Desentrañando Cardano

Juan Manuel Vera Osorio, *juan.verao@udea.edu.co, Ingeniería de sistemas, Universidad de Antioquia*

[[1]](#footnote-1)

***Abstract*— ToDo**

***Index Terms*— ToDo**

# I. INTRODUCCIóN

C

ardano emerge como una blockchain de código abierto desarrollada por investigadores y académicos de distintas partes del mundo, basada en la tecnología de Bitcoin y fundada en 2015 como una alternativa a Ethereum, la red donde se procesan las transacciones y operaciones realizadas con la criptomoneda ADA posee una de las capitalizaciones de mercado más grandes frente a la mayoría de redes presentes en el ecosistema actual y su moneda ADA se encuentra entre las más valiosas hace varios años.

Fundada por Charles Hoskinson, cofundador de Ethereum, Cardano propone una red enfocada al uso de la tecnología descentralizada para finanzas y aplicaciones Web3, usando un mecanismo de consenso mucho más sustentable que el “Proof of work” implementado por Bitcoin y otros sistemas descentralizados, además de tener la particularidad de que todas las partes fundamentales de la red son creadas consultadas y auditadas por académicos e investigadores.

A continuación, se hará revisión de las características más destacables de Cardano como red y protocolo, además de comparar sus diferencias o similitudes con otras blockchains populares.

# II. ADA

La criptomoneda de cardano, la cual recibe su nombre en inspiración a la primera programadora de computadores Ada Lovelace, es el activo usado para realizar transacciones y usar contratos inteligentes dentro de la red de Cardano. Es importante destacar que, de forma similar a Bitcoin, el suministro de ADA es limitado, cuando se introdujo a la red se decidió que exista una cantidad máxima de 45’000’000’000 de este activo, esto quiere decir que luego de la eventual finalización de la emisión de ADA por parte de la red la única forma de obtener este activo será mediante la compra de monedas que ya existen dentro de la red.

La distribución inicial de esta cripto moneda se realizó en el momento de su introducción a la red mediante una oferta inicial de moneda, en la cual se permite a interesados adquirir una cantidad inicial de la moneda, en este caso particular, 81% de la oferta inicial fue obtenida por usuarios particulares, siendo uno de los activos que ha tenido mayor adquisición inicial por parte de inversionistas mayoritarios.

Luego de esta distribución inicial, nuevo ADA debe de ingresar a la red, en el caso de Cardano, las nuevas monedas entran en circulación únicamente como recompensa por staking, mecanismo de consenso implementado por la red y el cual se detallará más adelante.

En el apartado del intercambio de ADA como activo, puede ser relativamente sencillo comprarlo o venderlo, pues actualmente es una de las monedas mas populares del mercado, la forma más rápida siendo a través de exchanges internacionales como Coinvase, Binance o kraken, cambiándolo por otras criptomonedas o incluso depósitos nacionales en algunos países que lo permiten, o alguna plataforma localizada como SatoshiTango, la cual permite comprar o vender ADA usando directamente pesos argentinos.

# III. Funcionamiento de la red

En su whitepaper Cardano afirma ser una red de “Tercera generación”, término usado en su whitepaper para describir la red debido a que realiza una diferenciación de las transacciones simples de las realizadas por aplicaciones descentralizadas, en este caso resulta evidente que la tecnología está inspirada en gran medida en las redes de Bitcoin y Ethereum. Esta red busca convertirse en una plataforma en la que cualquier tercero pueda apoyarse para crear sus propios tokens, aplicaciones y soluciones financieras que requieran o puedan aprovecharse de las tecnologías descentralizadas, presentando una similitud con los objetivos de plataformas como el conocido Ethereum, sin embargo, el desarrollo de Cardano también estudia el uso de las conocidas como sidechains en Bitcoin para lograr integrar transacciones complejas o Smart contracts sin que estas se vean afectadas por congestionamientos de la red o precios de comisiones demasiado altos, problemas frecuentes en redes como la mencionada Ethereum

Es debido a esto que la arquitectura de Cardano se consolida como una red con 2 capas de transacciones distintas; primero está la CSL (Cardano settlement layer), esta capa tiene como objetivo proporcionar el espacio en el que los validadores de Proof of Stake cumplan la tarea de registrar y verificar transacciones comerciales. Por otro lado, también existe la llamada CCL (Cardano computational layer), esta capa está destinada al despliegue de contratos inteligentes y aplicaciones complejas, en ella se almacenan datos mucho más específicos, como el peso en megabytes de una transacción, las firmas usadas para enviarla, además de los detalles de los contratos inteligentes, se podría afirmar que este detalle diferencia Cardano de redes que no distinguen transacciones con base en su complejidad, como Ethereum.

