

# Introducción a Cardano

---

# Antonio Sánchez

**CEO InforByt**

**Perito Judicial Informático**

**Presidente BlockChain Andalucía**

**Embajador Cardano**

**Embajador Zilliqa**

**CISO BlockChain OpenLab**

**CTO KeopSafe**

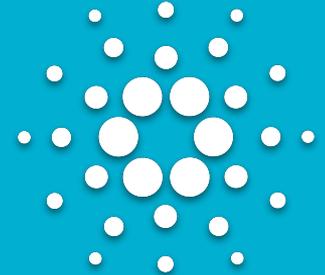


<https://es.linkedin.com/in/antonio-blockchain>

# Índice.

---

1. **Introducción sobre la historia y creación de Cardano.**
2. **Arquitectura actual: Tipos de estructuras de datos empleadas.**
3. **Mapa de ruta de Cardano.**
4. **Algoritmo de Consenso (Ouroboros, tipo PoS) y sus propiedades.**
5. **Seguridad en Cardano.**
6. **Detalles sobre ADA.**
7. **Casos de Uso.**
8. **Costes asociados al uso de la tecnología.**
9. **Ventajas / inconvenientes en temas de coste.**
10. **Cardano para Desarrolladores.**
11. **Su lenguaje de programación Plutus y Marlowe.**
12. **Ejemplos de desarrollos.**



# **Introducción sobre la historia y creación de Cardano.**

---

# Precedentes.

## 2008-2009 **Bitcoin.** ? Satoshi Nakamoto.

- Valor descentralizado.

## 2013 **Ethereum.** Vitalik, Charles Hoskinson, Gavin Wood, ...

- Smart contracts.

## 2015 **Inicia el proyecto.**

Problemáticas:

- Escalabilidad, interoperabilidad, sostenibilidad, gasto energético.

## 2017 MainNet **Cardano.**

- Sistema federado: IOG & Emurgo & Cardano Foundation.

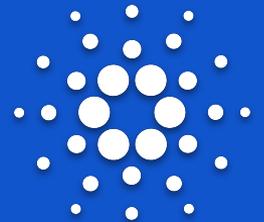


Cardano  
Foundation

- Modelo: Extended UTXO (Native tokens).
- Token Ada ₳. Exchanges: kraken, coinbase, binance, ++

## 2020 Shelley: **Proof of Stake**

- Nodos mantenidos y bloques creados por la comunidad.



# Cardano VS Ethereum.

	 <b>ZILLIQA</b>	 <b>BITCOIN</b>	 <b>ETHEREUM</b>	 <b>TEZOS</b>	 <b>CARDANO</b>
 Circulating / Total Supply	10,022,400,107 / 13,313,867,260 ZIL	18,303,512 / 21,000,000 BTC	110,372,129 ETH *inflation varies	705,020,740 XTZ *inflation varies	25,927,070,538 / 31,112,483,745 ADA
 Mainnet Launched	January 31, 2019	January 3, 2009	July 30 2015	September 17, 2018	September 29, 2017
 Consensus Mechanism	Proof of Work + practical Byzantine Fault Tolerance	Proof of Work	Proof of Work	Liquid Proof of Stake	Ouroboros Proof of Stake
 Transaction Throughput	~2828 tps	~7 tps	~15 tps	~50 tps	~250 tps
 Smart contract Support	Yes	No	Yes	Yes	Not yet
 Smart Contract Language	Scilla	-	Solidity	Michelson	Plutus
 Transaction Finality	Instant	~30 mins	~15 mins	~30 mins	~1 min



# Cardano

El nombre del proyecto, deriva del nombre de **Girolamo Cardano**, un erudito y médico italiano conocido por los primeros cálculos sistemáticos de probabilidades.

Mientras que su token nativo, **ADA**, deriva su nombre de Ada Lovelace, quien fue una reconocida matemática y escritora inglesa.



# Cardano.

- Es el primer proyecto Blockchain que está desarrollado partiendo de una filosofía **científica**.
- Cardano utiliza un algoritmo de consenso por Prueba de Participación con algunas particularidades que han sido integradas por ellos y que lleva el nombre de **Ouroboros**.
- Está basado en un **protocolo multicapa**, utiliza dos capas vinculadas entre sí, la capa de liquidación y la capa de control.
  - La **CSL** actúa como el Libro contable (Ledger) del balance y es la primera capa de la plataforma Cardano.
  - La **CCL** es la segunda capa que conforma Cardano, contiene toda la información sobre lo que pasa con las transacciones que se realizan en la plataforma.



Jeremy Wood y Charles Hoskinson



INPUT | OUTPUT

EMURGO 

# Fundación Cardano

Tiene como misión principal estandarizar, proteger y promover la tecnología que conforma el **Protocolo Cardano**.

Sus objetivos principales:

- Estudiar y proponer una regulación de Blockchain y las criptomonedas.
- Actuar como modelo de Blockchain y criptomoneda estándar.
- Proteger, mejorar y desarrollar el Ecosistema Cardano.
- Hacer crecer la comunidad Cardano dando la máxima formación posible.
- Servir de modelo de organización para que otras empresas se unan a la causa.





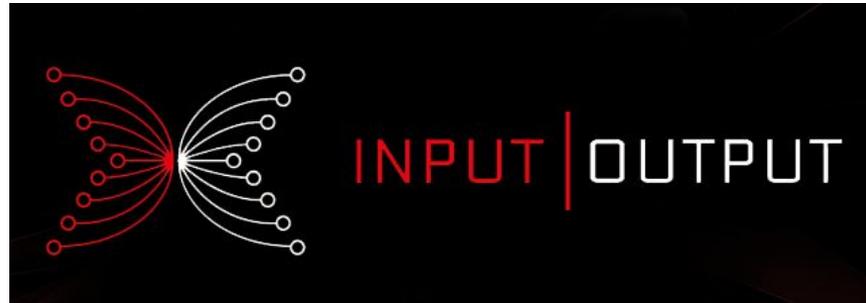
# IOHK

---

Esta empresa fundada en el año 2015 por **Charles Hoskinson** y **Jeremy Wood**, es una referencia mundial en ingeniería y tecnología. Está muy comprometida con el uso y la innovación, con un objetivo, proporcionar servicios financieros a tres mil millones de personas que están forzosamente fuera del sistema.

