

# Universidade de Vigo

## **Tecnoloxías de rexistro distribuído e Blockchain**

### **Trabajo tutelado**

Por: Pablo Pérez Paramos y Alexandre Moinelo Rodríguez

## Índice de contenidos

<b>1. Introducción.....</b>	<b>3</b>
a. Motivación.....	3
b. Definición del escenario.....	4
c. Objetivos.....	4
<b>2. Estudio.....</b>	<b>4</b>
a. Análisis de soluciones parecidas.....	4
b. Comparativa con la solución propuesta.....	5
1. Funcionalidades.....	5
2. Ciberseguridad.....	6
<b>3. Análisis.....</b>	<b>7</b>
a. Actores.....	7
b. Requisitos.....	8
c. Justificación del uso de Ethereum.....	9
<b>4. Diseño.....</b>	<b>10</b>
i. Casos de uso.....	10
ii. Diagramas de secuencia.....	11
iii. Arquitectura de comunicaciones.....	14
iv. Modelo de datos.....	15
<b>5. Implementación.....</b>	<b>17</b>
<b>6. Demostración del funcionamiento del sistema.....</b>	<b>17</b>
<b>7. Lean canvas.....</b>	<b>18</b>
<b>8. Aspectos legales.....</b>	<b>19</b>
<b>9. Conclusiones.....</b>	<b>20</b>
<b>10. Líneas futuras.....</b>	<b>21</b>
<b>11. Contribución.....</b>	<b>22</b>
<b>12. Referencias.....</b>	<b>22</b>

## 1. Introducción

La digitalización de la compraventa de entradas ha agilizado el acceso a eventos, pero también ha expuesto al sector a importantes problemas de seguridad y transparencia. La reventa abusiva, la compra masiva mediante bots y la proliferación de entradas falsas constituyen amenazas constantes que perjudican tanto a organizadores como a asistentes.

Ante este escenario, la tecnología blockchain se presenta como una solución sólida, al ofrecer trazabilidad, inmutabilidad y un sistema de verificación abierto para todas las operaciones de ticketing.

En este trabajo se desarrolla un prototipo funcional basado en blockchain en el que cada entrada se representa como un token no fungible (NFT). La propuesta consiste en emitir un NFT único por cada ticket, de forma que el contrato inteligente registra en todo momento su propietario legítimo y su estado (vigente, utilizado, cancelado, etc.). Todas las operaciones quedan registradas en la cadena. Este enfoque permite limitar automáticamente la reventa especulativa y, sobre todo, elimina la posibilidad de duplicación o falsificación de entradas. Con ello se demuestra el potencial de los contratos inteligentes y de los NFTs para redefinir la gestión de eventos y garantizar un proceso de ticketing más seguro, transparente y equitativo para todos.

### a. Motivación

En cuanto a motivaciones/ideas, tenemos el buscar soluciones a la reventa abusiva y los costos desorbitados que esta conlleva. Para resumir las ideas que tenemos en puntos clave tendríamos:

- Falta de transparencia: El comprador no sabe cuántas entradas hay, quién es el vendedor real y si la entrada ya se usó.
- La verificación de entradas tendría que ser algo sencillo y accesible a todo el público.
- La reventa tenga un precio controlado como por ejemplo 20-30% sobre el precio original, para también evitar la especulación.
- Evitar la duplicación de entradas y el “copio el pdf y lo reenvío”.

**b. Definición del escenario**

Una plataforma para entradas digitales de eventos (conciertos, partidos, teatro...). Queremos un pago en ETH (moneda prueba), evitando así la integración con monedas de países y la administración con bancos.

La dirección de la wallet haría referencia a la identidad del usuario y el control en puerta se hace con una app web sencilla que consulta la blockchain y marca el ticket como usado.

**c. Objetivos**

- Gestionar emisión, venta inicial y reventa de entradas.
- Reventa entre usuarios, con precio máximo (porcentaje sobre el precio base).
- Consulta de eventos y entradas del usuario.
- Marcado de entradas como “usadas” al entrar al recinto.

**2. Estudio****a. Análisis de soluciones parecidas**

En los últimos años han surgido diversas plataformas que permiten la compraventa y reventa de entradas para eventos. Entre ellas destacan TicketSwap, StubHub y Ticketmaster, ampliamente utilizadas por los usuarios para intercambiar entradas de forma digital.

TicketSwap es una aplicación enfocada en la reventa segura entre particulares. Su principal aportación es limitar el precio máximo al que un usuario puede revender una entrada, con el objetivo de evitar la especulación. Además, integra algunos mecanismos de verificación para comprobar la autenticidad del ticket antes de completar la transacción. No obstante, toda la validación depende de su propia base de datos interna: el usuario no posee realmente la entrada, sino un registro que TicketSwap confirma o invalida según sus políticas.

StubHub funciona como un gran marketplace donde cualquier usuario puede comprar o vender entradas. A diferencia de TicketSwap, permite fijar precios sin apenas restricciones, lo que facilita la reventa especulativa en eventos con alta demanda. Aunque ofrece garantías al comprador, la gestión de la propiedad y la verificación del ticket continúa siendo centralizada, por lo que la confianza del usuario recae íntegramente en la plataforma.

Ticketmaster, por su parte, actúa como vendedor oficial de la mayoría de grandes eventos. También permite la reventa dentro de su propio sistema, pero bajo condiciones muy controladas: decide cómo, cuándo y a qué precio se puede transferir una entrada. Al igual que las plataformas anteriores, el usuario no posee un identificador único verificable fuera de la aplicación, lo que dificulta la trazabilidad y la auditoría independiente.

En conjunto, estas soluciones han digitalizado el proceso de compra y transferencia de entradas, pero siguen compartiendo una característica esencial: todas dependen de una infraestructura centralizada. Esto implica que la autenticidad, el historial y la propiedad de cada ticket se gestionan desde los servidores de la empresa, y no por el propio usuario. Como consecuencia, persisten problemas como la falta de transparencia, la posibilidad de duplicaciones o fraudes, y la necesidad constante de confiar en un intermediario.

#### **b. Comparativa con la solución propuesta**

La solución propuesta difiere de los sistemas tradicionales al apoyarse en tecnología blockchain y en el uso de tokens no fungibles (NFTs) como representación digital única de cada entrada. Esto elimina la necesidad de confiar en intermediarios y traslada la verificación y la propiedad directamente al usuario, utilizando un contrato inteligente para gestionar todo el ciclo de vida del ticket.

