Universitat
de les Illes Balears

Aplicación basada en Blockchain para una Lotería en línea usando Tokens ERC-20 y ERC-721

Joan Amengual Mesquida

M. Magdalena Payeras Capellà

Macià Mut Puigserver

Contenidos

1. Introducción
2. Contribución
3. Protocolo
4. Implementación
5. Análisis de costes
6. Conclusiones

Introducción

Introducción

- La lotería es una actividad financiera que atrae a usuarios con la esperanza de ganar premios millonarios.
  - Gasto medio de 66,60 euros en décimos de lotería de navidad de 2021.
  - 2.408 millones de euros en premios.

LOTERÍAS Y APUESTAS DEL ESTADO

LOTERÍA NACIONAL

EL GORDO DE LA PRIMITIVA

EUROMILLONES

BONOLOTO

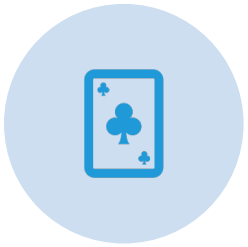
LA QUINIELA

LA PRIMITIVA

La Virgen de la granada.
Fra Angelico.
Museo Nacional del Prado.
Madrid.

Procedimiento

Una empresa de lotería pone en marcha el sistema. Cuenta con la confianza de los participantes.



Las personas interesadas compran los números disponibles.

La empresa de lotería genera algunos números ganadores al azar.

Los usuarios que dispongan de los números ganadores cobran sus premios.

Problemas

- **Métodos Tradicionales**

"¿Está en el suelo?": la imagen más sospechosa de una 'bola' de la Lotería de Navidad

¿FALTÓ TRANSPARECIA?

La eterna polémica de la Lotería de Navidad: el protocolo de las bolas y los bombos

Tras la especulación que causó la reinserción de una de las bolas en 2019, el año siguiente, se pausó el proceso del traslado de bolas en la tolva para reconducir la bola manualmente

Una de las bolas de los números del sorteo de Lotería de Navidad cae al suelo en 2015. (EFE)

Problemas

- **Determinación de ganadores**

Lío con las bolas en un quinto premio: ¿por qué se han acumulado dos en un bombo y se ha cogido "la de abajo"?

Como otros años, la polémica vuelve a rodear a los bombos que reparten los números y premios en la Lotería de Navidad. ¿Qué ha pasado en esta ocasión? Te lo contamos y te explicamos por qué se ha procedido así.

Problemas

- **Integridad de los resultados.**

El décimo puede acabar en los juzgados

El premio 'fantasma' de la Lotería de Navidad: nadie puede cobrar el 59395

Los trabajadores de una empresa de Barcelona escucharon a los Niños de San Ildefonso cantar su décimo, pero cuando fueron a la administración les dijeron que no aparece reflejado en el listado oficial de Loterías.

LOTERÍA DE NAVIDAD

La polémica de la Lotería Navidad: décimos cantados por error que no están en la lista oficial

Problemas

Cobro de los premios

Problemas con los acuerdos verbales

Cuando el premio 'Gordo' acaba en los tribunales... tres sentencias a considerar

La apropiación indebida aparece en numerosas sentencias, pero en 2019 el Supremo no la consideró en un asunto en el que la encargada de comprar los décimos se quedó con el que tenía el premio extraordinario.

LOTERÍA DE NAVIDAD 2021

Cómo cobrar un décimo premiado de la Lotería de Navidad si está roto o estropeado

En caso de que ocurra algún accidente que termine con un décimo de la Lotería de Navidad dañado o que directamente quede hecho añicos, ¿se puede cobrar el premio?

Loterías en Línea

- En 1999, Leason & Sulliv desarrollaron un sistema de lotería en línea centralizada.
- Coste mucho menor que las loterías tradicionales.
- Problemas únicos como falta de seguridad o liquidez.
- Prohibiciones gubernamentales a sistemas de loterías en línea.

Problemas con loterías en línea

Problemas de transparencia en el proceso de selección del ganador así como del dinero recaudado (bote).

Servidores centralizados pueden presentar vulnerabilidades.

El retiro de ganancias es un proceso bastante lento.

Nueva propuesta

Las loterías tradicionales, (físicas o en línea) no favorecen un entorno dinámico, seguro y confiable.

Propuesta: incorporar el uso de la tecnología Blockchain para mejorar estos aspectos mediante la utilización de Smart Contracts.

Ventajas del uso de Blockchain

- Rapidez y dinamismo.
- Confianza en reglas inmutables.
- Conocimiento del bote recaudado.
- Reducción de pérdidas, destrucción o manipulación de información.
- Pago de premios instantáneo.

