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. INTRODUCTION

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(Consultar y elaborar más), 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.

# III. Funcionamiento de la red

En su whitepaper Cardadno afirma ser una red de “Tercera generación”, termino 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 esta 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 congestinamientos 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 mas 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 metodo de consenso de la red, es importante hablar inicialmente del metodo 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.

Para la liquidación de transacciones, Cardano se apoya en sus 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 academicos 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 tambien 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, tambien es un metodo 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 mas 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 aun existen grupos independientes que fundan sus propios pools de staking como es el caso de Cardano Café o ACL.

# IV. Funcionamiento de los Smart Contracts

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

Los arquitectura de los contratos inteligentes de Cardanos es de dos capas, debido a que una parte de la del contrato se ejecunta 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, o transacción salida no gastada, son un concepto que tiene como objetivo evitar el fenomeno de double spending de monedas dentro de la red, las UTXO reprentan las monedas que pertenecen a una wallet y no han sido gastados en alguna transacción, este registro premite diferenciar las operaciones de entrada y salida liquidadas del saldo total de una entidad.

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 multiples lenguajes y con herramientas establecidas previamente por los desarrolladores de la red.

Un ejemplo es la plataforma Marlowe, esta plataforma de codigo 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, ademas 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 apliaciones descentralizadas.

# V. Conclusión

# VI. Referencias

1. This paragraph of the first footnote will contain the date on which you submitted your paper for review, which is populated by IEEE. It is IEEE style to display support information, including sponsor and financial support acknowledgment, here and not in an acknowledgment section at the end of the article. For example, “This work was supported in part by the U.S. Department of Commerce under Grant 123456.” The name of the corresponding author appears after the financial information, e.g. *(Corresponding author: Second B. Author).* Here you may also indicate if authors contributed equally or if there are co-first authors.

   The next few paragraphs should contain the authors’ current affiliations, including current address and e-mail. For example, First A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (e-mail: author@ boulder.nist.gov).

   Second B. Author Jr. was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

   Third C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba 305-0047, Japan (e-mail: author@nrim.go.jp).

   Mentions of supplemental materials and animal/human rights statements can be included here.

   Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org [↑](#footnote-ref-1)