Con respecto al método de consenso de la red, es importante hablar inicialmente del método Proof of Stake, implementado por redes como ethereum y en este caso, por cardano dentro de su propio sistema validación. El término “Staking” hace referencia a depositar o delegar monedas a en un smart contract o wallet y mantener esas monedas por un periodo determinado para obtener recompensas.

Proof of Stake o Prueba de Participación es un protocolo de consenso creado para reemplazar al conocido Proof of Work, aportando una mejor seguridad y escalabilidad a las redes que lo implementen. En este método existen los llamados nodos validadores, los cuales se encargan de validadar y registrar bloques nuevos que son procesados por la red, esta decide que nodo se encarga de validar un bloque, cada red decide si de forma totalmente aleatoria, o dando mayor probabilidad a los que cumplan ciertos criterios como el tiempo de participación en la red o la cantidad de moneda que posea, como es el caso de cardano.

Esto demuestra cómo el Proof of Stake difiere completamente del conocido protocolo de proof of work. Mientras que, en este, cada nodo lleva a cabo un intenso proceso de cálculo para resolver complejos rompecabezas criptográficos, en el proof of stake la dinámica cambia, convirtiéndolo en un método de consenso mucho más simple y respetuoso con el medio ambiente en términos energéticos. Por esta razón, numerosos proyectos blockchain están mostrando interés en adoptar este innovador protocolo.

Para la liquidación de transacciones, Cardano se apoya en su sistema llamado Ouroboros, su propio sistema de Proof of Stake incorporado que se encarga de verificar y registrar la información en la blockchain.

Desarrollado por académicos de la universidad de Edimburgo, Ouroboros plantea la conformación de grupos de nodos validadores (pools de stake) encargados de evitar el conocido double spending en las transacciones. Para poder participar como un validador, es necesario una wallet nodo y acumular ADA en esta. Gracias a esta implementación de Proof of Stake los usuarios de Cardano pueden acumular sus monedas para ganar recompensas, proceso también conocido como “Staking”. Adicionalmente, el staking hace destacar a Cardano de entre otras blockchains, pues es una alternativa mucho menos nociva para el medio ambiente comparada con el tradicional Proof of Work, con el beneficio adicional de que no es necesario equipos especiales para poder participar.

Sin embargo, también es un método de consenso que suele ser criticado debido a su tendencia a la posible centralización en grupos de alto poder adquisitivo, esto debido a que la probabilidad de que un pool sea seleccionado como validador de un bloque de transacciones está directamente relacionada con la cantidad de ADA que este posea, es decir, mientras más ADA haya en un pool, mayor probabilidad tiene de ser seleccionado por la red como el nodo validador de un bloque. Posiblemente es por este motivo que el staking es conocido por ser realizado principalmente por empresas de un poder adquisitivo considerable, aunque aún existen grupos independientes que fundan sus propios pools de staking como es el caso de Cardano Café o ACL, lo que demuestra que aún hay espacio para una mayor descentralización en la red.

En resumen, el riesgo de centralización es un desafío inherente al modelo de consenso Proof of Stake implementado por Cardano, pero el protocolo ha adoptado medidas como los límites de saturación de los pools para mitigar este problema y fomentar una mayor distribución de la participación en la validación de bloques.

A diferencia del proceso de minería del habitual proof of work, en el que las recompensas son monedas recién emitidas, las recompensas que otorga cardano por hacer staking se basan en la comisión de las transacciones y reservas de ADA existentes en un fondo en IOHK destinado para este propósito, debido a esto las recompensas no se otorgan cuando se valida un bloque, si no cada cierto tiempo.

