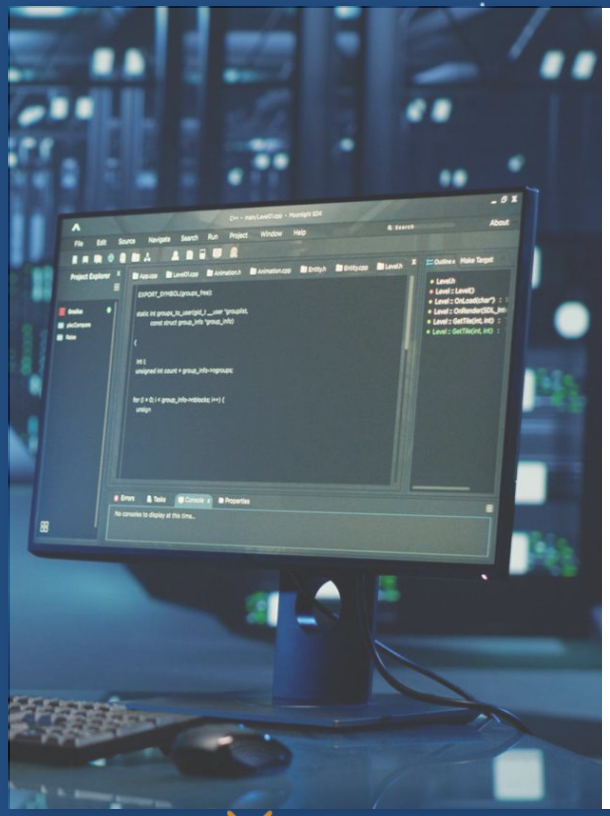


Con la llegada de Ethereum en 2015 y su introducción de contratos inteligentes, los oráculos adquirieron aún más importancia al permitir que estos contratos accedan a datos externos para su ejecución. Ethereum revolucionó el espacio blockChain al permitir la creación de dApps más complejas y versátiles, gracias a la capacidad de ejecutar código en la cadena de bloques.

Sin embargo, el uso de oráculos no está exento de desafíos y riesgos. La integridad y la confiabilidad de los datos externos son aspectos críticos a considerar, ya que cualquier manipulación o fallo en la fuente de datos puede comprometer la seguridad y la validez de los contratos inteligentes. Además, la descentralización y la resistencia a la censura, características fundamentales de blockChain, pueden verse comprometidas si se depende en exceso de un único oráculo centralizado.

En esta lección, se explorarán los diferentes tipos de oráculos, sus aplicaciones prácticas, los desafíos asociados y las mejores prácticas para su implementación y gestión en el contexto de las aplicaciones descentralizadas. Al comprender plenamente el papel y la importancia de los oráculos en el ecosistema blockChain, los participantes estarán mejor equipados para diseñar y desarrollar dApps seguras, confiables y eficientes.

Existen diversas plataformas donde pueden programarse oráculos, para su uso en aplicaciones descentralizadas(dApps) . Dentro de las plataformas más utilizadas para desarrollar oráculos se encuentran:



Ethereum

Ethereum es una de las plataformas blockChain más populares y ampliamente adoptadas para el desarrollo de dApps. Permite la creación de contratos inteligentes, que pueden incluir funcionalidades de oráculos para acceder a datos externos. Esta plataforma también puede ser utilizada para crear cualquier tecnología digital segura. Tiene un token diseñado para pagar el trabajo realizado apoyando el blockchain, donde los participantes también pueden utilizarlo para pagar bienes y servicios tangibles si se aceptan.
La plataforma Ethereum fue lanzada en 2015 por Buterin y Joe Lubin, fundador de la compañía de software blockchain ConsenSys.