### **1. Funcionalidades**

La principal diferencia funcional radica en que, mientras las plataformas actuales operan como servicios centralizados que otorgan permisos sobre un registro privado, la solución basada en NFTs convierte la entrada en un activo digital único, verificable y sin posibilidad de clonación.

**Tabla 1**

*Comparativa de soluciones tradicionales contra nuestra solución propuesta a aspectos a tener en cuenta para las funcionalidades*

Aspecto	Soluciones tradicionales	Solución propuesta (NFTs)
Propiedad del ticket	Controlada por la plataforma	Propiedad verificable en la blockchain

Autenticidad	Validación centralizada	Prueba criptográfica inmutable
Reventa	Dependiente de políticas de cada plataforma; comisiones altas	Reventa controlada mediante el <i>smart contract</i> , con límites definidos
Transferencia	Gestionada por terceros	Transferencia directa entre usuarios
Trazabilidad	Limitada o no accesible	Historial transparente y público en la blockchain

## 2. Ciberseguridad

El empleo de blockchain aporta integridad, trazabilidad y resistencia a ataques que buscan modificar o replicar entradas. La infraestructura descentralizada elimina el punto único de fallo presente en sistemas tradicionales, fortaleciendo la seguridad tanto para organizadores como para compradores.

**Tabla 2**

*Comparativa de soluciones tradicionales contra nuestra solución propuesta sobre riesgos y su seguridad*

Riesgo	Plataformas actuales	Solución propuesta
Falsificación de entradas	Alta	Prácticamente imposible
Suplantación o pérdida	Dependiente de base de datos y correo electrónico	La identidad se asocia a una clave criptográfica del usuario
Manipulación del inventario	Posible a nivel interno	El <i>smart contract</i> impide alteraciones no autorizadas
Transparencia	Información parcial	Registro completo accesible públicamente en blockchain

### 3. Análisis

El sistema se basa en una arquitectura de tres contratos inteligentes, se usan tres smart contracts porque cada uno aborda un componente distinto del problema: administración de eventos, representación de tickets y gestión económica. La separación mejora seguridad, claridad y modularidad.:

- **EventRegistry**: registro global de eventos (alta de eventos, validadores y estado activo/inactivo).
- **TicketNFT**: contrato ERC-721 responsable de representar cada entrada como NFT y de gestionar su estado.
- **TicketMarket**: contrato de mercado que vende entradas en primaria, gestiona la reventa y valida los tickets en puerta.

#### a. Actores

- **Organizador del evento**

Crea nuevos eventos mediante `EventRegistry.createEvent`. Recibe los ingresos de la venta primaria directamente desde `TicketMarket`. Gestiona validadores mediante `addValidator` y `removeValidator`. Puede activar o desactivar eventos, así como cancelar entradas.

- **Usuario comprador**

Compra entradas en venta primaria (`buyPrimary`) y secundaria (`buyFromResale`). Es propietario del NFT, que representa su entrada en `TicketNFT`. Puede listar su entrada para reventa mediante `listForResale`.

- **Usuario vendedor en reventa**

Lista su entrada en el marketplace a un precio permitido. Puede cancelar su listing mientras no sea comprado (`cancelListing`).

- **Validador**

Actor autorizado por el organizador para marcar tickets como usados. Ejecuta `TicketMarket.markUsed`, que actualiza el estado del NFT en `TicketNFT`.

- **Plataforma - Fee recipient**

Recibe automáticamente la comisión configurada (`feeBasisPoints`) en operaciones de reventa.

- **Smart contract**

En conjunto, los smart contracts actúan como infraestructura lógica descentralizada porque garantizan inmutabilidad, auditoría pública y ejecución determinista y eliminan la necesidad de un intermediario central en la gestión de entradas.

**b. Requisitos**

**i. Requisitos Funcionales**

**RF1 - Registro de eventos.** Un evento debe poder registrarse con nombre, fecha, precio base, máximo de reventa, número total de entradas, CID de metadatos y organizador.

**RF2 - Emisión de entradas.** Las entradas deben emitirse como NFTs únicos desde TicketNFT.mintTicket, llamado exclusivamente por TicketMarket.

**RF3 - Venta primaria.** Los usuarios deben poder comprar entradas mientras: el evento esté activo, haya aforo disponible, el pago sea igual al precio base, no se haya alcanzado el total de entradas.

**RF4 - Reventa regulada.** Un propietario puede listar una entrada si: es válida, el evento sigue activo y no ha pasado, no esté ya listada, el precio esté dentro del límite

**RF5 - Compra en reventa.** El sistema debe manejar pagos entre comprador, vendedor y plataforma. La transferencia del NFT se gestiona mediante safeTransferFrom.

**RF6 - Validación en acceso.** Validadores autorizados pueden marcar un ticket como usado (markUsed), actualizando su estado en TicketNFT.

**RF7 - Estados del ticket.** El NFT puede estar en estado: Valid, Used o Cancelled.

**RF8 - Cancelación automática de listings.** Listados deben invalidarse automáticamente cuando: el ticket se transfiere, caduca el evento o el ticket se marca como usado.

**RF9 - Seguridad de acceso.** Solo TicketMarket puede modificar estados o realizar transferencias críticas del NFT.

**ii. Requisitos No Funcionales**

**RNF1 - Seguridad.** Uso del patrón Checks-Effects-Interactions en pagos. Restricción estricta de acceso mediante onlyOrganizer y onlyMarket.

**RNF2 - Inmutabilidad y transparencia.** Todas las operaciones críticas generan eventos (EventCreated, TicketMinted, TicketListed, TicketSoldSecondary, etc.).

**RNF3 - Desacoplamiento modular.** Los tres contratos tienen roles distintos: gestión de eventos, representación del NFT, lógica económica.



**RNF4 - Prevención del fraude.** No se pueden usar tickets usados o cancelados. No se pueden revender tickets de eventos caducados o inactivos. No se pueden listar tickets ya listados.

**RNF5 - Control de reventa.** El sistema limita automáticamente el precio máximo permitido. Se evita la especulación automática.