Es una organización totalmente descentralizada. La compañía crea soluciones de infraestructura Blockchain para clientes gubernamentales y el sector público y privado, y es la fuerza detrás del contrato inteligente y la plataforma descentralizada.

Son los creadores de [Atala Prism](#) y de la Wallet de Nodo completo [Daedalus](#).



# **Arquitectura y tipo de estructura de datos.**

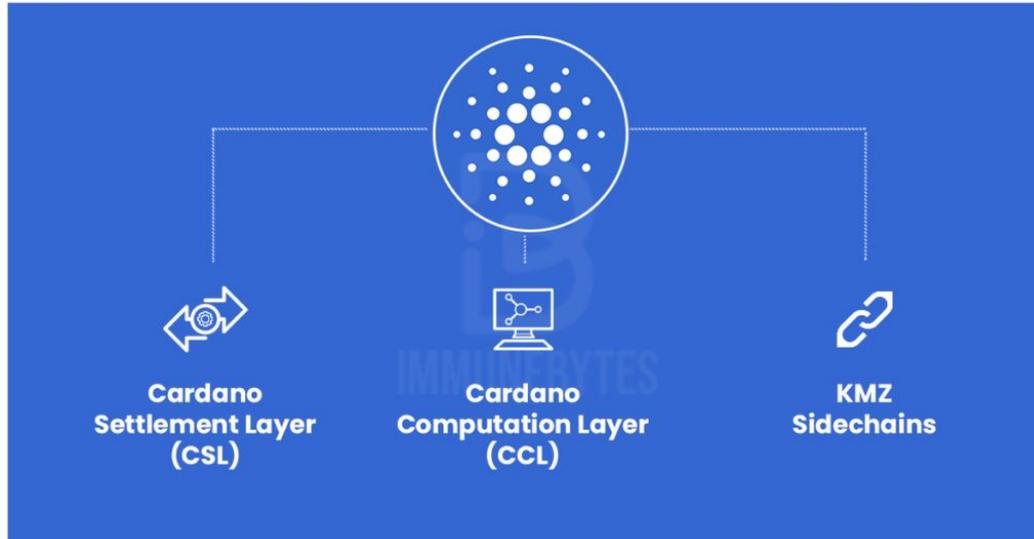
---

# Arquitectura.

La plataforma utilizará un **enfoque de doble capa**, capa de cálculo de Cardano (**CCL**) y capa de asentamiento de Cardano (**CSL**), con la suma de **cadenas laterales**.

Las dos capas separan los datos de la **transacción** de los datos del **contrato** sobre por qué ocurrieron las transacciones.

Las **cadenas laterales** permiten la interoperabilidad entre las dos capas y otras cadenas de bloques.

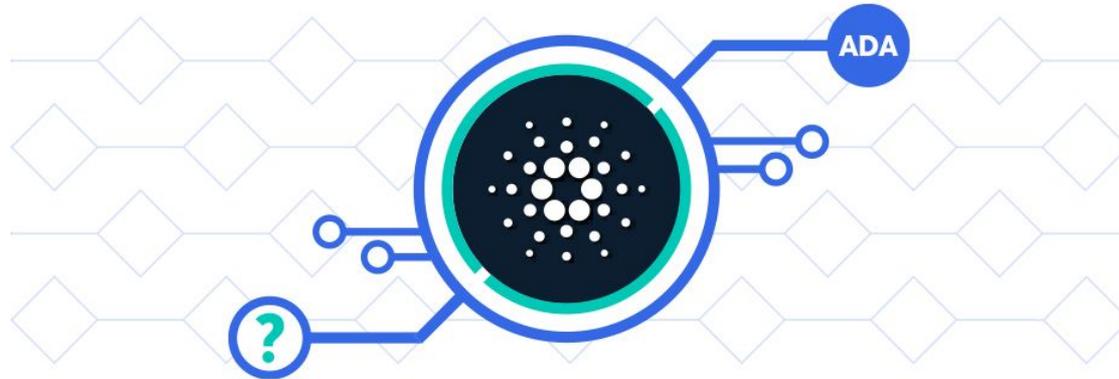


# Capa de computación de Cardano - CSL

---

Aquí es donde se ejecutan todos los **contratos inteligentes**, y donde Cardano se diferencia de algo como Bitcoin por ejemplo. Los fondos de los usuarios se mantienen aquí temporalmente para usar los contratos inteligentes.

Esto ha sido un desafío para **Ethereum** hasta la fecha porque el cómputo inteligente de contratos y la liquidación de transacciones ocurren en la misma capa.



# Capa de asentamiento de Cardano - CSL

---

Aquí es donde se hacen todos los pagos, y, a diferencia de la Capa de Computación (Computation Layer), la **SL** es “tonta”, no tiene muchas características, y tiene una base de código muy pequeña. Sus fondos se mantienen aquí por **seguridad**.



## Cadenas laterales - KMZ

---

Las cadenas laterales de Cardano se basan en las investigaciones de Kiayias, Miller y Zindros (KMZ) que utilizan pruebas de trabajo para permitir **transacciones entre cadenas.**

La Universidad de Edimburgo está demostrando el potencial de estas cadenas laterales para comprimir de manera confiable los datos de otras cadenas de bloques, permitir transacciones cruzadas y evitar doble gasto.



# Estructura de datos.

Los datos utilizan el modelo **CBOR** para la Serialización.

<https://cbor.io/>

# CBOR

## RFC 8949 Representación concisa de objetos binarios

"La representación concisa de objetos binarios (CBOR) es un formato de datos cuyos objetivos de diseño incluyen la posibilidad de un tamaño de código extremadamente pequeño, un tamaño de mensaje bastante pequeño y extensibilidad sin la necesidad de negociar versiones".

## Especificación

CBOR se especifica en un RFC estándar de Internet. Los RFC que sirven como estándares de Internet son generados por el **IETF** sobre la base de un extenso proceso de revisión técnica y control de calidad. Estos están destinados a durar.