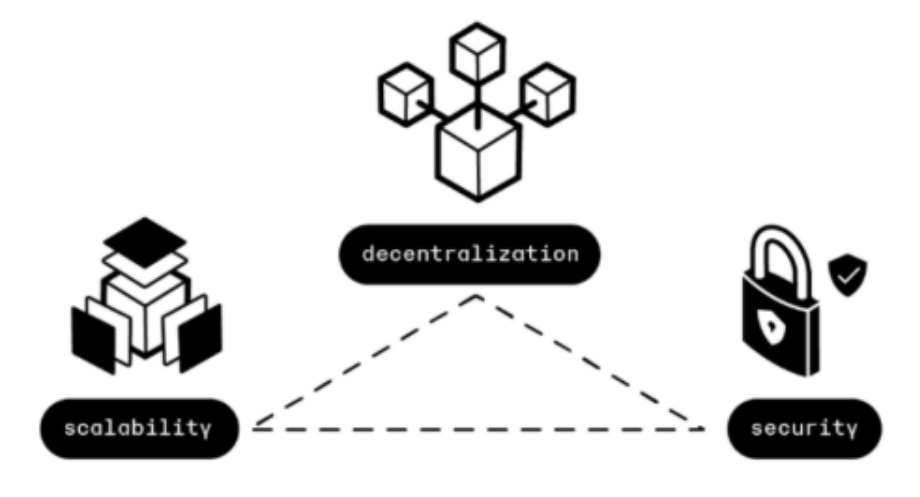
Propiedades de Ethereum

Ethereum se distingue por su naturaleza descentralizada, lo que implica que no está sujeto al control de ninguna entidad centralizada. A diferencia de la mayoría de los sistemas en línea, empresas y negocios que operan bajo una estructura centralizada de gobernanza, Ethereum funciona de manera autónoma y distribuida. Esta característica esencial garantiza que la red no tenga un punto único de fallo, ya que se ejecuta en miles de nodos en todo el mundo, lo que asegura su continuidad y resistencia a la censura. Además, esta descentralización protege la privacidad de los usuarios al mantener sus datos personales en sus propios dispositivos, mientras que el contenido, como aplicaciones y vídeos, permanece bajo el control directo de sus creadores, sin necesidad de obedecer las reglas impuestas por servicios de alojamiento centralizados como YouTube o App Store. La tecnología blockchain subyacente en Ethereum facilita la creación y mantenimiento de registros digitales seguros e inmutables.

Además de su naturaleza descentralizada, Ethereum tiene una serie de propiedades que lo convierten en un ecosistema versátil:

- **Smart Contracts (Contratos Inteligentes):** Ethereum introdujo los contratos inteligentes, que son protocolos informáticos que facilitan, verifican o hacen cumplir la negociación o el desempeño de un contrato, permitiendo así transacciones seguras y transparentes sin la necesidad de intermediarios.
- **EVM (Ethereum Virtual Machine - Máquina Virtual Ethereum):** La Máquina Virtual Ethereum es una plataforma de ejecución de contratos inteligentes que ejecuta el código exactamente como se ha programado, sin posibilidad de tiempo de inactividad, censura, fraude o interferencia de terceros.
- **Interoperabilidad:** Ethereum es compatible con múltiples tokens y protocolos, lo que facilita la interoperabilidad entre diferentes aplicaciones y redes, fomentando así la colaboración y la innovación.

- **Escalabilidad:** Aunque enfrenta desafíos de escalabilidad, Ethereum está en constante evolución para mejorar su rendimiento y capacidad de procesamiento de transacciones, con actualizaciones como Ethereum 2.0, que busca abordar estos problemas mediante la implementación de la prueba de participación (PoS) y fragmentación.



- **Comunidad y Desarrollo Activo:** Ethereum cuenta con una comunidad vibrante y comprometida de desarrolladores, investigadores, empresas y entusiastas que contribuyen al crecimiento y la expansión del ecosistema, a través de iniciativas como Ethereum Foundation, Ethereum Community Fund y Ethereum Enterprise Alliance.

Chainlink

Es una red descentralizada de oráculos que conecta blockChains con fuentes de datos externas del mundo real. Su principal objetivo es proporcionar una infraestructura segura y confiable para desarrollar y desplegar oráculos en una variedad de blockChains. Chainlink se basa en un enfoque descentralizado, utilizando una red de nodos oráculo distribuidos para recopilar, verificar y transmitir datos externos a la cadena de bloques. Esto garantiza la integridad y la confiabilidad de los datos utilizados por las aplicaciones blockChain. Además, Chainlink es compatible con múltiples blockChains y utiliza su token nativo LINK para incentivar la participación y la contribución en su ecosistema. En resumen, Chainlink proporciona una solución versátil y escalable para el acceso a datos externos en el ecosistema blockChain.