Smart Contract

Los Smart Contracts nos permiten definir un conjunto de reglas a cumplir para llevar a cabo las operaciones de:

- compra y venta de boletos de lotería
- generación de un ganador de forma aleatoria

beneficioso para aumentar la seguridad,

confianza a los usuarios de la aleatoriedad de los resultados.

Contribución

Objetivo:

solución a las carencias actuales de las loterías tradicionales.	nuevo sistema descentralizado, veloz, sin intermediarios, seguro y respectuoso con la privacidad de los usuarios.

Mejoras propuestas:

Información inmutable y púbica del bote recaudado.	Aumentar la confianza sobre los resultados ganadores.	Disponer de un sistema dinámico y automatizado.	Ofrecer privacidad sobre las identidades de los usuarios.	Evitar intermediarios ygenerar ganadores de forma transparente.

Protocolo

Protocolo

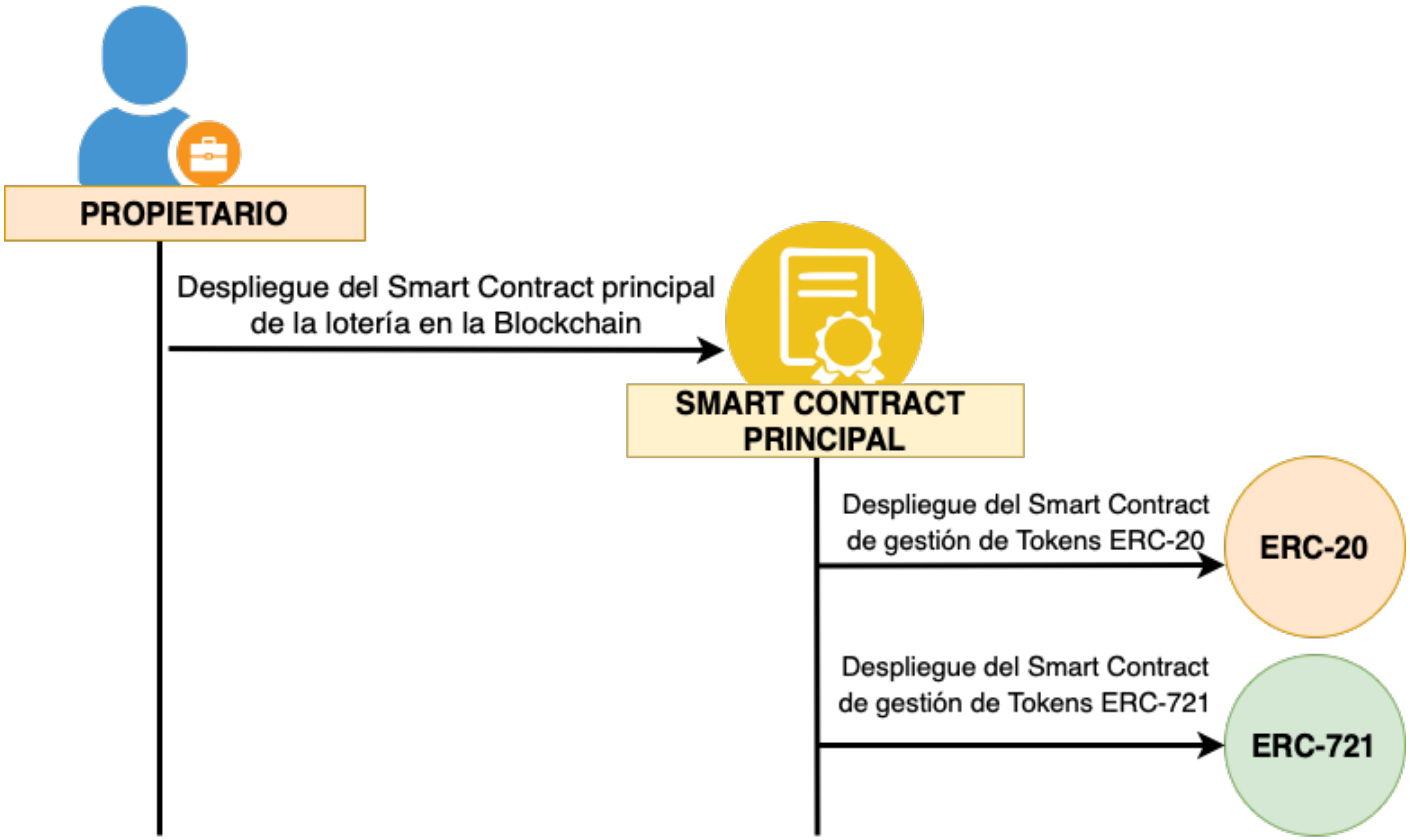
Tokens ERC-20 para la realización de compras de boletos.