Entre los pools más mencionados entre la comunidad se encuentran comúnmente los ofrecidos por exchanges, como Coinbase o Binance, igualmente, existen wallets como Exosdus o Daedalus que ofrecen a sus usuarios la posibilidad de realizar staking desde su propia wallet. Sin embargo, es importante tener en cuenta algunos detalles si se desea hacer staking, particularmente en cardano, uno de estos siendo que los pools de staking deben de permanecer conectados a la red las 24 horas del día, los 7 días de la semana, es debido a esto que todos los pools de staking cobran una comisión a los usuarios destinada al mantenimiento y los costos operativos del servicio.

Por otro lado, la recompensa que obtienen los usuarios es un porcentaje fijo de la cantidad de ADA que tengan en staking durante un periodo de tiempo. Estas recompensas se entregan cada vez que concluye una de las llamadas epoch, estas son medidas que comprenden una tanda de transacciones verificadas y registradas en la blockchain, las epoch de Cardano duran alrededor de 5 días, periodos en los que ocurren los pagos por staking.

Es importante tener en cuenta que cuando un usuario desea empezar a hacer staking dentro de Cardano, debe de esperar un periodo de aproximadamente 20 días para que su solicitud sea aceptada por el pool de staking que haya seleccionado. Esto se debe a que los pools de staking deben de permanecer conectados a la red las 24 horas del día, los 7 días de la semana, y es por esto que todos los pools de staking cobran una comisión a los usuarios destinada al mantenimiento y los costos operativos del servicio.

Es importante tener en cuenta estos detalles al momento de elegir un pool de staking, ya que pueden afectar la rentabilidad y la seguridad de los fondos depositados. Algunos de los pools más mencionados entre la comunidad son los ofrecidos por exchanges como Coinbase o Binance, así como wallets como Exosdus o Daedalus que ofrecen a sus usuarios la posibilidad de realizar staking desde su propia wallet.

# IV. Funcionamiento de los Smart Contracts

Los contratos inteligentes dentro de Cardano se construyen usando el lenguaje de programación conocido como Plutus, el cual guarda a su vez relación con otro lenguaje conocido como Haskell, diferenciándose de otras blockchains que implementan este tipo de contratos como Ethereum, que usa Solidity o Solana que permite construir contratos en typescript.

La arquitectura de los contratos inteligentes de Cardano es de dos capas, debido a que una parte de la del contrato se ejecuta en la red principal, es decir, se ejecuta on-chain y la otra en alguna aplicación desarrollada sobre Cardano, por lo que esta parte se ejecuta off-chain, no obstante, todas las operaciones con contratos inteligentes dentro de la red están sujetos al concepto de UTXO.

Los Unspent Transaction Output (UTXO) son una característica fundamental de la arquitectura de Cardano y otras blockchains basadas en UTXO, como Bitcoin. Los UTXO representan las monedas o activos digitales que pertenecen a una wallet y que aún no han sido gastados en una transacción. Este registro de UTXO permite a la red diferenciar claramente las entradas y salidas de cada transacción, evitando así el problema del doble gasto (double spending). Cada transacción consume uno o más UTXO como entrada y genera uno o más UTXO como salida. Cuando se realiza una transacción, los UTXO de entrada se "gastan" y se crean nuevos UTXO de salida, que representan los activos transferidos. Los nodos validadores de la red verifican que cada transacción cumple con las reglas del protocolo, asegurando que los UTXO de entrada efectivamente pertenecen a la wallet del remitente y que la transacción no intenta gastar los mismos UTXO más de una vez.

Este modelo UTXO ofrece varias ventajas en comparación con el modelo de cuentas utilizado por Ethereum. En primer lugar, es más eficiente en términos de almacenamiento y procesamiento, ya que solo se necesita registrar los UTXO no gastados, en lugar de mantener un registro completo de todas las transacciones y saldos de cuentas. Además, el modelo UTXO es inherentemente paralelo, lo que permite una mayor escalabilidad y rendimiento de la red.

Otra ventaja clave de los UTXO es su compatibilidad con los contratos inteligentes. Los scripts de validación de los contratos inteligentes en Cardano determinan las condiciones bajo las cuales los UTXO pueden ser gastados, lo que permite la creación de aplicaciones descentralizadas complejas y seguras.