Grupo de Trabajo de Ingeniería de Internet



Organización de estándares

Internet Engineering Task Force es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, enrutamiento y seguridad. Se creó en los Estados Unidos en 1986. [Wikipedia](#)

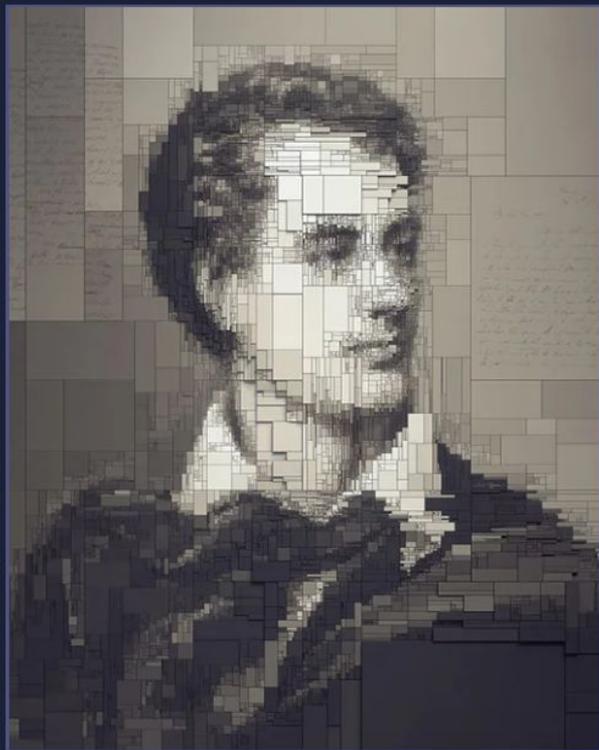
## Request for Comments

[rfc-editor.org](http://rfc-editor.org)

Los Request for Comments, más conocidos por sus siglas RFC, son una serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos. [Wikipedia \(ES\)](#)

# Hoja de Ruta

---



Cardano está clasificada como una de las **criptomonedas** desarrolladas más activamente, según [coincodcap.com](https://coincodcap.com).

# 01

## BYRON | Fundación

Cardano es una cadena de bloques de tercera generación, creada desde cero utilizando investigación, revisión por pares y un riguroso modelo de desarrollo formal. La historia comenzó en 2015, con la visión de abordar los tres desafíos estratégicos que enfrentan todas las redes blockchain: escalabilidad, interoperabilidad y sostenibilidad. Dos años, miles de compromisos de GitHub y cientos de horas de estudio más tarde, la primera versión de Cardano se envió en septiembre de 2017, y comenzó la era de Byron.

La primera encarnación de Cardano permitió a los usuarios comprar y vender la criptomoneda ada, llamada así por la programadora revolucionaria Ada Lovelace, en una red federada que ejecuta el innovador protocolo de consenso Ouroboros. El corazón de la red Cardano, Ouroboros, es el primer protocolo de prueba de participación creado sobre la base de la investigación académica, con un nivel de seguridad probado matemáticamente.

La era de Byron también vio la entrega de la billetera Daedalus, la billetera de escritorio oficial de IOHK para ada, así como Yoroi, una billetera liviana de la compañía hermana de IOHK, Emurgo, diseñada para transacciones rápidas y uso diario.

Por mucho que la era Byron se tratara de los primeros desarrollos tecnológicos cruciales, también se trataba de construir una comunidad e involucrar a las personas en la creación de la cadena de bloques del futuro. Cardano ha pasado de ser un pequeño grupo de entusiastas a una comunidad global, con ada alojado en más de 30 intercambios y con una **capitalización de mercado promedio** que lo convierte en una de las principales criptomonedas del mundo.

Vea cómo lo hicimos a continuación ...

## SHELLEY | Descentralización

Después de la era de Byron, la era de Shelley de Cardano es un período de crecimiento y desarrollo para la red. A diferencia de la era de Byron, que comenzó en un momento dado cuando se lanzó la red principal, la transición a Shelley está diseñada para lograr una transición suave y de bajo riesgo sin interrupciones del servicio.

La era Shelley abarca los primeros pasos críticos en el viaje de Cardano para optimizar la descentralización, y como cualquier primer paso, estos serán graduales pero significativos. Durante la era de Byron, la red se federó, pero a medida que avanza la era de Shelley, más y más nodos se desplazarán hacia la comunidad Cardano. Una vez que los participantes de la red ejecuten la mayoría de los nodos, Cardano estará más descentralizado y como resultado disfrutará de una mayor seguridad y solidez.

Shelley también verá la introducción de un esquema de delegación e incentivos, un sistema de recompensas para impulsar los grupos de estaca y la adopción de la comunidad. Como una red de prueba de participación, los usuarios apuestan su ADA para participar en la red. Cuidadosamente diseñado utilizando la teoría de juegos y las últimas investigaciones sobre las redes de prueba de participación, el esquema de delegación y de incentivos permitir y alentar a los usuarios a delegar su participación hasta piscinas estaca - siempre activa, nodos de red-run comunidad - y ser recompensados por honesta participación en la red.

Al final de la era de Shelley, esperamos que Cardano sea 50-100 veces más descentralizado que otras grandes redes de blockchain, con el esquema de incentivos diseñado para alcanzar el equilibrio alrededor de 1,000 grupos de estaca. Las redes de blockchain prominentes actuales a menudo están controladas por menos de 10 grupos de minería, exponiéndolos a un grave riesgo de compromiso por comportamiento malicioso, algo que Cardano evita con un sistema inherentemente diseñado para fomentar una mayor descentralización. No solo eso, sino que toda la red de Cardano funciona a una fracción del costo de energía de las cadenas de bloques de prueba de trabajo equivalentes, utilizando el equivalente de electricidad de una sola casa, en lugar de un país pequeño.

Cardano está clasificada como una de las [criptomonedas](#) desarrolladas más activamente, según [coincodcap.com](#).



Cardano está clasificada como una de las [criptomonedas](#) desarrolladas más activamente, según [coincodcap.com](#).