Los usuarios deben tener la propiedad absoluta sobre sus boletos.

Confianza en que estos boletos son únicos y no existen dos iguales.

Uso del token ERC-721, Non-Fungible Token (NFT).

Smart Contract Principal



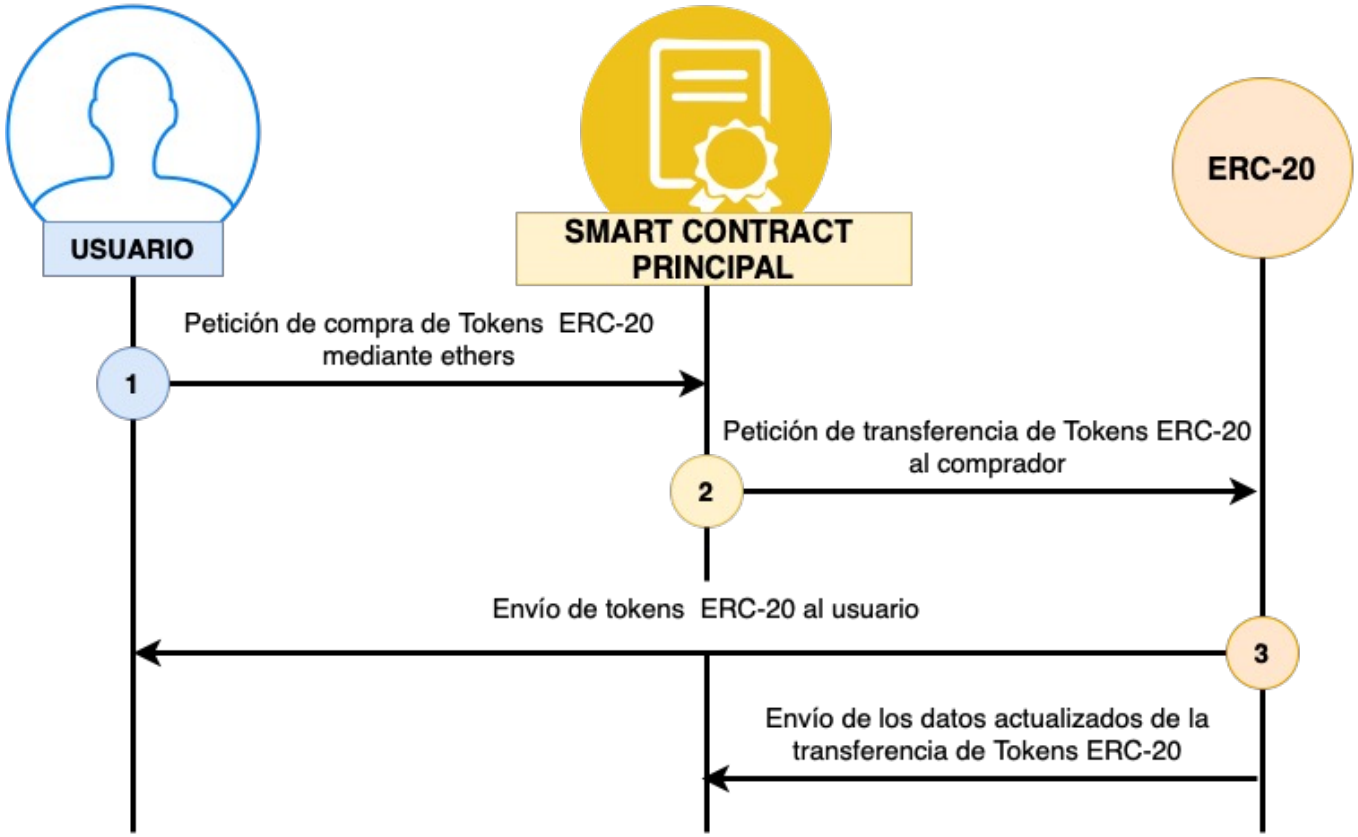
FASES

GESTIÓN DE TOKENS ERC-20

GESTIÓN DE BOLETOS DE LOTERÍA

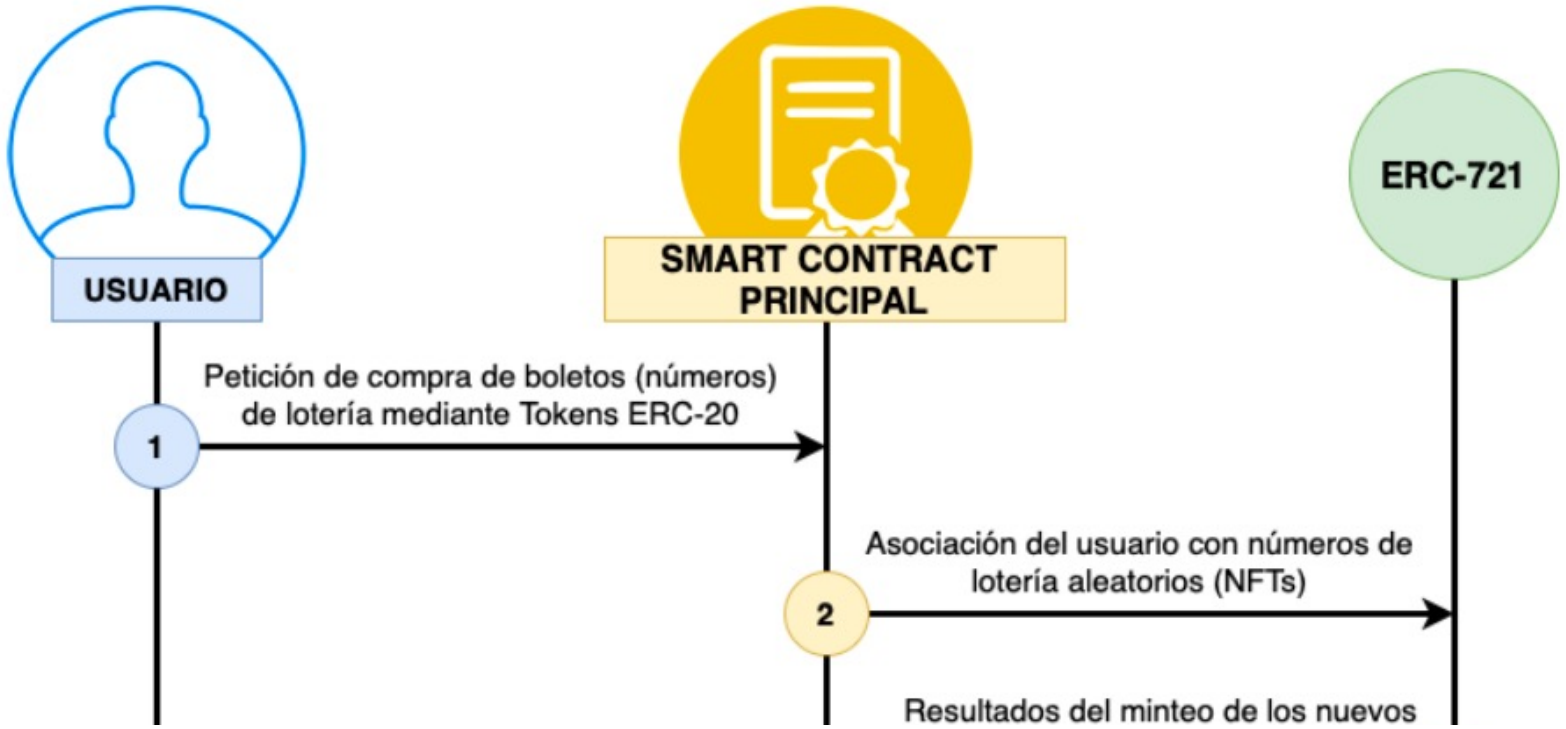
EMISIÓN DE LOS PREMIOS

Gestión de Tokens ERC-20



Gestión de Boletos de Lotería

Los boletos son números generados aleatoriamente en un rango preestablecido.
Cada número se corresponde a un token NFT, asignando la propiedad única al comprador.