En resumen, los UTXO son un elemento fundamental de la arquitectura de Cardano, que permiten una gestión eficiente de las transacciones, evitan el doble gasto y facilitan la implementación de contratos inteligentes y aplicaciones descentralizadas en la red.

En Cardano, los smart contracts determinan la forma, el momento y la dirección en la que liberar y validar una UTXO, al respecto los desarrolladores mencionan en el whitepaper; *“El componente en la red principal (validator-script) es un script que se utiliza para validar que cada transacción que contiene cualquier valor bloqueado por el script (UTXO que residen en la dirección del script) se ajusta a las reglas del contrato. Se requieren herramientas y lenguajes especializados para crear estos scripts.”.* Si la transacción cumple con todos los requisitos, se confirma el envío del UTXO por parte del contrato y puede ser verificado por los nodos validadores para que sea registrado en la blockchain.

Por otro lado, la parte del contrato que se ejecuta off-chain en las aplicaciones descentralizadas sirve para que estas puedan ofrecer funciones para que los usuarios puedan crear y enviar transacciones a la red principal de Cardano, estos servicios, a diferencia de los contratos pueden ser desarrollados en múltiples lenguajes y con herramientas establecidas previamente por los desarrolladores de la red.

Un ejemplo es la plataforma Marlowe, esta plataforma de código abierto es una de las herramientas más usadas para la creación de aplicaciones descentralizadas en Cardano. Creada por IOHK, Marlowe brinda un espacio de trabajo para la creación, testeo y despliegue de los contratos en la red principal, simplificando el proceso de creación de contratos para que sea accesible por personas que no tienen conocimientos avanzados en Plutus.

En conclusión, los smart contracts en Cardano representan una pieza fundamental en la evolución de la blockchain, ofreciendo un enfoque único y robusto para la implementación de aplicaciones descentralizadas y la ejecución de posibles casos de uso. Adicionalmente, presenta una arquitectura flexible, además de un modelo robusto de validación y una considerable variedad de herramientas de desarrollo, Cardano puede posicionarse como líder en el espacio de las blockchains inteligentes, promoviendo la adopción masiva de la tecnología blockchain y catalizando la transformación digital en diversas industrias debido a su claro enfoque hacia el desarrollo de aplicaciones descentralizadas.

# V. aplicaciones descentralizadas en la red

Como se ha mencionado anteriormente, gran parte del valor de cardano reside en su capacidad para sostener el funcionamiento de aplicaciones descentralizadas, por lo que en la red se pueden encontrar juegos play-to-earn, los llamados exchanges descentralizados en incluso mercados de arte digital, a continuación, se van a mencionar algunas de las iniciativas mas famosas y se va a revisar brevemente su propósito.

Indigo es una de las aplicaciones descentralizadas más destacadas en el ecosistema de Cardano. Esta plataforma ofrece a los usuarios la posibilidad de convertir bienes físicos, como obras de arte, propiedades o activos empresariales, en tokens digitales o acciones representativas. Esto permite la comercialización y negociación de estos activos de manera descentralizada, sin necesidad de intermediarios.

La tecnología de Indigo se basa en contratos inteligentes desarrollados sobre la red de Cardano, lo que garantiza la transparencia, seguridad y trazabilidad de todas las transacciones. Cada token emitido representa un activo físico de manera única e indivisible, lo que permite a los propietarios fraccionar la propiedad y facilitar su comercialización a nivel global.

Uno de los principales beneficios es la inclusión financiera que ofrece, al permitir a personas de todo el mundo acceder a oportunidades de inversión y negociación de activos que tradicionalmente estaban reservados a un grupo reducido de inversores. Además, la plataforma elimina las barreras geográficas y reduce significativamente los costos y tiempos de transacción.

La aplicación también cuenta con herramientas de gestión de activos, que permiten a los propietarios monitorear el valor de sus inversiones, recibir dividendos o participar en la toma de decisiones sobre los activos tokeniz ados. Todo esto se logra de manera descentralizada y segura, gracias a la tecnología blockchain de Cardano.