En 2014, Sergey Nazarov, con la visión de conectar el mundo real con las cadenas de bloques, fundó SmartContract.com, la empresa matriz de Chainlink. La idea era crear una red de oráculos descentralizada que proporcionara datos confiables y seguros a los contratos inteligentes.

El desarrollo de Chainlink cobró impulso en 2017 con la publicación del whitepaper y la exitosa ICO que recaudó $32 millones. Dos años después, en 2019, se lanzó la red principal de Chainlink, lo que marcó un hito crucial en su camino hacia la adopción masiva.

La integración con importantes proyectos de blockchain como Ethereum, Tezos y Hyperledger consolidó la posición de Chainlink como una solución líder para la integración de datos. En 2020, la red se expandió aún más al asociarse con la Red Nacional de Servicios Blockchain (BSN) de China y al lanzar Chainlink Verifiable Random Function (VRF), una herramienta fundamental para juegos y aplicaciones de lotería.

El crecimiento de Chainlink continuó en 2021 con el lanzamiento de Chainlink Keepers, un servicio de automatización descentralizado, y al alcanzar un valor total bloqueado (TVL) de $10 mil millones. La integración con SWIFT, la red de mensajería financiera global, en 2022, marcó un paso significativo hacia la integración de la tecnología blockchain en las finanzas tradicionales.

CHAINLINK POSEE LAS SIGUIENTES CARACTERÍSTICAS:

- **Oráculos descentralizados:**

  Chainlink permite la creación y operación de oráculos descentralizados, que son servicios que conectan contratos inteligentes con fuentes de datos externas del mundo real de manera segura y confiable. Estos oráculos garantizan la integridad y la precisión de los datos proporcionados, evitando la manipulación y el fraude.

- **Seguridad:**

  los nodos de Chainlink utilizan una variedad de técnicas de seguridad para proteger los datos. Esto incluye criptografía para proteger la integridad de los datos, firmas digitales para verificar la autenticidad de los datos y consenso de blockchain para garantizar que los datos sean precisos.

CHAINLINK POSEE LAS SIGUIENTES CARACTERÍSTICAS:

- **Escalabilidad:**

  La red Chainlink está diseñada para escalar a medida que aumenta la demanda de datos, con lo cual se logra mediante el uso de una arquitectura de varios niveles y la fragmentación. La arquitectura de varios niveles permite que la red se divida en capas, lo que mejora el rendimiento y facilita la gestión.