**RNF6 - Escalabilidad.** Mappings y structs permiten consultas eficientes.

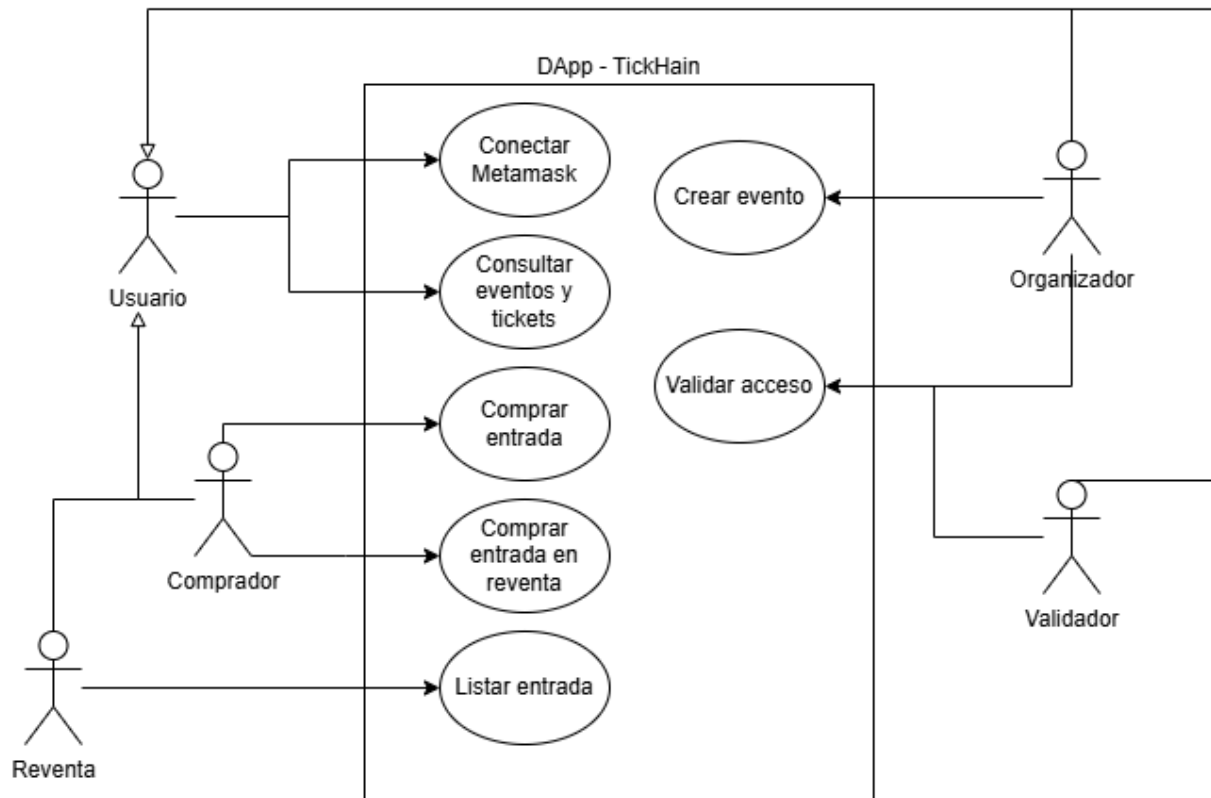
### **c. Justificación del uso de Ethereum**

La elección de Ethereum como plataforma tecnológica se fundamenta en los siguientes aspectos:

- **Estandarización y madurez tecnológica:** Ethereum es la red pionera en contratos inteligentes y soporta estándares ampliamente adoptados, como **ERC-721**, que permite la creación de NFTs interoperables entre aplicaciones, carteras y marketplaces.
- **Descentralización y seguridad:** Su arquitectura distribuida asegura que la información asociada a cada entrada no esté controlada por una única entidad. Esto elimina la posibilidad de manipular, duplicar o revocar tickets sin consentimiento del propietario.
- **Ecosistema y herramientas de desarrollo:** Existen herramientas consolidadas como Remix, Metamask y OpenZeppelin, que permiten desarrollar contratos inteligentes de manera segura y auditable.
- **Interoperabilidad futura:** Las entradas emitidas como NFTs pueden integrarse con otros servicios, como sistemas externos de verificación, mercados secundarios regulados o aplicaciones móviles, sin necesidad de modificar la lógica central del sistema.
- **Cumplimiento legal potencial:** Gracias a la ejecución de reglas directamente en el contrato, Ethereum permite incorporar restricciones normativas —como límites de precio o prohibiciones de reventa— sin depender de intermediarios. Esto facilita su adopción en países donde la regulación del mercado secundario de entradas está siendo reforzada, como Reino Unido, y posiciona la solución para posibles cambios regulatorios en España.