Emisión de los premios

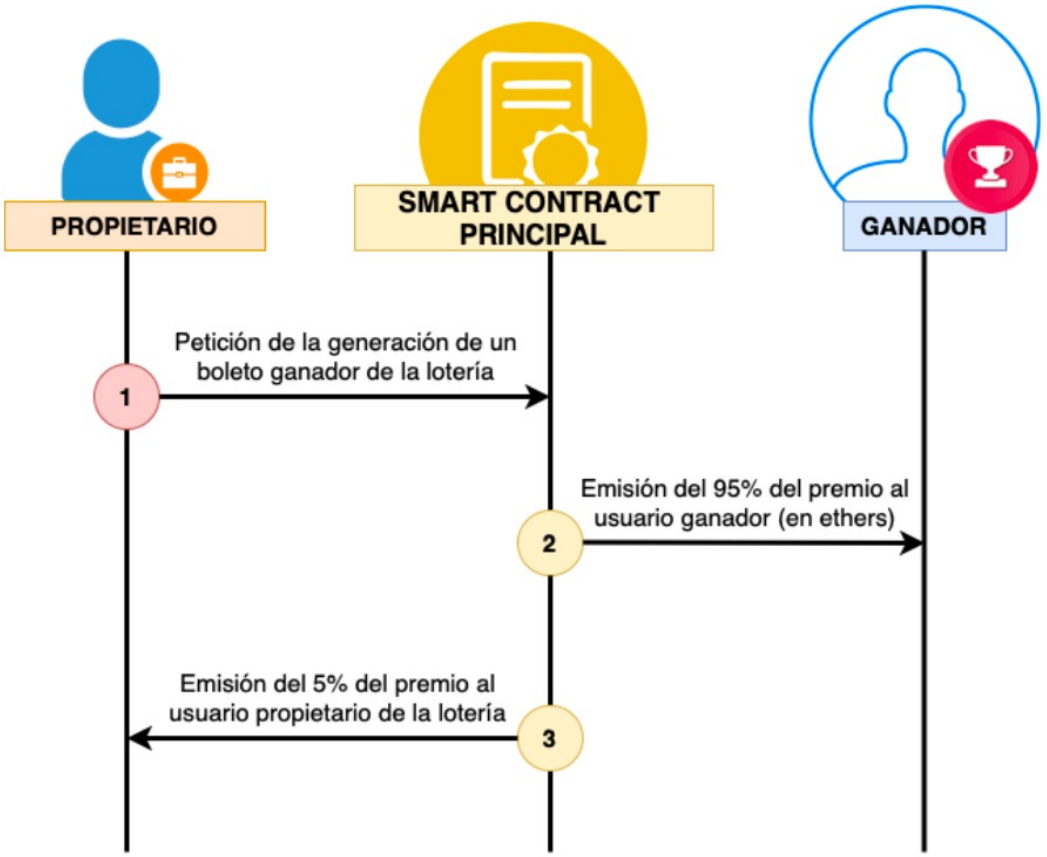
Elegir de forma aleatoria un número de boleto.

Hash SHA256. Una de las entradas es la marca de tiempo (*timestamp*) del último bloque de la Blockchain, buscando así tener más aleatoriedad en la salida.

Emisión de los premios.

Premio del ganador: 95 % del bote recogido. Recompensa al propietario del proyecto de la lotería: 5 % del bote recogido.

Emisión de los premios



Implementación

Programación de los Smart Contracts

Implementación de la interfície del frontend

Actores

- **Owner de la Lotería (dirección que despliega el proyecto):**
  0x6E302fdE93Fc3b33Be3651735D8416e7A5C4EB3a
- **Usuario A (comprador de tickets de lotería):**
  0x9fAac8E7b96e9f3D259e125874241E9783e94912
- **Usuario B (comprador de tickets de lotería):**
  0xCFb3a40D1D1461F34393c030442eb9c9155282bF
- **Dirección del Smart Contract (Ganache):**
  0xbB6BB60Ba7Ae88e348FB77e5c7aa7662CFA4d0D1

Interfaz de la gestión de los tokens ERC-20, que nos servirán para comprar boletos de lotería