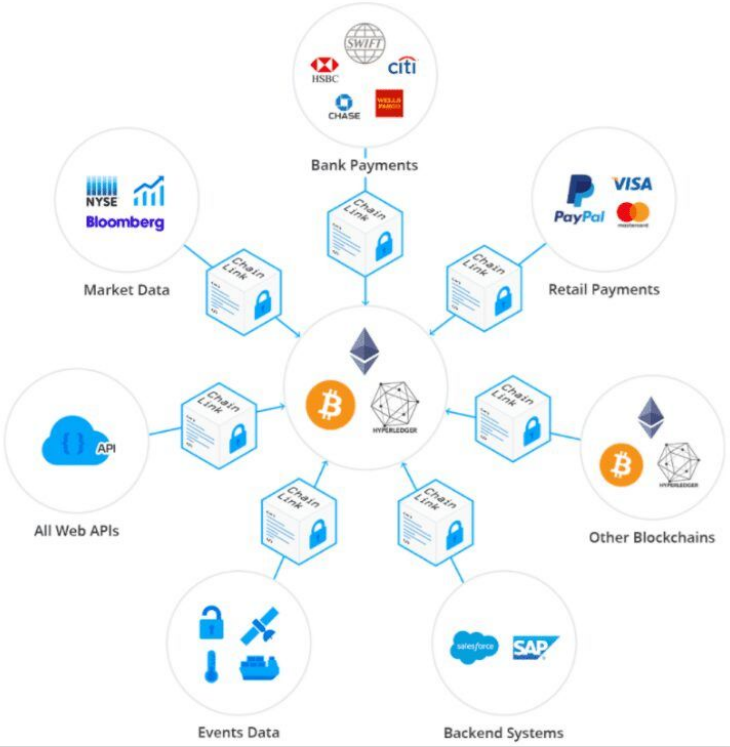
- **Flexibilidad:**

  La red Chainlink puede admitir una amplia gama de tipos de datos. Lo anterior incluye datos financieros, datos meteorológicos, datos de IoT y más. Además, la red también es compatible con una variedad de contratos inteligentes, lo que la hace flexible para una amplia gama de aplicaciones.

CHAINLINK POSEE LAS SIGUIENTES CARACTERÍSTICAS:

- **Transparencia:**

  el funcionamiento de la red Chainlink es transparente y auditable. Cualquier persona puede verificar la fuente de los datos y cómo se procesan. Esto se logra mediante el uso de contratos inteligentes y registros públicos.



Binance Smart Chain (BSC)

Es una blockChain compatible con Ethereum que permite el desarrollo de contratos inteligentes y la integración de oráculos para acceder a datos externos. Esta plataforma ofrece funcionalidades similares a Ethereum, lo que significa que los desarrolladores pueden aprovechar su infraestructura para crear dApps y contratos inteligentes de manera eficiente. Al igual que Ethereum, BSC proporciona un entorno seguro y confiable para ejecutar código descentralizado y acceder a información externa a través de oráculos. Esto hace que Binance Smart Chain sea una opción atractiva para aquellos que buscan construir aplicaciones descentralizadas que requieran interacción con datos del mundo real de forma segura y eficiente.

En 2019, Binance, el exchange de criptomonedas líder en el mundo, anunció Binance Chain, una blockchain diseñada para la eficiencia y el alto rendimiento. Un año después, en 2020, se lanzó Binance Smart Chain (BSC), una blockchain compatible con EVM que permite la ejecución de contratos inteligentes y la creación de aplicaciones descentralizadas (dApps).

BSC ganó rápidamente popularidad debido a sus características atractivas, como las bajas tarifas, la alta velocidad de transacción y la compatibilidad con Ethereum. Esto generó un crecimiento exponencial en 2021, con un aumento significativo en la cantidad de usuarios, proyectos y dApps en la plataforma.

El ecosistema DeFi en BSC prosperó con el lanzamiento de proyectos como PancakeSwap, Venus y Autofarm, convirtiendo a BSC en la segunda blockchain más grande en términos de valor total bloqueado (TVL).

En 2022, BSC se ha integrado con la red de oráculos Chainlink, permitiendo a los desarrolladores acceder a datos del mundo real en sus dApps. Además, se ha lanzado el puente BSC-Polygon, facilitando la transferencia de activos entre ambas cadenas. BSC también se ha asociado con proyectos líderes en la industria para impulsar la adopción de la tecnología blockchain.

Características clave de BSC:

- **Escalabilidad:** BSC puede procesar hasta 3.000 transacciones por segundo, lo que la convierte en una de las blockchains más rápidas del mercado.
- **Compatibilidad con EVM:** BSC es compatible con la Máquina Virtual Ethereum (EVM), lo que facilita la migración de dApps desde Ethereum a BSC.
- **Bajas tarifas:** Las tarifas de transacción en BSC son significativamente más bajas que en Ethereum, lo que la hace más atractiva para los usuarios y desarrolladores.
- **Interoperabilidad:** BSC se está integrando con otras blockchains para crear un ecosistema interoperable.