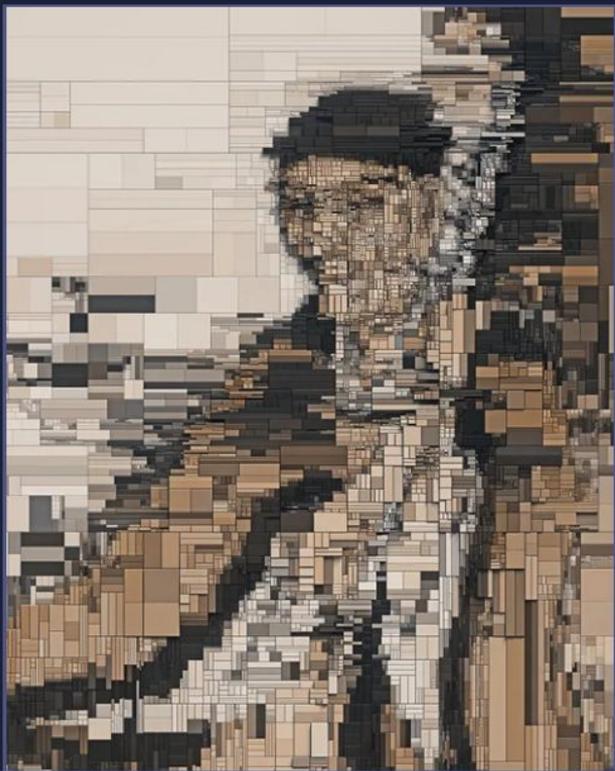
## 03

### GOGUEN | Contratos Inteligentes

Con la integración de los contratos inteligentes, la era de Goguen representa un gran paso adelante en la capacidad de la red Cardano. Donde la era Shelley descentraliza el núcleo del sistema, Goguen agrega la capacidad de construir aplicaciones descentralizadas (DApps) sobre la sólida base de Cardano de investigación revisada por pares y desarrollo de alta seguridad.

El trabajo para Goguen se ha llevado a cabo en paralelo con Shelley, y cuando se complete, permitirá a los usuarios con antecedentes técnicos y no técnicos crear y ejecutar contratos inteligentes funcionales en la red Cardano. Uno de los objetivos para la era de Goguen ha sido la creación de [Plutus](#), un lenguaje de desarrollo de contratos inteligentes y plataforma de ejecución con el lenguaje de programación funcional Haskell. Plutus ya está disponible para pruebas y aporta los beneficios de la programación funcional a la creación de contratos inteligentes. También permite una base de código para admitir componentes dentro y fuera de la cadena, mejorando la coherencia y la usabilidad de la experiencia de desarrollo en comparación con las implementaciones de contratos inteligentes existentes.

La era de Goguen también abarca el trabajo para hacer que Cardano sea accesible a audiencias más amplias a través de [Marlowe](#), lo que permite a los expertos financieros y comerciales sin conocimientos técnicos previos crear contratos inteligentes. Marlowe es un lenguaje de alto nivel específico de dominio (DSL) para contratos financieros que se basa en Plutus. Marlowe viene con [Meadow](#), una plataforma de creación de aplicaciones fácil de usar que los no programadores pueden usar para crear contratos financieros inteligentes. Juntos, Marlowe y Meadow simplifican el proceso de creación de contratos inteligentes para aplicaciones financieras, permitiendo que los expertos en la materia contribuyan directamente sin requerir habilidades profundas de programación. La combinación de Plutus y Marlowe permitirá una nueva clase de contratos inteligentes a nivel empresarial con funcionalidad verificada, capaz de apuntalar implementaciones a gran escala en el mundo real.



Cardano está clasificada como una de las **criptomonedas** desarrolladas más activamente, según [coincodex.com](https://coincodex.com).

## 04

### BASHO | Escalada

La era de Basho de Cardano es una era de optimización, que mejora la escalabilidad e interoperabilidad de la red. Mientras que las eras de desarrollo anteriores se centraron en la descentralización y la nueva funcionalidad, Basho se trata de mejorar el rendimiento subyacente de la red Cardano para respaldar mejor el crecimiento y la adopción de aplicaciones con un alto volumen de transacciones.

Uno de los principales desarrollos de Basho será la introducción de cadenas laterales: nuevas cadenas de bloques, interoperables con la cadena principal de Cardano, con un inmenso potencial para ampliar las capacidades de la red. Las cadenas laterales se pueden usar como mecanismo de fragmentación descargando el trabajo de la cadena principal en una cadena lateral para aumentar la capacidad de la red. También se pueden usar para introducir características experimentales sin afectar la seguridad de la cadena de bloques principal.

Basho también verá la introducción de estilos de contabilidad paralelos. Si bien la cadena de bloques principal de Cardano continuará utilizando un modelo UTXO, la capacidad de admitir y cambiar entre UTXO y modelos basados en cuentas se agregará mediante cadenas laterales. El resultado será una mayor interoperabilidad para Cardano, así como la capacidad de admitir nuevos tipos de casos de uso en la red.

En general, la era de Basho verá a Cardano convertirse en una de las plataformas blockchain de más alto rendimiento, resilientes y flexibles de la industria. Esto proporcionará una infraestructura de red con la capacidad de escalar de manera sostenible y segura, así como la capacidad de agregar nuevas funcionalidades sin comprometer la confiabilidad en el núcleo de la red.

La era de Voltaire de Cardano proporcionará las piezas finales necesarias para que la red de Cardano se convierta en un sistema autosustentable. Con la introducción de un sistema de votación y tesorería, los participantes de la red podrán utilizar sus derechos de participación y voto para influir en el desarrollo futuro de la red.

Para que la red Cardano se vuelva verdaderamente descentralizada, requerirá no solo la infraestructura distribuida introducida durante la era Shelley, sino también la capacidad de mantenerse y mejorar con el tiempo de manera descentralizada. Con ese fin, la era de Voltaire agregará la capacidad de los participantes de la red para presentar propuestas de mejora de Cardano que puedan ser votadas por las partes interesadas, aprovechando el proceso de replanteo y delegación ya existente.

Para financiar el desarrollo futuro de la red, Voltaire también verá la adición de un sistema de tesorería, mediante el cual una fracción de todas las tarifas de transacción se agruparán para proporcionar fondos para las actividades de desarrollo realizadas después del proceso de votación.

Cuando existan un sistema de votación y de tesorería, Cardano estará verdaderamente descentralizado y ya no estará bajo la administración de IOHK. En cambio, el futuro de Cardano estará en manos de la comunidad, que tendrá todo lo que necesita para crecer y evolucionar Cardano desde la base segura y descentralizada establecida por IOHK.

Estamos trabajando en más contenido para esta era de la hoja de ruta y actualizaremos esta página en el momento adecuado. Mientras tanto, todas las actualizaciones más recientes sobre el progreso técnico se entregan como parte de los [Informes técnicos semanales de Cardano](#).