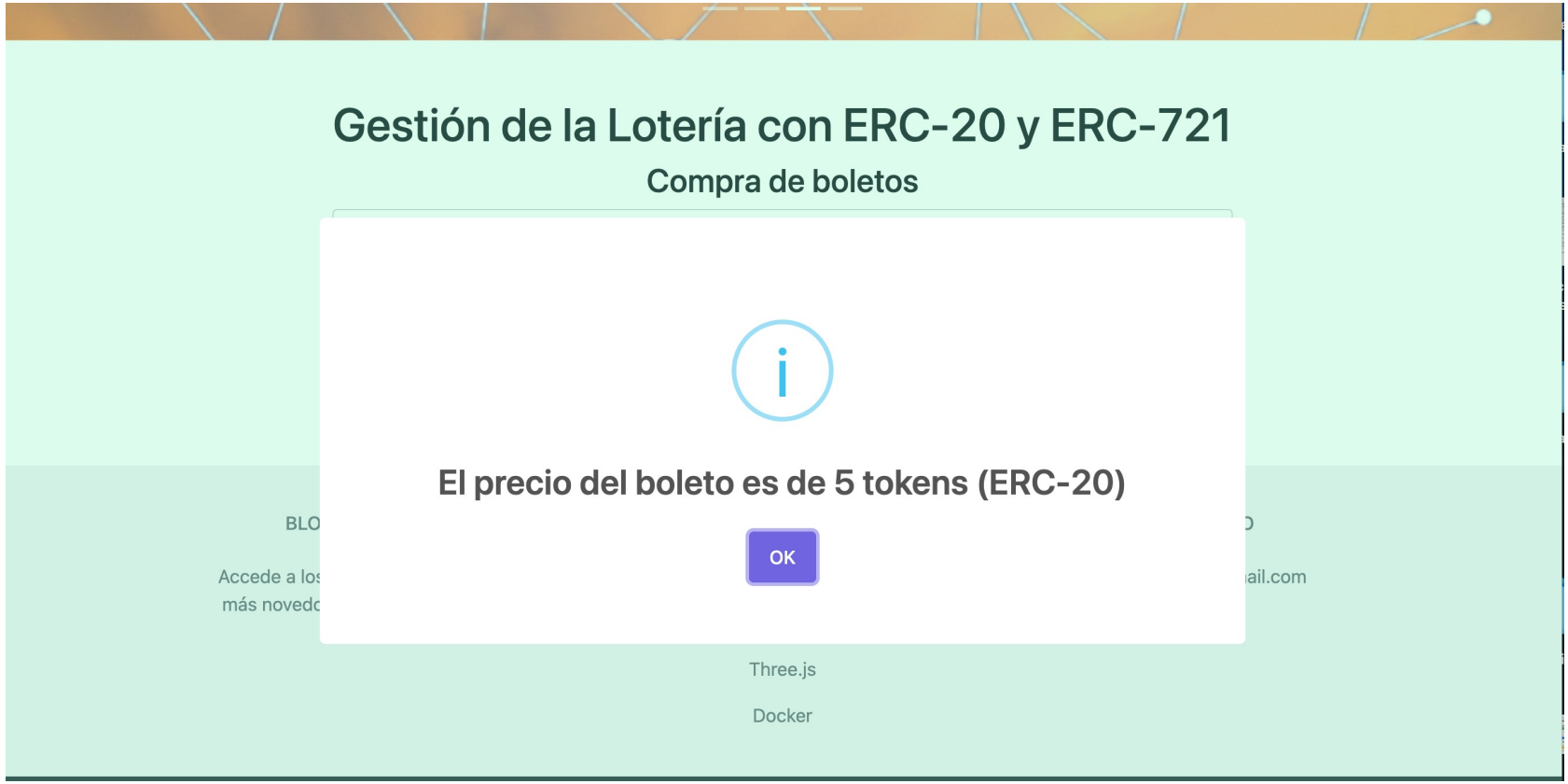
El usuario A compra 50 tokens ERC-20 para posteriormente comprar boletos de lotería con estos tokens ERC-20

El usuario B compra 120 tokens ERC-20 para posteriormente comprar boletos