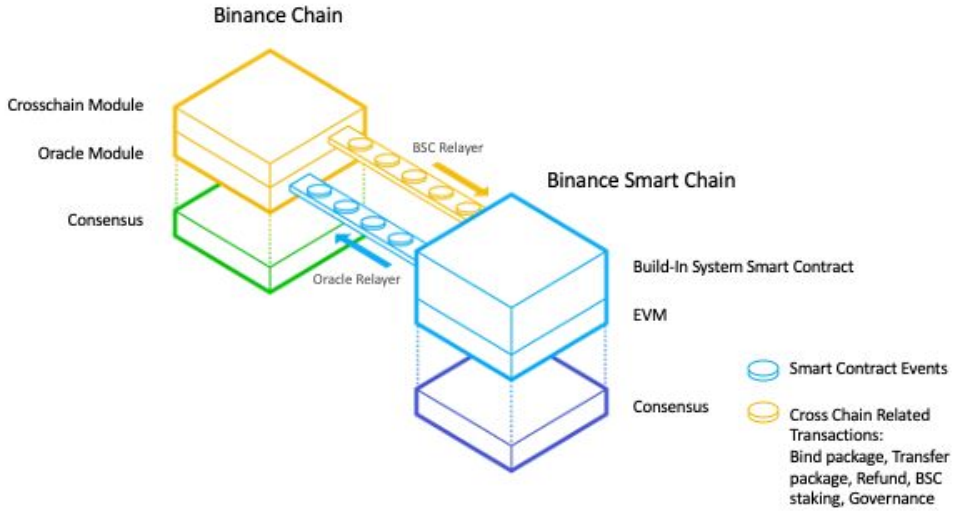
BSC ha tenido un impacto significativo en la industria de las criptomonedas. Ha proporcionado una plataforma escalable y de bajo costo para el desarrollo de dApps, lo que ha impulsado la innovación y la adopción de la tecnología blockchain.

Ejemplos de proyectos en BSC:

- **PancakeSwap:** es un exchange descentralizado que permite a los usuarios intercambiar criptomonedas sin la necesidad de un intermediario.

- **Venus:** es un protocolo de préstamos y préstamos que permite a los usuarios depositar y prestar criptomonedas.

- **Autofarm:** es un agregador de rendimiento que permite a los usuarios optimizar sus rendimientos en DeFi.



Polkadot

Es una plataforma de blockChain interoperable que facilita la conexión entre blockChains independientes. Además de su capacidad para interoperar entre múltiples blockChains, Polkadot ofrece funcionalidades para el desarrollo y despliegue de oráculos. Estos oráculos tienen la capacidad de recopilar y transmitir datos entre diferentes blockChains de manera eficiente y segura. Al permitir que los oráculos interoperen con múltiples blockChains, Polkadot amplía las posibilidades de aplicación de la tecnología blockChain al facilitar el intercambio de información y activos entre diferentes redes descentralizadas. Esto hace de Polkadot una plataforma atractiva para aquellos que buscan construir sistemas blockChain que requieran interoperabilidad y acceso a datos externos.

En 2016, Gavin Wood, cofundador de Ethereum, concibió Polkadot como una solución al problema de la fragmentación en el ecosistema blockchain. Su visión era crear una plataforma que permitiera la interoperabilidad entre blockchains independientes, facilitando el intercambio de datos y activos.