Cardano está clasificada como una de las [criptomonedas](#) desarrolladas más activamente, según [coincodcap.com](#).

**Algoritmo de consenso**

**Ouroboros**

---

# Algoritmo de Consenso - OUROBOROS

---

**Ouroboros** es un protocolo de prueba de participación, que se distingue de la prueba de trabajo. En lugar de depender de “mineros” para resolver ecuaciones computacionalmente complejas para crear nuevos bloques y recompensar al primero que lo haga, la prueba de participación selecciona a los participantes para crear nuevos bloques basándose en su participación (en el caso de Cardano, la cantidad de **ADA** que controlan) en la red.



# Algoritmo de Consenso - OUROBOROS

---

Liderado por **Aggelos Kiayias** en la Universidad de Edimburgo, **Ouroboros** y sus posteriores implementaciones **BFT**, **Praos**, **Génesis e Hydra**, proporcionan una nueva línea de base para resolver algunos de los mayores desafíos del mundo, de forma segura y a escalable.

Las redes que usan **Ouroboros** son mucho más eficientes energéticamente que las que usan pruebas de trabajo, a través de Ouroboros, Cardano es capaz de lograr una eficiencia energética sin precedentes.

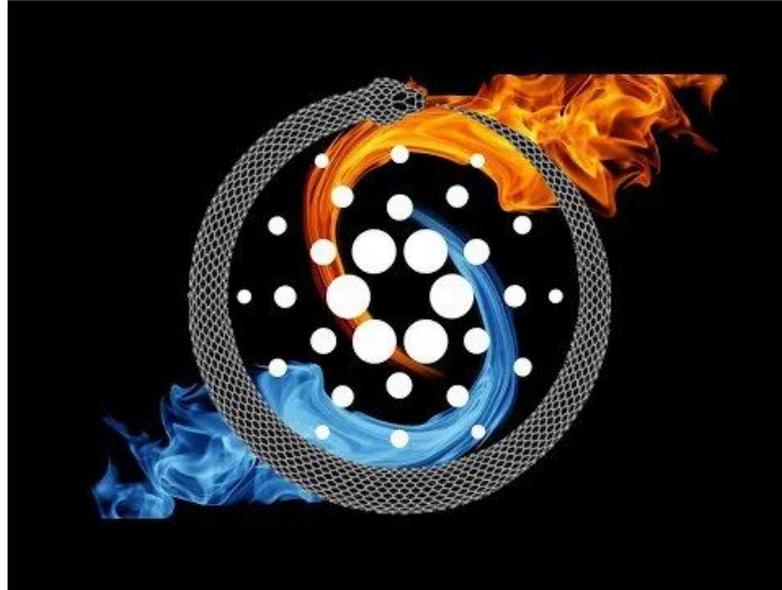
Al mismo nivel de descentralización, por ejemplo, 100 stake pools, lo que supera la red actual en Bitcoin, Cardano podría consumir tan sólo 0,01567GWh (gigavatios-hora) por año. Bitcoin, por su parte, requeriría [181 TWh](#) por año.



# OUROBOROS CLASSIC.

---

La primera implementación del protocolo de Ouroboros, se publicó en 2017. Esta primera implementación (denominada Ouroboros Classic) sentó las bases del protocolo como un rival energéticamente eficiente para la prueba de trabajo, introdujo el marco matemático para analizar la prueba de participación e introdujo un novedoso mecanismo de incentivo para recompensar a los participantes en un entorno de prueba de participación.



# OUROBOROS BFT.

---

Ouroboros BFT (**Tolerancia a la Falla Bizantina**) es un simple protocolo que fue usado por Cardano durante el reinicio de Byron, que fue la transición del antiguo código base de Cardano al nuevo.

Ouroboros BFT ayudará a preparar la red de Cardano para la liberación de Shelley y, con ello, su descentralización.

En lugar de requerir que los nodos estén en línea todo el tiempo, **Ouroboros BFT** asume una red federada de servidores la Blockchain y una comunicación sincrónica entre los servidores, proporcionando un consenso de libro mayor de una manera más simple y determinista.



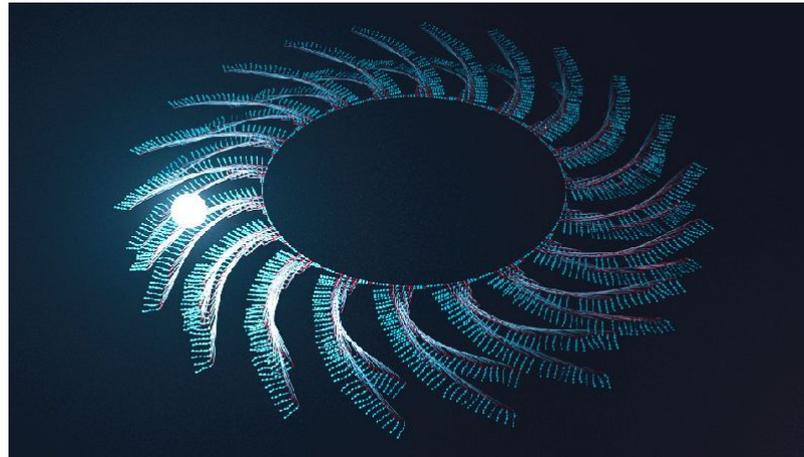
# OUROBOROS PRAOS

---

Se basa y proporciona mejoras sustanciales de seguridad y escalabilidad a Ouroboros Classic.

Al igual que Ouroboros Classic, **Ouroboros Praos** procesa los bloques de transacciones dividiendo las cadenas en franjas, que se agregan en épocas. Sin embargo, a diferencia de Ouroboros Classic, Praos se analiza en un entorno semi sincrónico y es seguro contra los atacantes adaptables.

Praos garantiza que un adversario fuerte no pueda predecir el próximo líder de la franja y lanzar un ataque centrado (como un ataque **DDoS**) para subvertir el protocolo.



# OUROBOROS GÉNESIS

---

**Génesis** mejora aún más a Ouroboros Praos al añadir una nueva regla de selección en cadena, que permite a las partes arrancar desde un bloque de génesis, sin la necesidad de puntos de control confiables o suposiciones sobre la disponibilidad pasada.