de lotería con estos tokens ERC-20

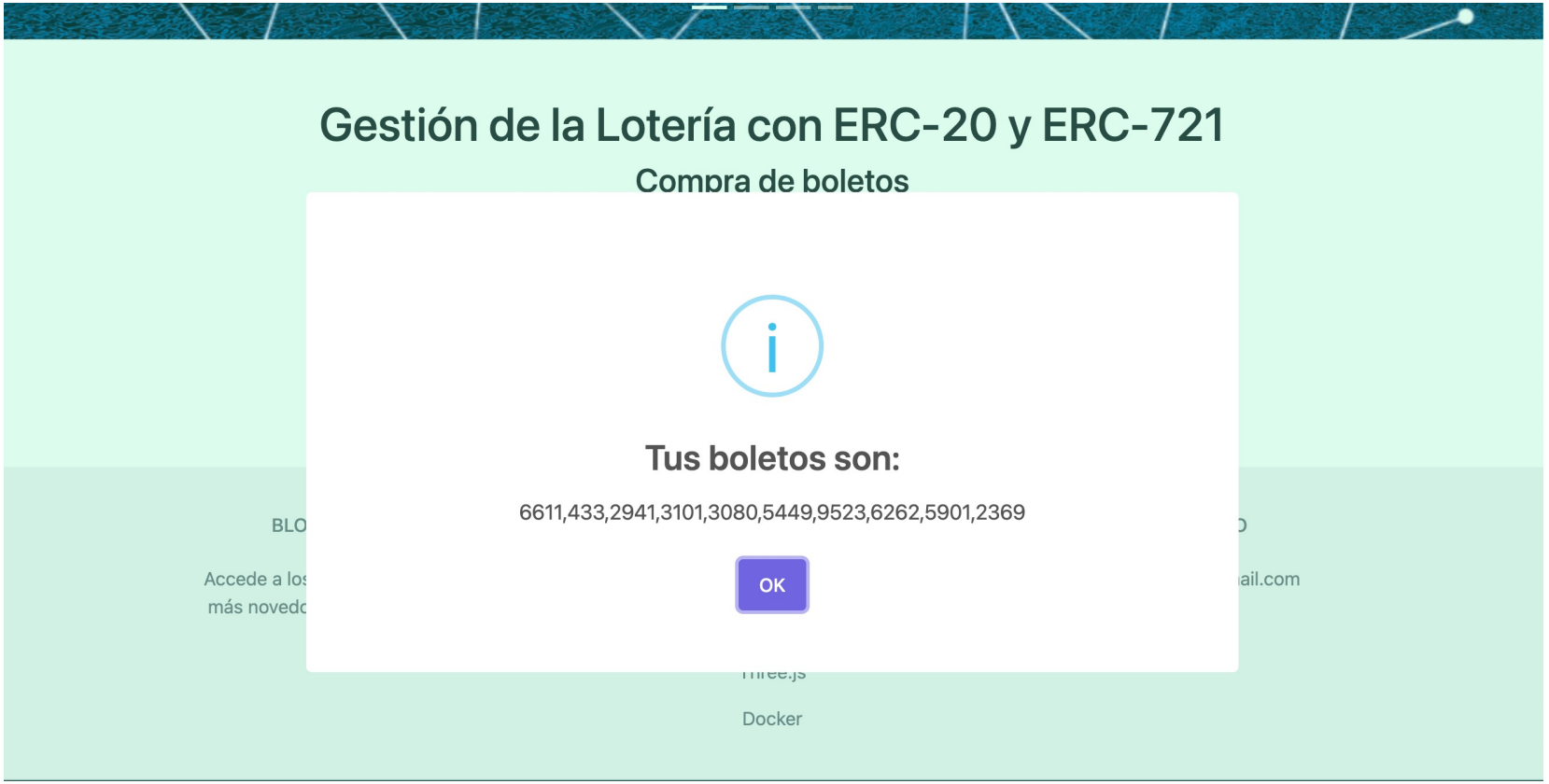
Con el usuario A y B se han comprado un total de 170 tokens ERC-20.
Esta imagen muestra el total de tokens ERC-20 restantes en el proyecto