En el apartado de la compra de arte digital, destaca la plataforma ADAX, desarrollada sobre Cardano y especializada en esta área. ADAX es un protocolo descentralizado que facilita las operaciones de compra, venta y comercialización de arte digital dentro del ecosistema de Cardano. A diferencia de los mercados centralizados de NFTs, ADAX elimina la complejidad y los procedimientos complicados, ofreciendo a los usuarios total libertad y control sobre sus activos digitales. Los usuarios pueden crear, listar y negociar NFTs de manera completamente descentralizada, sin la intervención de terceros o intermediarios. Esto se logra gracias a la integración de ADAX con la red de Cardano y el uso de contratos inteligentes. Cada transacción y operación realizada en ADAX se registra de manera transparente en la blockchain de Cardano, garantizando la trazabilidad y seguridad de las operaciones.

Adicionalmente, ADAX ofrece herramientas avanzadas para la gestión de las colecciones de NFTs, como la posibilidad de fraccionar la propiedad, establecer regalías para los creadores y programar subastas automatizadas. Todo ello sin perder el control sobre los activos digitales.

En cardano también se encuentra una aplicación llamada Lenfi, una aplicación descentralizada de préstamos, debido a que los prestamos son un nicho que no suele ser del interés de los consumidores comunes del mundo blockchain, etsa plataforma no es muy conocida por los usuarios ajenos a cardano, sin embargo, es una de las plataformas con mayor cantidad de ADA depositado en sus contratos inteligentes en los últimos años. El protocolo Lenfi tokeniza deudas y garantías en formatos digitales transferibles mediante bonos de préstamo. “La propiedad de fondos sin permiso permite a los usuarios crear y gestionar fondos de liquidez sin autorización centralizada”, mencionan en su whitepaper.

Sundaeswap, por su lado, es una popular plataforma de intercambio descentralizado construida sobre la red de Cardano. Además de permitir el intercambio de tokens, esta también ofrece funcionalidades de staking de ADA. En la plataforma, los usuarios pueden depositar sus ADA en diferentes pools de liquidez, recibiendo a cambio tokens LP (Liquidity Provider) que representan su participación en esos pools. Estos tokens LP les permiten recibir recompensas por el staking de sus ADA, ya que los pools generan comisiones por cada transacción realizada. Esta plataforma también se destaca por tener un volumen de operaciones promedio de alrededor de 20 millones de ADA, lo que la convierte en una de las plataformas DEX más activas y líquidas dentro del ecosistema de Cardano. Esto se debe a la creciente adopción de la red Cardano y al interés de los usuarios por participar en las oportunidades de staking y trading que ofrece la plataforma.

Además de las funcionalidades de intercambio y staking, Sundaeswap también permite a los usuarios crear y listar sus propios tokens personalizados en la red de Cardano. Esto abre la puerta a la creación de nuevas aplicaciones descentralizadas y a la tokenización de activos, ampliando aún más las posibilidades de la plataforma dentro del ecosistema.

Cardano también tiene su propia versión del popular juego play to earn Axie Infinity, basado en Ethereum y que permite a los jugadores recolectar tokens NFT. Este juego en Cardano llamado Drunken Dragons, un juego basado en blockchain que combina elementos de juegos de rol, estrategia y coleccionables. Los jugadores pueden adquirir NFT de dragones únicos, que luego pueden usar para participar en batallas, completar misiones y ganar recompensas en forma del token nativo del juego. La integración de Drunken Dragons con la cadena de bloques Cardano ofrece varias ventajas. En primer lugar, el uso del mecanismo de consenso de Prueba de participación hace que el juego sea más eficiente energéticamente y respetuoso con el medio ambiente en comparación con el sistema de Prueba de trabajo utilizado por axios. Esto se alinea con el enfoque de Cardano en la sostenibilidad y el desarrollo responsable.

Además, la arquitectura de Cardano basada en UTXO permite un procesamiento de transacciones y una escalabilidad más eficientes, lo cual es crucial para un juego con una base de jugadores en crecimiento. El uso de las capacidades de contrato inteligente de Cardano también permite la creación de mecánicas de juego complejas y la gestión segura de los activos del juego, como los Dragon NFT. Una de las craacterísticas únicas del juego es la capacidad de criar y evolucionar dragones, creando variantes nuevas y más poderosas. Esto agrega una capa adicional de juego y estrategia, ya que los jugadores pueden combinar estratégicamente diferentes rasgos de dragón para crear NFT raros y valiosos, adicionalmente también incorpora un intercambio descentralizado, que permite a los jugadores comprar, vender e intercambiar sus Dragon NFT en la red Cardano, esto proporciona una economía vibrante en el juego y oportunidades para que los jugadores moneticen sus esfuerzos en el juego.