**Génesis** también proporciona una prueba de la componibilidad universal del protocolo, que demuestra que el protocolo puede componerse con otros protocolos en configuraciones arbitrarias en un entorno real, sin perder sus propiedades de seguridad. Esto contribuye significativamente a su seguridad y sostenibilidad, y a la de las redes que lo utilizan.



# OUROBOROS HYDRA

---

**Hydra** es una arquitectura de escalabilidad fuera de la cadena que aborda tres desafíos clave de escalabilidad: alta producción de transacciones, baja latencia y mínimo almacenamiento por nodo.

**Hydra** propone y describe la introducción de canales estatales multipartitos, que ofrece un procesamiento de transacciones paralelo para mejorar drásticamente la salida de transacciones por segundo (**TPS**) de Cardano, y la confirmación instantánea de las transacciones.



# Proof of Stake

---

**Stake:** Cantidad de tokens.

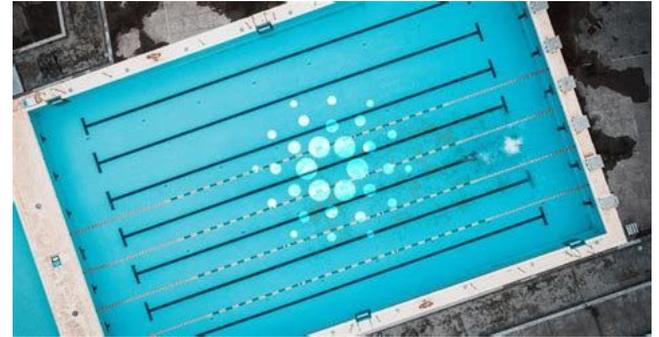
**Ouroboros Protocol:** Los Stake Pool firman bloques de forma aleatoria en proporción a su **Stake**. Reciben recompensas por su trabajo y las reparten con los delegantes.

**Epoch:** 5 días (432.000 slots, 21.600 blocks)

**Slot:** 1 seg

**Rol:**

- **Stake Pool.** Entidad que se compone de un conjunto de nodos encargados de crear bloques. Min. 2vcpus 8Gb Pledge, Fees, Saturation.
- **Delegante.** Participa en el protocolo de consenso vinculando su stake a un pool de su elección.



# Seguridad en Cardano

---

# Seguridad en Cardano

**Cardano**, y en general cada red blockchain pública, tiene activos preciados, como las moneda nativa de Bitcoin, en este caso BTC. Puede ser también la moneda nativa ADA, y muchos otros activos en el caso de Cardano. La red debe ser segura para los activos que tienen valor y nadie debe ser capaz de hacer algo dudoso con dichos activos.

Por ejemplo, que nadie sea capaz de realizar el ataque de doble gasto, cambiar la historia de la Blockchain, o evitar el envío de activos libremente.

El protocolo debe ser resistente a los ataques a corto plazo y el libro mayor de la red debe permanecer inmutable a largo plazo. Cada consenso de la red está diseñado de un modo que se tolera un cierto número de participantes deshonestos, incluso si tienen un poder relativamente grande.



**Token ADA**

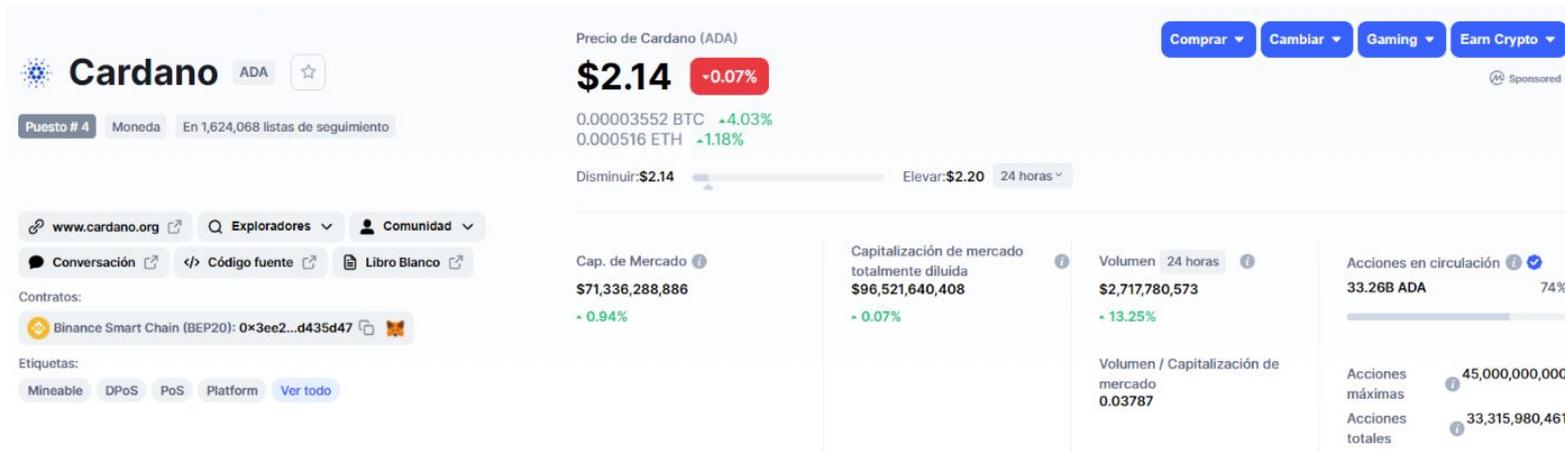
---

# Token ADA

**ADA** es una moneda digital. Cualquier usuario, ubicado en cualquier parte del mundo, puede usar ada como un intercambio seguro de valor, sin necesidad de que un tercero medie en el intercambio.

Cada transacción se registra de forma permanente, segura y transparente en la cadena de bloques de **Cardano**.

Cada titular de ada también tiene una participación en la red cardano. Ada almacenada en una billetera se puede delegar a un grupo de apuestas para ganar recompensas, para participar en el funcionamiento exitoso de la red, o se puede comprometer a un grupo de apuestas para aumentar la probabilidad de que el grupo reciba recompensas.