## 4. Diseño

### i. Casos de uso



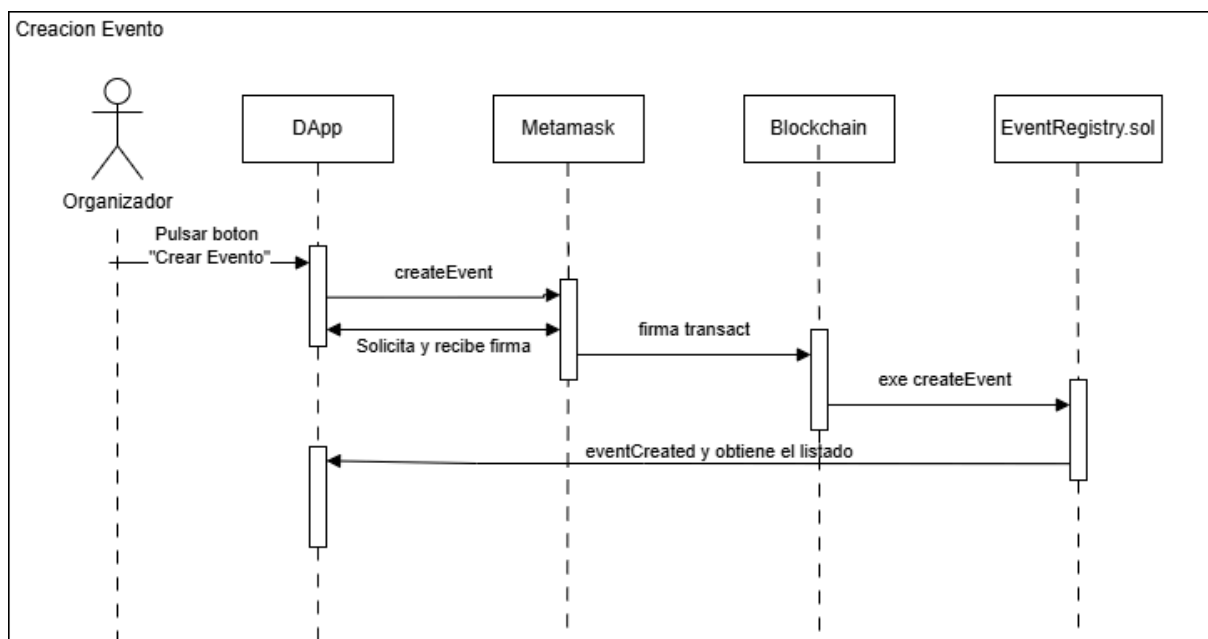
1. **Conectar MetaMask.** Permite que cualquier usuario vincule su wallet con la aplicación. Esta acción habilita el acceso a sus cuentas y permite a la DApp firmar transacciones mediante MetaMask.
2. **Consultar eventos y tickets.** El usuario puede visualizar los eventos activos y los tickets que posee. Este caso de uso permite al usuario navegar por la información del sistema sin necesidad de realizar transacciones.
3. **Comprar entrada.** El comprador adquiere una entrada en venta primaria. Este proceso interactúa con el contrato TicketMarket, que valida el aforo, el estado del evento y genera el NFT asociado mediante TicketNFT.
4. **Comprar entrada en reventa.** El comprador adquiere tickets que otros usuarios han puesto a la venta en el mercado secundario. El sistema gestiona la transferencia del NFT y el reparto de pagos entre el vendedor y la plataforma.

5. **Listar entrada.** El propietario de un ticket puede ponerlo a la venta en el mercado de reventa. El sistema valida que la entrada sea válida, no usada, y que el precio esté dentro de los límites permitidos para esa reventa.
6. **Crear evento.** Caso de uso exclusivo del organizador. Permite registrar un nuevo evento en la blockchain, definiendo sus parámetros (precio, fecha, aforo, metadatos) y dejándolo disponible para la venta de entradas.
7. **Validar acceso.** Caso de uso exclusivo de validadores u organizadores. Permite marcar una entrada como usada en el momento del acceso al evento, evitando su reutilización o reventa posterior.

El diagrama muestra cómo las acciones de los distintos actores convergen en la DApp, que actúa como intermediaria entre ellos y los contratos inteligentes:

- Los usuarios realizan acciones de navegación o conexión sin modificar el estado on-chain.
- Los compradores generan transacciones que interactúan con TicketMarket y TicketNFT.
- Los organizadores realizan acciones administrativas sobre eventos.
- Los validadores interactúan con la parte de control de acceso, actualizando el estado del ticket en la blockchain.

## ii. Diagramas de secuencia



El diagrama ilustra claramente el flujo estándar de una DApp:

- La DApp no firma ni envía transacciones por sí misma.
- MetaMask actúa como intermediario seguro entre usuario y blockchain.
- La blockchain ejecuta el método del contrato inteligente.
- La DApp actualiza su interfaz únicamente tras la confirmación on-chain.

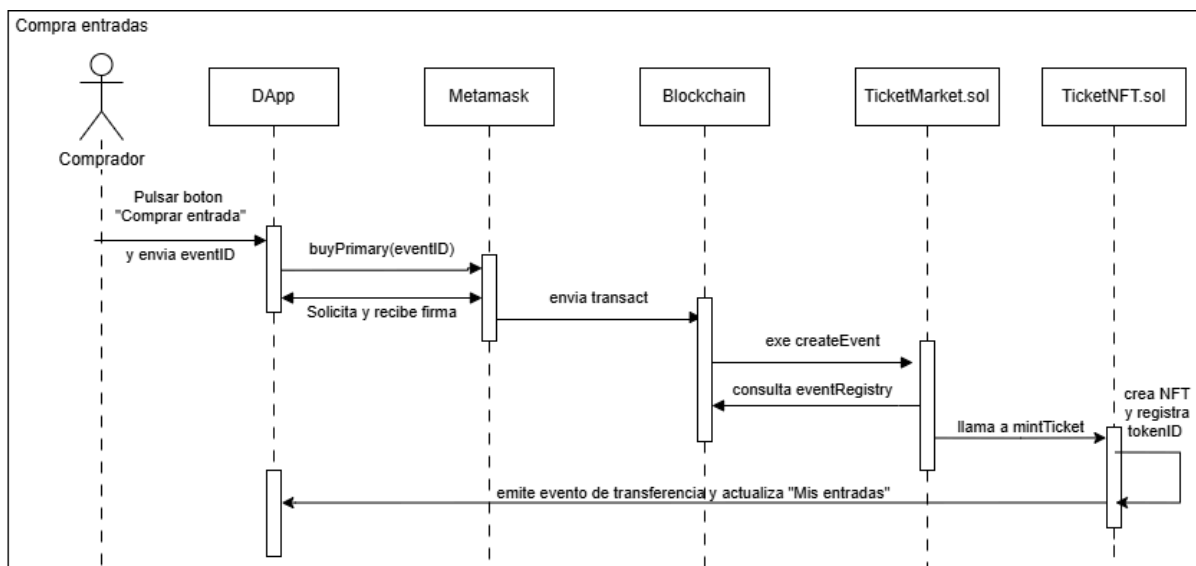


Diagrama de secuencia del proceso de compra de una entrada en la DApp TicketChain. El flujo muestra cómo la solicitud del usuario se firma mediante MetaMask, se ejecuta on-chain a través de TicketMarket y culmina con la creación del NFT correspondiente en TicketNFT. El diagrama de secuencia para la compra de entradas en reventa sería prácticamente igual.