# VI. Conclusión

En conclusión, Cardano se posiciona actualmente como una blockchain con un enfoque solido en la sostenibilidad, la descentralización y la innovación tecnológica, promoviendo el desarrollo de aplicaciones descentralizadas sobre su red mientras mantiene costos acordes y accesibles incluso para terceros sin muchos recursos. Su arquitectura de dos capas, su mecanismo propio de proof of stake “Uroboros” y su énfasis académico la diferencian de otras blockchains populares.

Adicionalmente, cardano ofrece una variedad de aplicaciones descentralizadas entre las que se pueden encontrar distintas aplicaciones útiles e innovadoras, desde distintas alternativas para tokenizar activos físicos como obras de arte, propiedades o acciones, hasta juegos que permiten la obtención de recompensas de ADA mientras se juega. Estas aplicaciones demuestran el potencial de cardano para impulsar la integración de tecnologías blockchain en distintos mercados y sectores financieros.

De igual forma, la integración de smart Contracts desarrollados mediante el lengaje Plutus, la facilidad para escalar aplicaciones gracias al modelo UTXO, así como el uso del proof of stake como mecanismo de consenso, conforman una lista particular de características que convierten a cardano en una alternativa atractiva para los desarrolladores interesados en el desarrollo de aplicaciones descentralizadas. Adicionalmente en la red ya existen plataformas como Sundaeswap, Lenfi o ADAX que ejemplifican como cardano promueve nuevas oportunidades en el ámbito de la innovación para aplicaciones descentralizadas.

Por otro lado, los beneficios de cardano en cuanto a sostenibilidad ambiental y consumo de recursos es un factor clvae que la diferencia de otras blockchains que usan el mecanismo de consenso proof of work. Gracias a su implementación de proof of stake, cardano reduce significativamente su consumo energético y la huella de carbono producida por su red, gracias a esta característica, se convierte en una alternativa más responsable con el medio ambiente, un detalle importante en un mundo que busca soluciones tecnológicas más sostenibles hacia el futuro.

A medida que el ecosistema de cardano continue creciendo y evolucionando, es probable que la red mantenga su posición como una red destacada en el ecosistema de las blockchains modrenas, impulsando la transformación digital y abriendo nuevas oportunidades para la innovación. Su enfoque en la investigación, la sostenibilidad y la descentralización la convierte en una alternativa sólida y prometerdora en el panorama actual de tecnologías descentralizadas, con un enorme potencial para marcar un referente en la adopción de las blockchains en nuevos sectores de las tecnologías de la información.

# VII. Referencias

[1] "Cardano Whitepaper" Whitepaper.io, 2022. [Online]. Available: <https://whitepaper.io/document/581/cardano-whitepaper>.

[2] "Protocolo Indigo". [Online]. Available: <https://indigoprotocol.io>.

[3] "SundaeSwap", Sundae Labs, 2024. [Online]. Available: <https://sundae.fi/products/sundaeswap>.

[4] "Drunken Dragon Game" Drunken Dragon Entertainment, 2024. [Online]. Available: <https://www.drunkendragon.games>.

[5] "ADAX" adax, 2024. [Online]. Available: <https://adax.pro>.

[6] "Lenfi" lenfi, 2024. [Online]. Available: <https://adax.pro>.

[7] "Proof of stake Sidechains" Peter Gaži; Aggelos Kiayias; Dionysis Zindros, 2019. [Online]. Available: <https://ieeexplore.ieee.org/document/8835275>.

[8] "Why Cardano" IOHK, 2020. [Online]. Available: <https://why.cardano.org/en/introduction/motivation/>.

[9] "Proyecto Cardano, tercera generación de criptomonedas" Benazco Ángel, Jorge Wolfgang; García Machiñena Morell, Guillermo, 2021. [Online]. Available: <https://riull.ull.es/xmlui/handle/915/24719>.

1. [↑](#footnote-ref-1)