# Casos de Uso

---

# ¿CUÁLES SON LOS CASOS DE USO DE BLOCKCHAIN EMPRESARIAL?



## TRANSACCIONES GLOBALES

- Procesamiento de pago más rápido
- Costes reducidos
- Mayor eficiencia en las transacciones



## COMERCIO

- Mayor transparencia y confianza para la financiación comercial
- Más control para las manufacturas
- Reducción de papeleo y costo



## SEGURIDAD ALIMENTICIA

- Responsabilidad por la seguridad alimentaria
- Reducir el desperdicio de alimentos
- Deshacerse del fraude alimentario



## CADENA DE SUMINISTRO

- Sistema de registro asegurado con visibilidad de toda la cadena
- Seguimiento de todos los productos
- Detectará rápidamente al personal corrupto



## VENTAS AL POR MENOR

- Ayuda a combatir productos falsificados
- Realiza un seguimiento de todos los bienes de lujo
- Se ocupa de cuestiones de robo



## SERVICIOS GUBERNAMENTALES

- Manera segura de preservar los derechos de los ciudadanos
- Ofrece crecimiento exponencial de la economía
- Digitalización de la identificación ciudadana



## PROPIEDAD INTELECTUAL

- Asegura marcas y patentes de propiedades intelectuales
- Ofrece pago por trabajo patentado
- Reducción del abuso de propiedad intelectual



## ATENCIÓN MÉDICA

- Se deshace de las falsificaciones de drogas
- Seguimiento de la información del paciente
- Agiliza múltiples resultados de pruebas al mismo tiempo



## PETRÓLEO Y GAS

- Pago seguro de fletes y auditoría
- Mejora la eficiencia al calcular rutas de envío
- Ahorra 5% de ingresos con exactitud



## BIENES RAÍCES

- Reduce el coste de la propiedad
- Promueve la propiedad fraccional
- Aumenta la escalabilidad



## HUMANITARISMO

- Asegura que la donación vaya al lugar correcto
- Ofrece transparencia a los ciudadanos donantes
- Promover la equidad y la confianza



## MEDIOS Y ENTRETENIMIENTO

- Mejor valor artístico
- Conecta a artista con un mejor sueldo
- Marketing eficiente en las redes sociales



## VIAJES

- Agilizar el procesamiento de pasajeros
- Promueve la identificación transfronteriza
- Agenda de todos los vuelos con mayor precisión



## SEGUROS

- Reduce el papeleo
- Reclamaciones de seguro más rápidas
- No más explotadores de los consumidores

# Costes asociados

---

## ¿HAY ALGUNOS RETOS DE IMPLEMENTACIÓN?



### INTEROPERABILIDAD

Las tecnologías de las blockchains empresariales actuales carecen de la interoperabilidad entre todas las redes.



### REDES HEREDADAS

Transformar todas las redes heredadas con blockchain puede requerir mucho tiempo y dinero.



### HABILIDADES

No hay una fuerza laboral adecuada con el conjunto de habilidades para desarrollar una nueva tecnología de nivel empresarial.



### METODOLOGÍA

La falta de una metodología adecuada hace que las innovaciones más nuevas estén llenas de defectos.



### ADOPCIÓN MASIVA

En realidad, la adopción masiva aún no es posible, ya que la red se ocupa de una salida más lenta



### DESAFÍOS DE COSTOS

Transformar todo el ecosistema de la red heredada puede requerir más presupuesto.

# Cardano para Desarrolladores

---

# Cardano para Desarrolladores

Máquinas  
Virtuales

The diagram consists of two circles connected by a horizontal line. The left circle is pink and contains the text 'Máquinas Virtuales'. The right circle is dark purple and contains the text 'Contratos Inteligentes'.

Contratos  
Inteligentes

# Máquinas Virtuales

---



**IELE**

**IELE es una máquina virtual dedicada que proporciona una base para el protocolo Cardano blockchain.**

**Ejecuta y verifica contratos inteligentes, además de proporcionar un lenguaje legible para los desarrolladores de blockchain.**

**El testnet IELE proporciona un mejor rendimiento y está basado en registros, lo que significa que puede hacer uso de una gama más amplia de análisis y optimizaciones que una máquina virtual basada en pila como KEVM.**

**La depuración de contratos es más fácil porque IELE tiene un código de error de estado diferente para cada una de las excepciones que pueden ocurrir al ejecutar las funciones dentro de un contrato.**

---



KEVM

**KEVM es una versión mejorada por construcción de la máquina virtual de Ethereum (EVM).**

**Permite a los desarrolladores experimentar con cualquier contrato inteligente que pueda ejecutarse en el EVM y ofrece una seguridad y un rendimiento mejorado.**

---

# Conjunto de habilidades y requisitos

Para usar las redes de prueba KEVM e IELE se requieren las siguientes habilidades:

1. Familiaridad con la escritura de contratos inteligentes en Solidity.
2. Necesitará un conjunto de contratos inteligentes bien definidos para usar en las redes de prueba.
3. Conocimiento avanzado del protocolo de llamada a procedimiento remoto JSON (RPC).
4. No es necesario registrarse para usar.

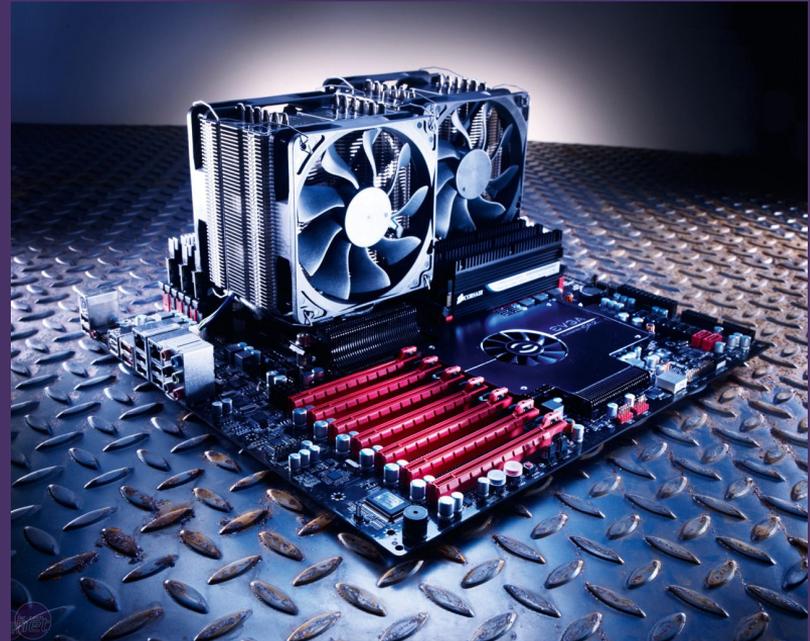


## Para el testnet KEVM:

1. Se necesita una máquina virtual Java (JVM) para ejecutar el cliente. La versión debe ser 1.8.x. El cliente no ha sido probado con JVM 1.9.
2. Salida de 64 bits.
3. Espacio en disco adecuado: se necesitará suficiente espacio para que la cadena de bloques crezca. Se recomienda un SSD de al menos 35G.
4. El cliente Mantis se ha probado ampliamente en pequeñas instancias de Ethereum Classic con 2G de RAM. Esto es suficiente para ejecutar el cliente y el minero.

