



TECNOLÓGICO
NACIONAL DE MÉXICO



INSTITUTO TECNOLÓGICO DE MÉXICO, CAMPUS VERACRUZ

DAPP DINOCOIN
REPORTE

REYES AVILA KARLA
ALUMNO

E17021901
NUMERO DE CONTROL

INGENIERIA EN SISTEMAS COMPUTACIONALES
CARRERA

TRANSACCIONES CON BLOCKCHAIN
MATERIA

GENARO MENDEZ LOPEZ
CATEDRATICO

18:00-19:00 PM
HORARIO

ÍNDICE

INTRODUCCIÓN	2
Descripción.....	2
Objetivo	2
Objetivos Específicos	2
Tecnología Blockchain	3
¿Qué es un Smart Contract?.....	4
Alcance	4
Proceso de consulta de saldo	5
Proceso de transferencia de pago.....	5
Proceso de intercambio de puntos	5
Token ERC20 “DinoCoin”	6
Función totalsupply	6
Función balanceOf.....	6
Función allowance	6
Función approve	7
Función TransferFrom	7
Función Transfer.....	7
Función SendPoints.....	8
Función ExchangePoints	8
Evidencia en Remix.....	9
Conclusión.....	11
Repositorio Github	11

INTRODUCCIÓN

La tecnología blockchain “cadena de bloques”, es un procedimiento de validación y almacenamiento seguro y descentralizado de la información basado en el consenso de todas las partes intervinientes. Apareció en la primera década del siglo XXI asociado a la criptomoneda. Aunque los aspectos técnicos son bastante complejos, es posible explicar su funcionamiento y estructura de forma simple. Supongamos que se realiza una serie de transacciones de información entre agentes que forman parte de una red, y que quedan registradas en un sistema informático interconectado. Cuando se acumula una cantidad suficiente de registros se pone en marcha un sistema de verificación en el que opera un cierto conjunto de los actores de la red. En el momento en que todos estos agentes dan su visto bueno -esta verificación puede ser automáticamente ejecutada por programas de ordenador específicos, si el tipo de información lo permite-, se cierra un bloque, lo que significa que toda la información que se ha producido hasta ese instante queda almacenada y su acceso encriptado. Pero este proceso no se produce sólo en un servidor concreto, sino que queda registrado en todos los ordenadores de la red. En ese momento se empieza a registrar la información que formará parte del siguiente bloque, que se puede cerrar además asignando una clave que depende de los contenidos y también de la clave del bloque anterior, reforzando de esta forma la inmutabilidad del registro.

Descripción

La página web hace la simulación de comprar una imagen o figura digital de dinosaurios en 2d. dentro de la misma se logran hacer consultas del saldo que se tiene en la cuenta usada para la misma.

Se tiene la moneda “DinoCoin” que es el utilizado para la transferencia del pago o la transferencia de intercambio de puntos.

Objetivo

Establecer la factibilidad de los Smart contracts en la compraventa de imágenes o figuras.