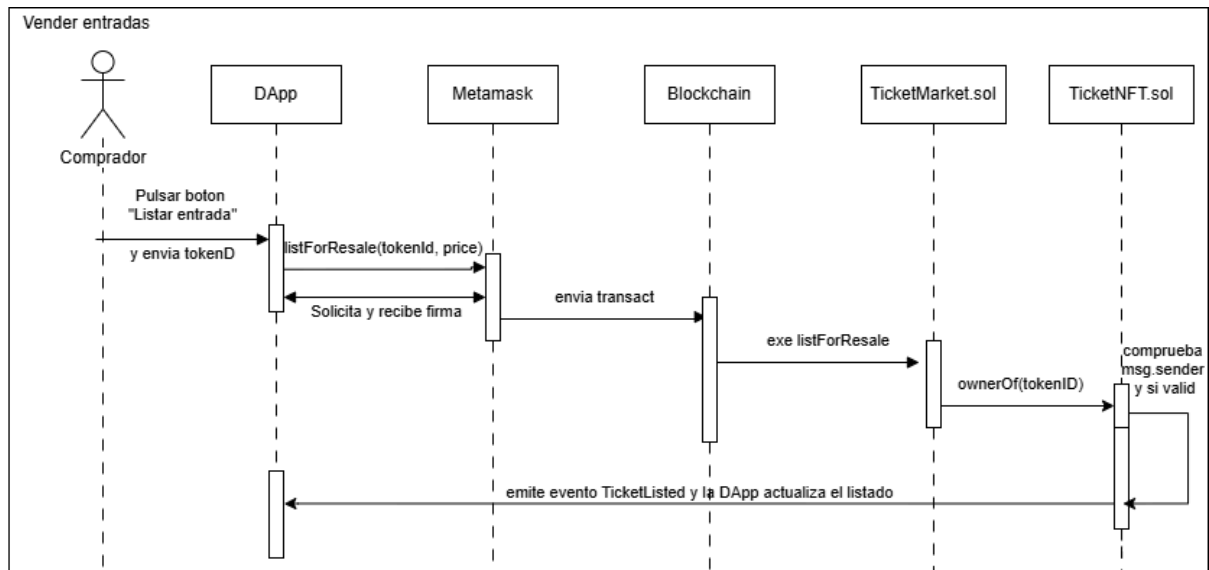
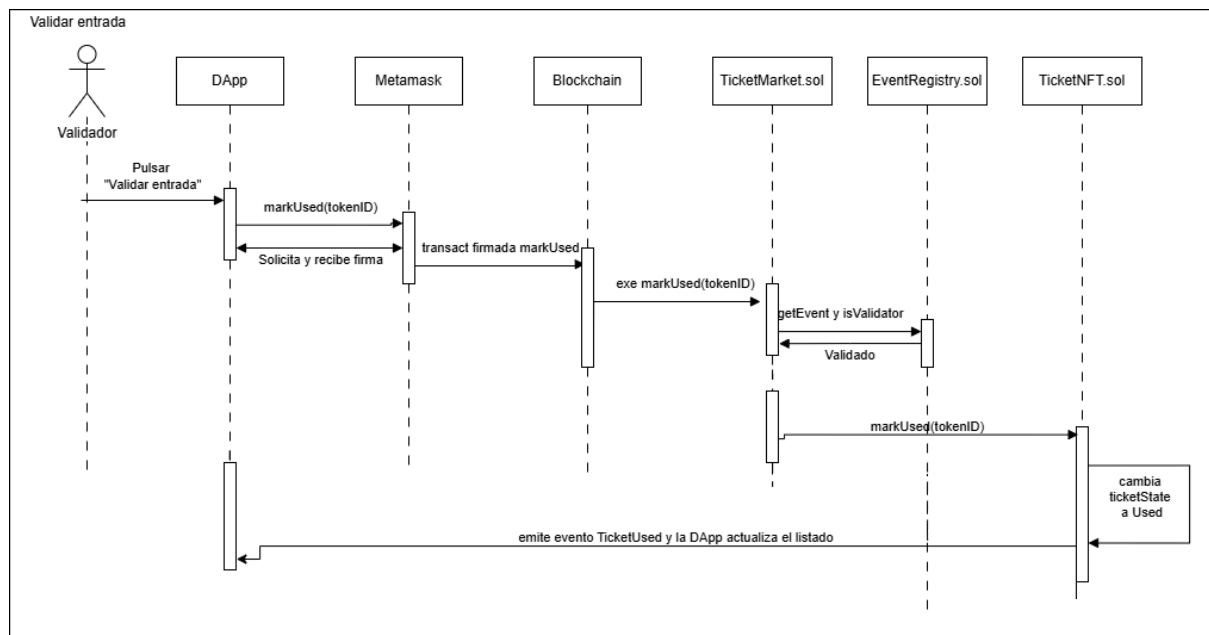


Diagrama de secuencia del proceso de listar una entrada para su venta en el mercado secundario. El comprador inicia la acción desde la DApp, que solicita firma en MetaMask. Una vez enviada, la transacción es ejecutada por el contrato TicketMarket, que verifica la propiedad del ticket en TicketNFT y crea un nuevo listado. Tras emitirse el evento TicketListed, la DApp actualiza la interfaz.



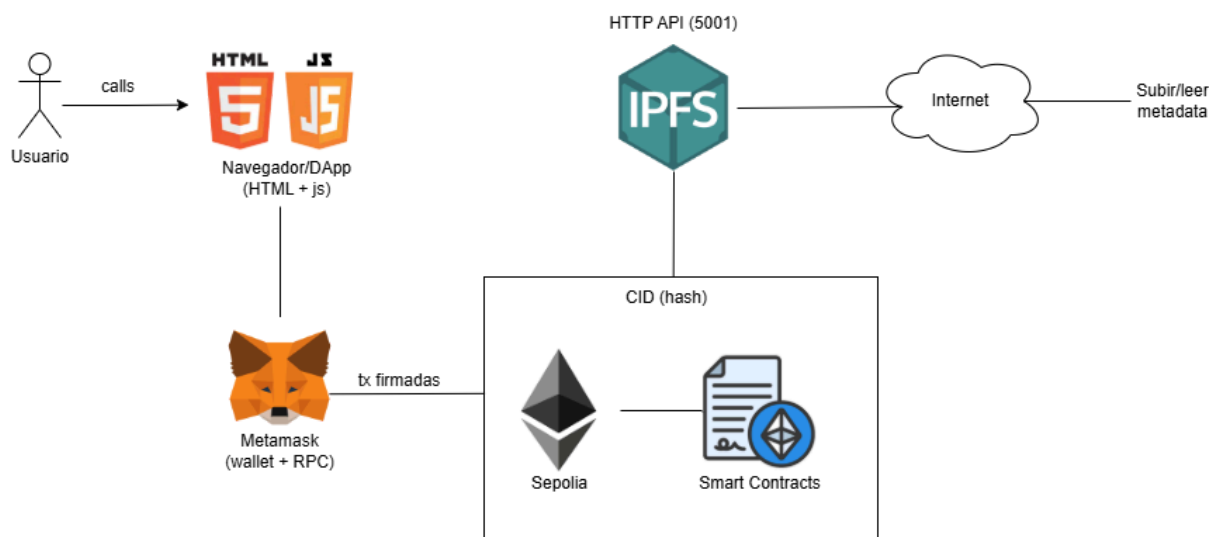
El diagrama representa el flujo completo de validación de un ticket durante el acceso al evento. El proceso comienza cuando el Validador introduce o escanea el tokenId del ticket en la DApp y pulsa el botón “Validar entrada”.