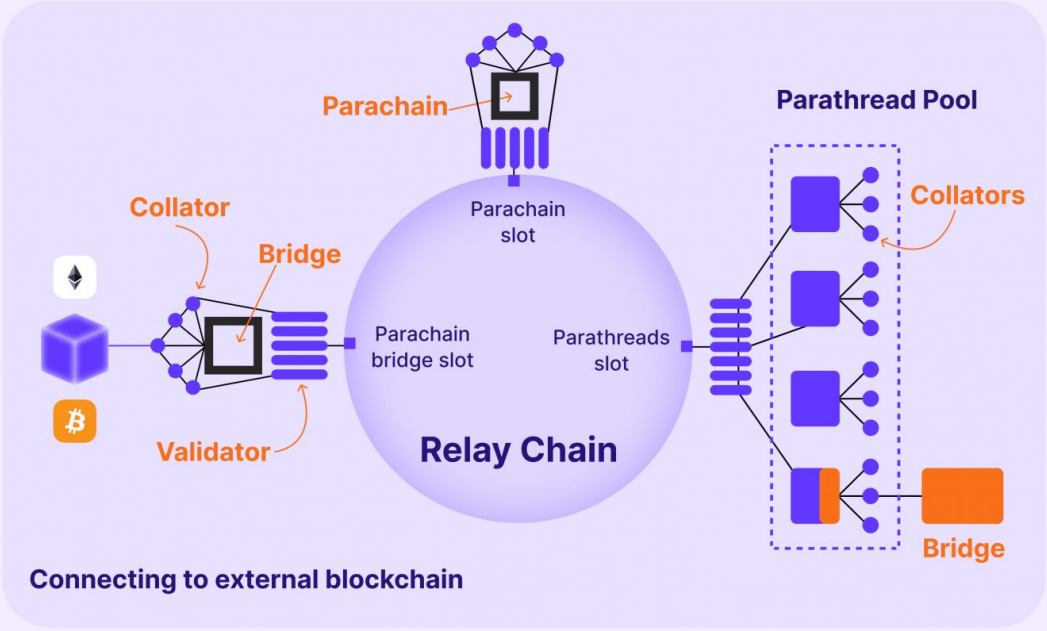
Dos años después, en 2017, se lanzó Web3 Foundation, una organización sin fines de lucro dedicada al desarrollo de Polkadot. Ese mismo año, la ICO de Polkadot recaudó $420 millones, lo que demuestra el gran interés en la propuesta de interoperabilidad.

El año 2020 marcó un hito con el lanzamiento de Kusama, una red de prueba "canario" para Polkadot, y posteriormente, la red principal de Polkadot. Desde entonces, la plataforma ha experimentado un crecimiento exponencial en la cantidad de usuarios, proyectos y paracaídas (blockchains independientes que se conectan a Polkadot). Durante el 2021, se lanzaron importantes paracaídas como Moonbeam, Acala y Clover, cada uno con sus propias funcionalidades y casos de uso. Esto ha contribuido a la diversificación del ecosistema de Polkadot y ha impulsado su adopción.

En 2022, Polkadot ha continuado su evolución con el lanzamiento de XCM v2, una nueva versión del protocolo de comunicación entre paracaídas que mejora la interoperabilidad. Además, se ha lanzado Statemint, un paracaída para la emisión de activos digitales, y se han establecido alianzas con proyectos líderes en la industria para impulsar la adopción de la tecnología blockchain.

Algunas características **clave de Polkadot** son:

- **Interoperabilidad:** Polkadot permite que las blockchains independientes se comuniquen e interoperen entre sí.
- **Seguridad:** Polkadot utiliza una arquitectura de sharded security para garantizar la seguridad de la red.
- **Escalabilidad:** Polkadot puede escalar horizontalmente al agregar nuevas paracaídas a la red.
- **Gobernanza:** Polkadot tiene un sistema de gobernanza on-chain que permite a los titulares de DOT participar en la toma de decisiones.



Polkadot es un protocolo de red que facilita la transferencia de datos, no solo tokens, entre blockchains, lo que la convierte en un entorno multi-chain. Su impacto en la industria de las criptomonedas ha sido considerable al abordar el desafío de la fragmentación de las blockchains, al permitir la comunicación e interoperabilidad entre blockchains independientes.

Así, en la red Ethereum, la distribución de registros se produce únicamente entre usuarios dentro de esta red, mientras que en Polkadot, la información se guarda en dispositivos que operan en todas las redes integradas en este protocolo.

Cardano

Es una blockChain de tercera generación que se distingue por su enfoque en la seguridad, la escalabilidad y la sostenibilidad. Aunque su ecosistema de contratos inteligentes está actualmente en desarrollo, se espera que Cardano permita el desarrollo de oráculos en el futuro. Estos oráculos tendrán como objetivo proporcionar acceso a datos externos para aplicaciones descentralizadas en la red Cardano. Dado el énfasis de Cardano en la investigación académica y en la implementación de protocolos robustos, se espera que los oráculos en esta plataforma sean seguros y confiables. A medida que Cardano continúa evolucionando y madurando, es probable que veamos un mayor desarrollo y adopción de oráculos para complementar su infraestructura blockChain y mejorar sus capacidades en términos de funcionalidad y utilidad para los desarrolladores y usuarios.