Objetivos Específicos

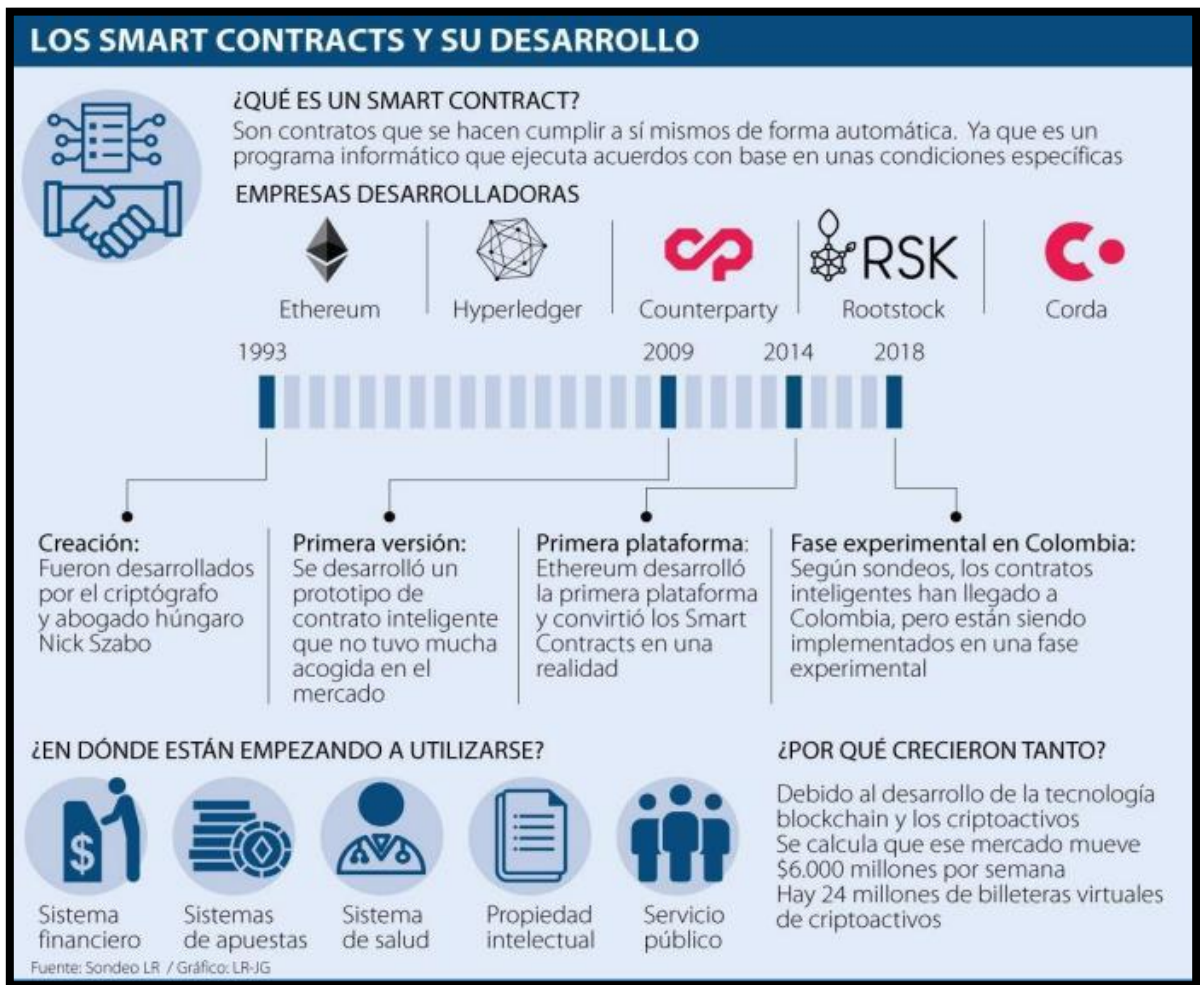
- Describir la tecnología de Smart contracts, analizando los avances y cambios que presentará este proceso.
- Analizar la viabilidad técnica y jurídica para la implementación de los smart contracts en la compraventa.

Tecnología Blockchain

En el año 2009 Satoshi Nakamoto lanzo el proyecto de la Criptomoneda Bitcoin junto con blockchain que se convirtió en la primera cadena de bloques en ejecutar la transacción, esta primera cadena obtuvo el nombre del Bloque génesis. El objetivo del proyecto Bitcoin no era otro que garantizar la seguridad, la transparencia y la privacidad entre los usuarios

El avance tecnológico de los últimos tiempos ha permitido la utilización de los medios electrónicos para realizar todo tipo de actividades económicas, incluyendo la posibilidad de efectuar pagos por medios electrónicos y sin la necesidad de utilizar elementos físicos como lo son las monedas y billetes de curso legal que tradicionalmente conocemos; sin embargo, también existen medios de pago que si bien actualmente no son reconocidos en forma oficial en México, como es el caso de las llamadas criptomonedas, lo cierto es que ello no ha impedido que cada vez más personas se interesen por adquirir este tipo de instrumentos digitales, lo que se advierte del hecho de que un 12% de la población adulta mexicana posee alguna criptomoneda, por lo que el país se ubica como la novena nación con la mayor tasa de posesión de estos instrumentos en todo el mundo.

¿Qué es un Smart Contract?