Fondos recolectados en total por el proyecto de lotería almacenados en el Smart Contract

El precio de un boleto de lotería es de 5 Tokens ERC-20.

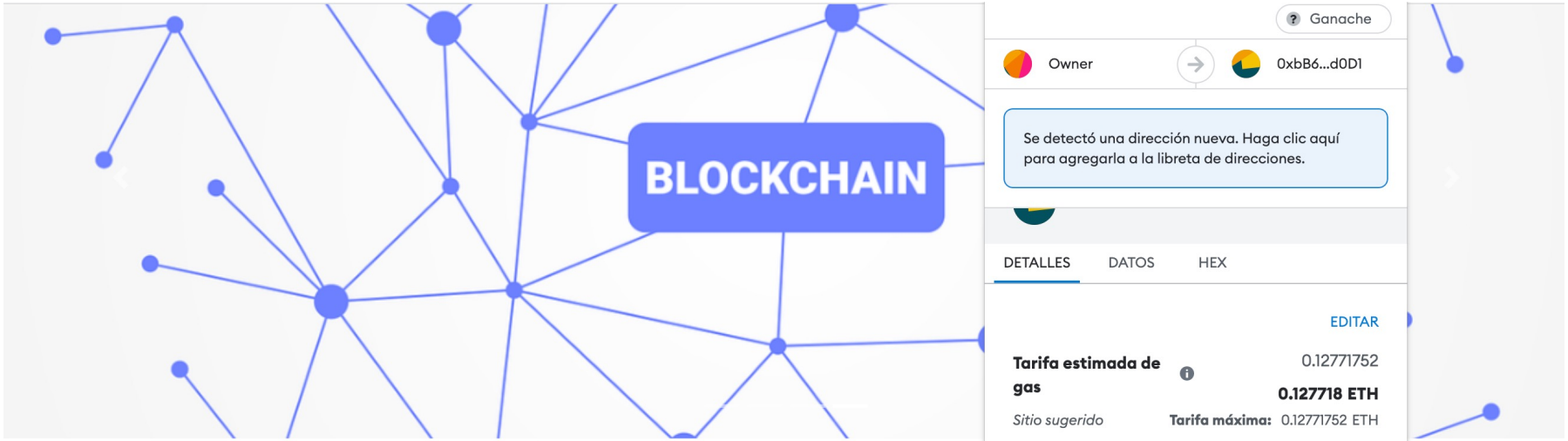


Número de los boletos de la lotería comprados por el usuario A. En total ha comprado 10 boletos mediante sus 50 tokens ERC-20.



Número de los boletos de la lotería comprados por el usuario B. En total ha comprado 24 boletos mediante sus 120 tokens ERC-20.