El inicio de Cardano se remonta al año 2015, cuando Charles Hoskinson, uno de los cofundadores de Ethereum, junto con Jeremy Wood, establecieron la compañía IOHK (Input Output Hong Kong). Con el objetivo de desarrollar una plataforma blockchain de tercera generación, IOHK inició el proyecto Cardano. En 2017, Cardano lanzó su primera fase, Byron, que introdujo la funcionalidad básica de la red, incluyendo su criptomoneda nativa, ADA. Desde entonces, el proyecto ha pasado por varias fases de desarrollo, cada una centrada en mejorar la escalabilidad, la interoperabilidad y la sostenibilidad de la red. En 2021, Cardano alcanzó un hito importante con el lanzamiento de su fase de gobernanza descentralizada, llamada "Alonzo", que permitió la implementación de contratos inteligentes en la red.

A medida que continúa su evolución, Cardano se ha convertido en un actor destacado en el espacio de las criptomonedas, con un enfoque en la investigación académica y la implementación de tecnologías innovadoras para promover la inclusión financiera y la descentralización a nivel mundial.

A continuación se exponen algunas de las características más relevantes de Cardano:

- Está diseñado para ser altamente escalable, lo que significa que puede manejar un gran volumen de transacciones de manera eficiente. Utiliza un protocolo de consenso único llamado Ouroboros, que permite un alto rendimiento y una escalabilidad mejorada a medida que la red crece. Ouroboros utiliza un enfoque de prueba de participación (PoS) para validar transacciones, lo que reduce significativamente el consumo de energía en comparación con otros protocolos de consenso como la prueba de trabajo (PoW).
- Se esfuerza por lograr la interoperabilidad con otras blockchains y sistemas financieros tradicionales. Esto significa que Cardano puede comunicarse y compartir datos con otras plataformas, lo que permite la transferencia de activos digitales y la ejecución de contratos inteligentes entre diferentes redes. La interoperabilidad es fundamental para la adopción generalizada de blockchain y para la creación de un ecosistema financiero más conectado y eficiente.

- La seguridad es una prioridad clave en Cardano. Implementa un enfoque basado en evidencia y revisión académica para garantizar la seguridad y la robustez de su protocolo. Además, Cardano está diseñado para ser resistente a ataques maliciosos y cuenta con múltiples capas de protección, incluyendo criptografía avanzada y protocolos de consenso seguros. Esto ayuda a proteger los activos y la integridad de la red, brindando confianza a los usuarios y desarrolladores.

- Aplica un modelo de gobernanza descentralizada que permite a los titulares de ADA participar en la toma de decisiones sobre el futuro de la red. Esto se logra a través de un sistema de votación transparente y abierto, donde los titulares de ADA pueden proponer y votar sobre cambios en el protocolo, mejoras y proyectos de desarrollo. La gobernanza descentralizada fomenta la transparencia, la inclusión y la innovación, permitiendo que la comunidad participe activamente en la evolución de Cardano.

- La seguridad es una prioridad clave en Cardano. Implementa un enfoque basado en evidencia y revisión académica para garantizar la seguridad y la robustez de su protocolo. Además, Cardano está diseñado para ser resistente a ataques maliciosos y cuenta con múltiples capas de protección, incluyendo criptografía avanzada y protocolos de consenso seguros. Esto ayuda a proteger los activos y la integridad de la red, brindando confianza a los usuarios y desarrolladores.

- Aplica un modelo de gobernanza descentralizada que permite a los titulares de ADA participar en la toma de decisiones sobre el futuro de la red. Esto se logra a través de un sistema de votación transparente y abierto, donde los titulares de ADA pueden proponer y votar sobre cambios en el protocolo, mejoras y proyectos de desarrollo. La gobernanza descentralizada fomenta la transparencia, la inclusión y la innovación, permitiendo que la comunidad participe activamente en la evolución de Cardano.

Cardano proporciona una plataforma escalable, sostenible y segura para el desarrollo de aplicaciones descentralizadas (dApps).