La DApp prepara la llamada al método markUsed(tokenId) del contrato TicketMarket y envía la solicitud de firma a MetaMask. Una vez firmada la transacción, MetaMask la remite a la blockchain para su ejecución.

La red ejecuta la función markUsed dentro del contrato TicketMarket, que primero consulta en EventRegistry si msg.sender es un validador autorizado para el evento asociado al ticket, utilizando las funciones getEvent e isValidator. Si el validador está autorizado y el ticket sigue en estado válido, TicketMarket invoca markUsed(tokenId) en el contrato TicketNFT.

El contrato TicketNFT actualiza el estado del ticket de Valid a Used y emite el evento TicketUsed. Tras la confirmación on-chain de la transacción, la DApp detecta dicho evento y actualiza la interfaz, reflejando que el ticket ha sido validado y ya no puede utilizarse ni revenderse.

### iii. Arquitectura de comunicaciones



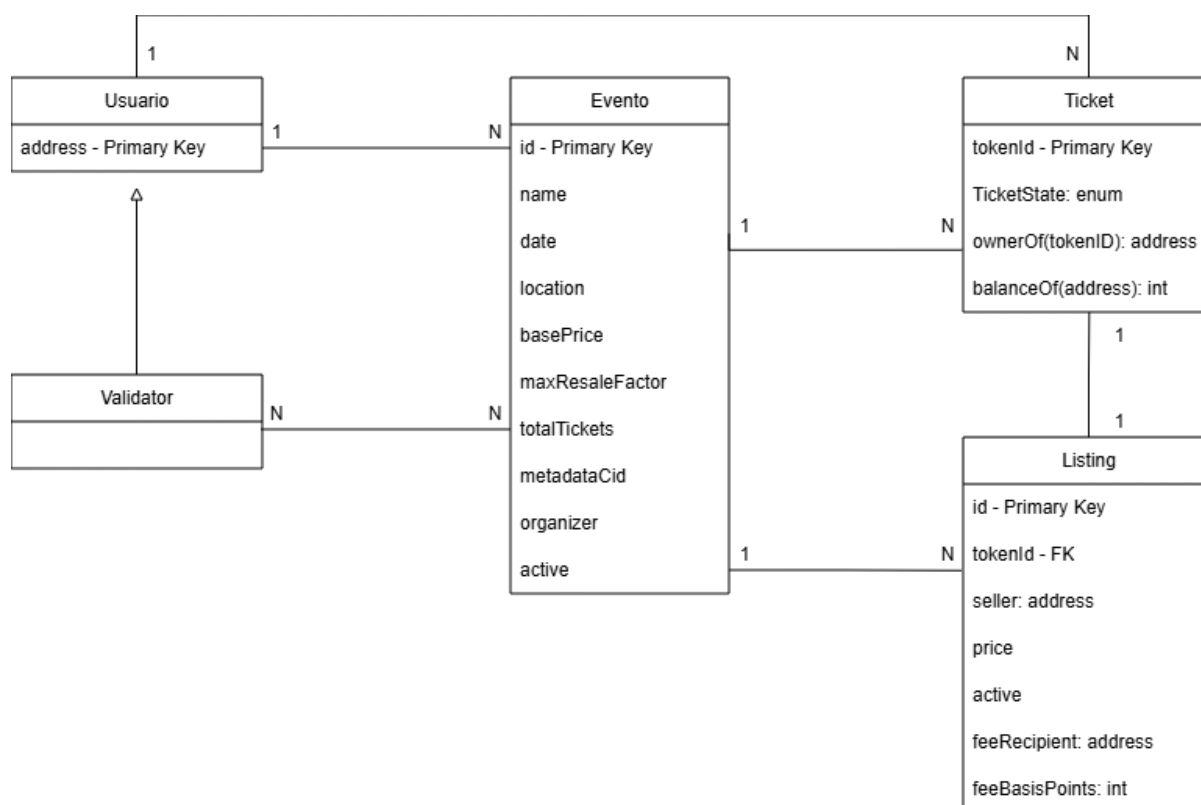
La arquitectura de comunicaciones de TicketChain sigue el modelo típico de una DApp Web3. El usuario interactúa con la aplicación desde el navegador, donde se ejecuta la

interfaz desarrollada en HTML y JavaScript. La DApp utiliza MetaMask como proveedor Web3, que permite obtener la cuenta del usuario, firmar transacciones y enviarlas de forma segura a la red Ethereum Sepolia, donde se ejecutan los contratos inteligentes del sistema (EventRegistry, TicketNFT y TicketMarket). Las operaciones de lectura —como consultar eventos, tickets o listings— se realizan directamente mediante ethers.js sin necesidad de firma.

Además, la arquitectura incorpora un nodo IPFS, desplegado mediante Docker, que se utiliza para almacenar los metadatos de los eventos (por ejemplo, descripciones o imágenes). La DApp sube estos archivos a IPFS y recibe un CID que posteriormente se guarda en los contratos inteligentes como referencia. De este modo, la blockchain almacena únicamente el identificador, mientras que el contenido permanece descentralizado en IPFS.

En conjunto, la arquitectura se basa en la interacción entre el navegador, MetaMask, IPFS y la blockchain, permitiendo un sistema de ticketing sin servidor centralizado, seguro y totalmente transparente.

#### iv. Modelo de datos



El modelo de datos del sistema TicketChain se articula en torno a cuatro entidades principales: Usuario, Evento, Ticket y Listing, junto con la entidad de rol Validator. Estas entidades representan la información esencial gestionada por los contratos inteligentes desplegados en la blockchain.