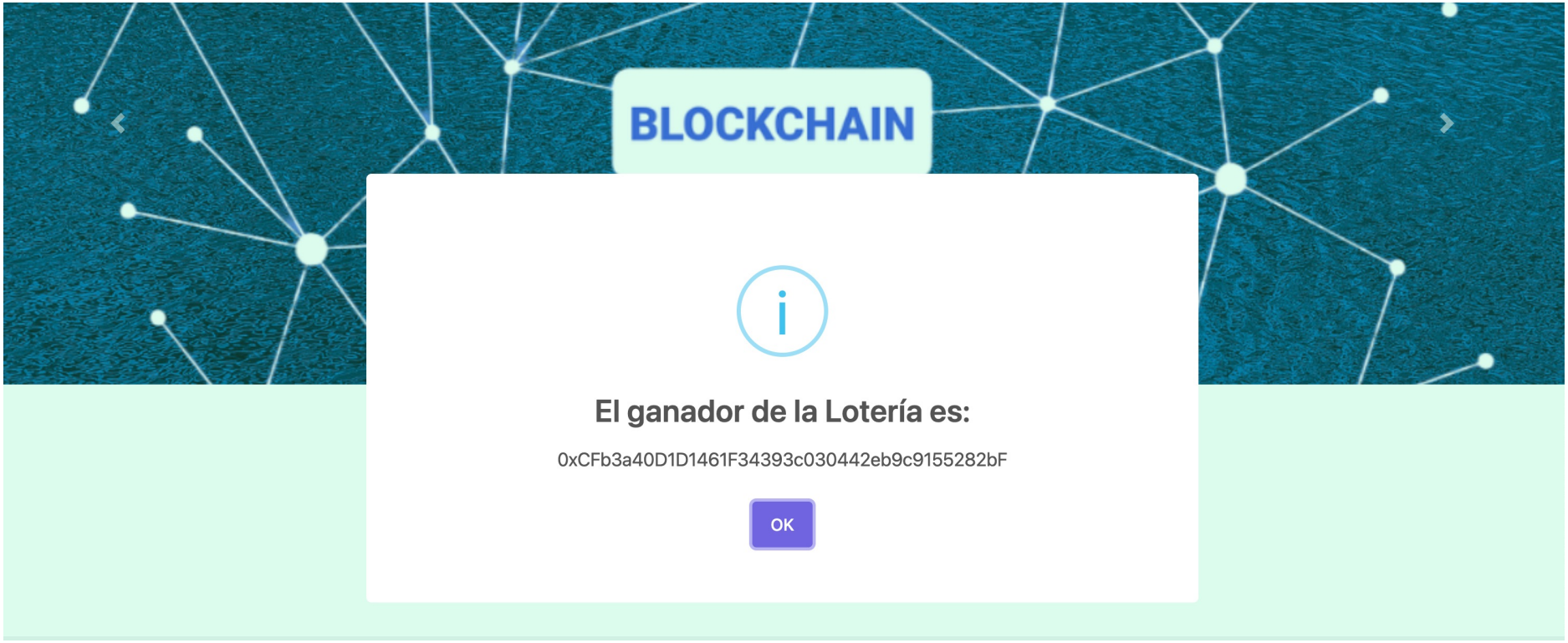
El owner genera el ganador de la lotería



El ganador de la lotería es la dirección:

0xCFb3a40D1D1461F34393c030442eb9c9155282bF

que equivale al usuario B, el cual recibe el premio de la lotería en su wallet



Análisis de Costes

Funciones del Smart Contract	Blockchain			
	Polygon		Binance Smart Chain	
	MATIC	USD	BNB	USD
Creación del Smart Contract	0.0142	0.00839	0.0570263	16.98
Compra de tokens ERC-20	0.001605	0.000948	0.006326	1.884
Devolución de tokens	0.000165	0.000097	0.000705	0.21
Compra de boletos	0.000895	0.00052	0.003354	0.999
Generación del ganador	0.0002652	0.000156	0.001002	0.2984

Conclusiones

Se ha realizado la implementación de un protocolo de lotería mediante el uso de la tecnología blockchain permitiendo ofrecer unas características únicas a los usuarios como:

- Transparencia
- Mayor seguridad en la información
- Velocidad de operación

Disponemos de un proyecto de lotería con información descentralizada y almacenada de forma segura mediante las operaciones reguladas por Smart Contracts.

Universitat
de les Illes Balears

Aplicación basada en Blockchain para una Lotería en línea usando Tokens ERC-20 y ERC-721

Joan Amengual Mesquida

M. Magdalena Payeras Capellà

Macià Mut Puigserver