## Para el testnet IELE:

1. Se necesita una máquina virtual Java (JVM) para construir el cliente, como con el testnet KEVM. La versión debe ser 1.8.x. El cliente no ha sido probado con JVM 1.9.
2. Se recomiendan 230 de espacio en disco y 10 MB de RAM.



# Contratos Inteligentes

---



**PLUTUS**

**Plutus: una plataforma de contrato funcional**

**Plutus proporciona una plataforma de ejecución y un lenguaje de programación funcional que se ejecuta en la capa de liquidación de Cardano y ofrece considerables ventajas de seguridad. Ofrece una manera más fácil y sólida de demostrar que sus contratos inteligentes son correctos y que no encontrarán los problemas encontrados en el diseño anterior del lenguaje de contratos inteligentes.**

**Al usar Plutus puede confiar en la ejecución correcta de sus contratos inteligentes. Ha sido diseñado con tres audiencias principales en mente: desarrolladores, expertos en negocios y academia.**

**Plutus está integrado en Haskell, es familiar para los programadores de Haskell, a la vez que es más fácil de analizar que el propio Haskell.**

---



MARLOWE

**Marlowe: un lenguaje contractual para el mundo financiero**

**Marlowe es un nuevo lenguaje para modelar instrumentos financieros como contratos inteligentes en una cadena de bloques. Ha sido diseñado para personas que son ingenieros de negocios o expertos en la materia en lugar de desarrolladores experimentados.**

**Es un lenguaje simple de dominio específico (DSL) que comprende una pequeña cantidad de poderosos bloques de construcción que pueden ensamblarse en contratos financieros expresivos.**

**Está incrustado en el lenguaje Haskell, que tiene su propio ecosistema establecido y marco de prueba. No necesita experiencia en programación para usar Marlowe y puede explorar sus construcciones financieras con un editor y simulador de contratos basado en navegador.**

---

# **Ecosistema Cardano**

---

# Ecosistema actual de Cardano.

## CARDANO ECOSYSTEM

The infographic displays the Cardano ecosystem across several categories:

- Lending & Borrowing:** MELD, Kitty Party, AADA, nexo, Liqwid, Paribus.
- Launchpad:** OCCZIM, CARD STARTER, Ventup.io, TRUSTPAD, synthesis.
- Synthetic Assets:** wrap assets, Indigo.
- Stablecoin:** STASIS, AgeUSD.
- Derivative:** MATRIXSWAP.
- Insurance:** ensuro.
- Oracle:** CHARLI3, API3, ERGO, WolframAlpha.
- Graph/Query:** fluree, DANDELION, HONEYCOMB, BLOCKFROST.
- DEX (Liquidity):** Polyswap, FIRE, ORION, YaySwap, SundaeSwap, Daemon Exchange, ERGODEX, Vy Finance, adax, CardSwap, Ardana, PHARO, cardax, COINLINK, Minswap, FANANCE, MIRQUR.
- Wallet:** GeroWallet, AdaLite, DAEDALUS, CARDWALLET, Ellipal, infinito wallet, RAY, TREZOR, Atomic Wallet, Medusa, YOROJ, SAMS, ccwallet.io, EXODUS, Guarda Wallet.
- Payment:** Travala.com, SEMPO, revuto, SIRIN LABS, coti, Celsius, metaps+.
- NFT/Gaming:** Bondly, ADAZOO, CNFT.IO, TEBOS, Sushibytes, PlanetPalz, Playermint, IFTY, BitBunny, cryptoknities, WIFF CLUB, Minty, CardanoTales, CRYPTO SUPREME, Tokhun, CryptoDoggies, PunksterArt, RIDOTTO, unsigned\_algorithms, Artano, CHAIN GAMES, CARDANO KIDZ, s-mint, NOVELLIA, CLAY MATEZ, CARDANO GANG, niftyteddy, RETRONFT, NFT DOT, HOUSEOFTOKEN, BoomPopz, CARDANO BITS, Yummi universe, CRYPTOMAYOR, CARDANO COMICS, Cardacity, NFT-DAO, coindodo.io, Burblr.io, DEADPXLZ, SOCCA DOODZ, WAP | NFT, SpaceBudz, Bitcasino.io, cryptomage, TIMETRA TTTERS.
- Other:** S&Mee, diwala, WOO, TESSERACT, TrustSwap, Iagon, Cardanoscan, quidli, SingularityNET, ADApools.org, Algoz, KUBE, CATACT, Ledgeity, HYPERLEDGER, Alpha Impact, venus, CREDMARK, goblin, WORLD MOBILE, CARDANOWALL, NERVOS, tangem.

## Enlaces importantes.

---

- [Librería de IOHK \(Material Técnico\).](#)
- [Foro Cardano en Español \(Mucha Documentación\).](#)
- [Curso Udemy de Marlowe \(Gratis en Ingles\).](#)
- [Curso Udemy de Plutus \(Gratis en Ingles\).](#)
- [Conector dApps de Emurgo.](#)
- [Academia Emurgo \(Muy recomendable pero cuesta dinero\).](#)
- [Guia para crear un Stake Pool \(De un amigo muy bien detallado\).](#)
- [¿Que es Cardano? \(Mucha información sobre ADA\).](#)



Muchas Gracias :)

## Contacto:

**Antonio Sánchez**

[Antoniofsc87@gmail.com](mailto:Antoniofsc87@gmail.com)

**Linkedin:**

<https://www.linkedin.com/in/antonio-blockchain/>

**Telegram: @Etherman**

**Grupo Cardano: @CardanoEsp**