Un Usuario se identifica mediante su dirección pública y puede desempeñar diferentes roles: organizador de eventos, propietario de tickets, vendedor en el mercado secundario o validador autorizado. Existe una relación 1–N entre Usuario y Evento, ya que un mismo usuario puede crear múltiples eventos, mientras que cada evento tiene un único organizador.

Cada Evento contiene información como nombre, fecha, localización, precio base y aforo, y se relaciona con numerosos Tickets, que se representan mediante tokens ERC-721. La relación Evento–Ticket es de 1–N, ya que cada entrada pertenece a un único evento, pero un evento puede generar muchas entradas.

Los Tickets pueden estar en estado válido, usado o cancelado y pueden ser revendidos. Para ello existe la entidad Listing, que modela los anuncios de reventa. La relación entre Ticket y Listing es 1–0..1, ya que un ticket puede no estar listado o tener un único anuncio activo en el mercado.

Finalmente, la entidad Validator representa la autorización de determinados usuarios para validar entradas en un evento concreto, configurando una relación N–N entre Usuario y Evento, puesto que múltiples validadores pueden operar en un evento y un mismo usuario puede validar distintos eventos.



## 5. Implementación

BC - Trabajo Tutelado - Implementación DApp Tickhain

### DApp Tickets – Venta y reventa controlada

Cuenta conectada: 0x9ca138540fD77Eaf4e82bC51EED9B81c647A5C2B sepolia

[Conectar MetaMask](#)

OK Wallet conectada. Lista para operar.

#### 1. Crear evento (organizador)

Nombre del evento

Concierto XYZ

Fecha y hora del evento

dd/mm/aaaa --:--

Lugar

Madrid, Wizink Center

Precio base (en ETH)

0.05

Factor máximo reventa (ej. 130 = 130%)

130

Número total de entradas

100

Límite de tickets por cartera (0 = sin límite)

4

#### Eventos y aforo

[Actualizar listado](#)

**[ID 0] Partido Madrid - Celta**

Madrid 10/12/2026, 16:00:00

Base: 0.0001 ETH Máx. reventa: 100%

Límite por cartera: 2 por cartera Cooldown: 20 s entre compras

Emitidos: 2/1000 Restantes: 998 Activo

Metadatos IPFS: QmcMBCF2jv...

[Usar este evento](#)

[Ver tickets de reventa](#)

**[ID 1] Partido Celta - Barcelona**

Madrid 2/2/2026, 16:00:00

Base: 0.0001 ETH Máx. reventa: 100%

Límite por cartera: 10 por cartera Cooldown: 1 s entre compras

Emitidos: 3/1000 Restantes: 997 Activo

Metadatos IPFS: QmSx8Nj7U...

[Usar este evento](#)

[Ver tickets de reventa](#)

## 6. Demostración del funcionamiento del sistema

BC - Trabajo Tutelado. Demostración del funcionamiento del sistema

### DApp Tickets – Venta y reventa controlada

Cuenta conectada: 0x9ca138540fD77Eaf4e82bC51EED9B81c647A5C2B sepolia

[Conectar MetaMask](#)

OK Wallet conectada. Lista para operar.

#### 1. Crear evento (organizador)

Nombre del evento

Concierto XYZ

Fecha y hora del evento

dd/mm/aaaa --:--

Lugar

Madrid, Wizink Center

Precio base (en ETH)

0.05

Factor máximo reventa (ej. 130 = 130%)

130

Número total de entradas

100

Límite de tickets por cartera (0 = sin límite)

4

#### Eventos y aforo

[Actualizar listado](#)

**[ID 0] Partido Madrid - Celta**

Madrid 10/12/2026, 16:00:00

Base: 0.0001 ETH Máx. reventa: 100%

Límite por cartera: 2 por cartera Cooldown: 20 s entre compras

Emitidos: 2/1000 Restantes: 998 Activo

Metadatos IPFS: QmcMBCF2jv...

[Usar este evento](#)

[Ver tickets de reventa](#)

**[ID 1] Partido Celta - Barcelona**

Madrid 2/2/2026, 16:00:00

Base: 0.0001 ETH Máx. reventa: 100%

Límite por cartera: 10 por cartera Cooldown: 1 s entre compras

Emitidos: 3/1000 Restantes: 997 Activo

Metadatos IPFS: QmSx8Nj7U...

[Usar este evento](#)

[Ver tickets de reventa](#)

## 7. Lean canvas



## 8. Aspectos legales

El mercado de venta y reventa de entradas presenta diferentes marcos regulatorios según el país, especialmente en relación con prácticas abusivas, especulación y falsificación. En España, aunque la reventa de entradas no está prohibida de forma general, sí existen limitaciones que dependen del tipo de evento, del lugar en que se celebra y de la normativa autonómica o municipal aplicable. Además, en determinados espectáculos culturales y deportivos, se han detectado problemas recurrentes relacionados con la falta de control en los mercados secundarios, la emisión múltiple de tickets digitales y la ausencia de trazabilidad real sobre la propiedad de las entradas.

Estas condiciones han generado un entorno donde los usuarios deben confiar en intermediarios privados y donde la responsabilidad legal recae casi por completo en las plataformas centralizadas, que pueden modificar unilateralmente sus políticas o anular entradas sin intervención del comprador. La legislación española, aunque consciente del problema, todavía no ha desarrollado un marco específico para el control tecnológico de la reventa, lo que abre una oportunidad para soluciones innovadoras que aporten transparencia y seguridad jurídica.

En este sentido, es relevante observar la evolución normativa internacional. El Reino Unido ha aprobado recientemente una regulación que prohíbe la reventa de entradas por encima de su precio original, obligando a las plataformas a verificar la autenticidad de los tickets, limitar las tarifas y controlar que los usuarios no revendan más entradas de las que adquirieron inicialmente. Esta intervención legislativa, motivada por abusos en la reventa y por el encarecimiento artificial del acceso a eventos, marca una tendencia que otros países europeos podrían adoptar en los próximos años.

Este contexto legal enlaza directamente con la propuesta de este proyecto. La solución basada en NFTs permite incorporar las restricciones normativas —presentes y futuras— de manera nativa en el sistema, codificándolas en el propio contrato inteligente. Entre las posibilidades que ofrece se encuentran:

- Restringir automáticamente el precio de reventa
- Trazar el historial completo de cada entrada
- Prohibir transferencias no autorizadas o fraudulentas
- Garantizar que ninguna entrada sea revendida más veces de las permitidas
- Facilitar auditorías independientes sin revelar datos personales

En otras palabras, nuestra arquitectura no solo responde a las necesidades del mercado actual, sino que también se anticipa a posibles cambios regulatorios en España, alineándose con tendencias como la observada en el Reino Unido. Esto dota al sistema de un valor añadido: no depende de una interpretación jurídica posterior, sino que integra el cumplimiento legal dentro del propio diseño técnico

## 9. Conclusiones

El desarrollo de este proyecto ha permitido demostrar que la tecnología blockchain, y en particular el uso de tokens no fungibles (NFTs), constituye una alternativa eficaz y viable para mejorar los sistemas actuales de gestión de entradas para eventos. Frente a los modelos tradicionales, basados en plataformas centralizadas y expuestos a problemas persistentes de fraude, duplicación, especulación y falta de trazabilidad, la propuesta implementada aporta un enfoque técnico que resuelve estas limitaciones desde la base del propio diseño.

En primer lugar, la representación de cada entrada como un NFT único e inmutable garantiza su autenticidad, elimina la posibilidad de falsificación y otorga a los usuarios propiedad real sobre sus tickets. El uso de contratos inteligentes permite gestionar sin necesidad de intermediarios, reduciendo riesgos y aumentando la transparencia del sistema.

Asimismo, el control automatizado de la reventa a través del smart contract ofrece un mecanismo eficaz para limitar la especulación y asegurar que las reglas definidas por el organizador (precio máximo, número de transferencias, estado del ticket) se cumplan necesariamente. Este enfoque resulta especialmente relevante en un contexto donde algunos países, como el Reino Unido, han comenzado a regular de forma estricta la reventa de

entradas. La solución propuesta permite incorporar estas restricciones mediante lógica programada, facilitando el cumplimiento normativo presente y futuro.

La implementación realizada —incluyendo el contrato inteligente, la gestión de eventos, la restricción de reventas y el control de estados del ticket— la arquitectura basada en blockchain proporciona un sistema descentralizado, verificable y resistente a manipulaciones, lo que representa una mejora sustancial en términos de seguridad y confianza, además de demostrar la viabilidad técnica del modelo y sienta las bases para un sistema de ticketing escalable y adaptable. Además, la separación entre la capa de lógica (smart contract) y la interfaz de usuario permite futuras ampliaciones sin comprometer la integridad del sistema.

Finalmente, este proyecto contribuye a la exploración del uso de NFTs en contextos funcionales más allá del arte digital, mostrando su potencial como herramienta para resolver problemas reales de identidad, propiedad y control de acceso. La propuesta abre el camino hacia nuevas líneas de investigación y desarrollo, como la integración con sistemas de validación física, la adopción en eventos de gran escala o la incorporación de mecanismos de privacidad avanzados.

En conjunto, los resultados obtenidos permiten concluir que la solución diseñada no solo es técnicamente sólida, sino que también aporta ventajas diferenciales claras frente a los modelos actuales, posicionándose como una alternativa innovadora, segura y alineada con las tendencias regulatorias emergentes en el sector de los eventos.

## **10. Líneas futuras**

Estas líneas de trabajo refuerzan el potencial del modelo, permiten transformarlo en un producto plenamente funcional y abren la puerta a investigación futura en áreas como seguridad, identidad digital, regulación y experiencia de usuario. Aunque el sistema desarrollado demuestra la viabilidad y el potencial del uso de NFTs para la gestión de entradas digitales, existen diversas líneas de trabajo que podrían ampliarlo, perfeccionarlo o adaptarlo a escenarios reales de mayor escala. Entre las principales líneas futuras destacan:

- Integración con sistemas físicos de control de acceso. Una extensión natural sería integrar el sistema con: lectores físicos de QR/NFC, dispositivos móviles del personal de acceso y sistemas automatizados de tornos o puertas inteligentes.
- Desarrollo de una aplicación móvil. En los días que vivimos una evolución natural de este trabajo sería una aplicación móvil, lo que permitiría una mayor facilidad de uso y un gran aumento del público que usaría nuestro sistema.
- Compatibilidad con múltiples redes blockchain.
- Adaptación a marcos regulatorios futuros. La reciente normativa del Reino Unido anticipa un escenario global con mayor control sobre la reventa.
- Programación avanzada de eventos dinámicos. En un futuro se podría cancelar automáticamente un evento, emitir reembolsos on-chain y actualizar dinámicamente el estado del evento o los precios.

## 11. Contribución

Para explicar cómo hemos distribuido el trabajo y qué ha realizado cada integrante, lo hemos organizado en los siguientes apartados:

- Memoria. Hecho por Pablo Pérez Paramos
- Código. Hecho por Alexandre Moinelo Rodríguez
- Vídeo Promocional. Hecho por ambos.
- Presentación. Hecho por ambos.

## 12. Referencias

[1]

<https://cryptozombies.io/es/course/>

[2]

<https://www.elcorreo.com/culturas/musica/reino-unido-veta-reventa-inflada-entradas-tas-20251125192646-nt.html>

[3]

<https://www.swissinfo.ch/spa/reino-unido-ilegalizar%C3%A1-la-reventa-de-entradas-de-eventos-por-un-precio-mayor-al-original/90390421>

[4]

<https://elpais.com/sociedad/2025-07-01/la-ley-de-consumo-sostenible-pretende-prohibir-que-la-reventa-incremente-el-precio-de-las-entradas-a-conciertos-o-espectaculos.html>

[5]

<https://www.quicknode.com/guides/ethereum-development/nfts/como-crear-y-lanzar-un-erc-721-nft>

[6]

<https://informaticapolo.com/creando-tu-propio-nft-con-un-contrato-inteligente-en-solidity/>

[7]

[https://www.elconfidencial.com/tecnologia/2022-09-07/reventa-entradas-startups-esta-fa-precio-original\\_3484070/](https://www.elconfidencial.com/tecnologia/2022-09-07/reventa-entradas-startups-esta-fa-precio-original_3484070/)

[8]

<https://www.gate.com/es/learn/articles/real-world-use-cases-for-smart-contracts-and-dapps/814>