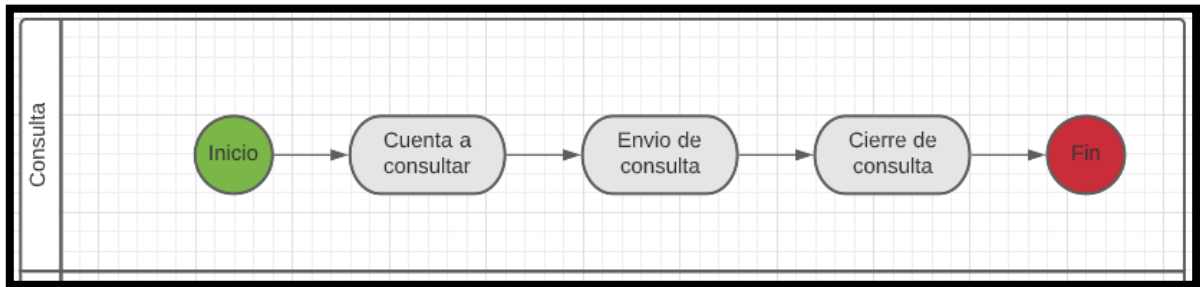


Alcance

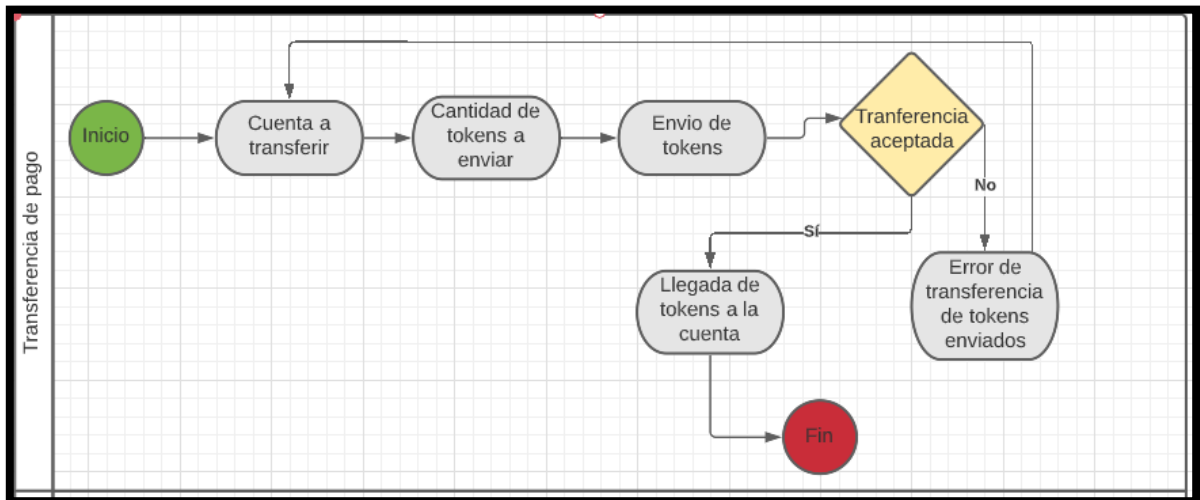
Con la página web se pretende utilizar los medios electrónicos para realizar todo tipo de actividades económicas, incluyendo la posibilidad de efectuar pagos por medio de las wallets y los tipos de monedas, igual para realizar un intercambio de bienes y servicios.

De igual forma se quiere mejorar la calidad de la página web, y la de las imágenes volviéndolas animadas y en 3d, con la intención de llamar la atención de más personas.

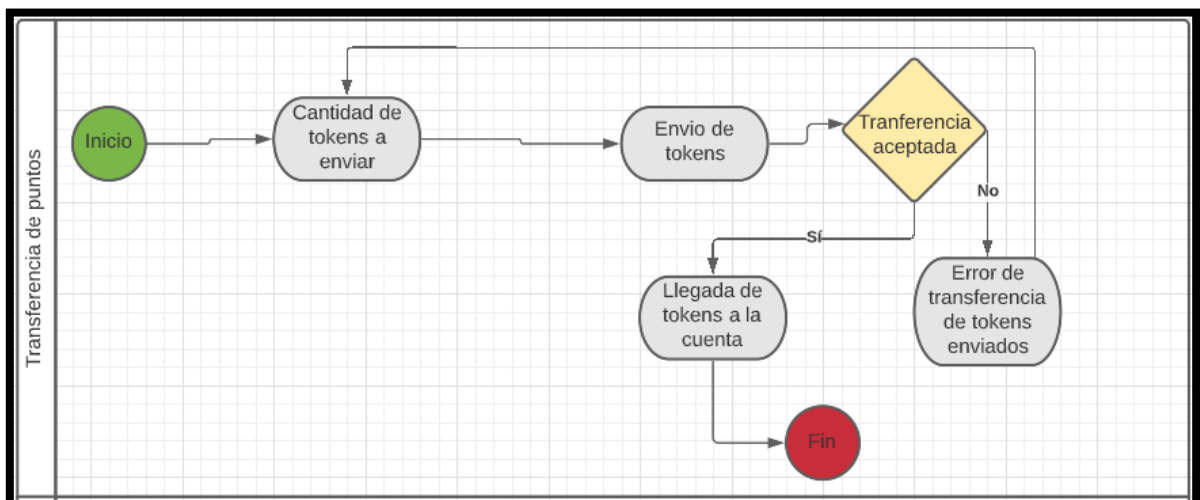
Proceso de consulta de saldo



Proceso de transferencia de pago



Proceso de intercambio de puntos



Token ERC20 “DinoCoin”

Dentro del constructor se tiene establecido el nombre, símbolo, decimales y cantidad en existencia, dichas variables se establecieron previamente por lo que aquí solo se despliegan los datos colocados.

```
constructor() public {  
    name = "MyFirstToken";  
    symbol = "DinoCoin";  
    decimals = 0;  
    _totalSupply = 10000000;  
}
```

Función totalsupply

Cuando es llamada por un usuario, la función superior retorna la oferta total de tokens que el contrato contiene.

```
function totalSupply() public view returns (uint) {  
    return _totalSupply - balances[address(0)];  
}
```

Función balanceOf

Cuando se llama, dicha función retorna el balance de tokens que dicha dirección posee. Las cuentas son públicas, por lo que podrás solicitar el balance de cualquier usuario siempre y cuando conozcas la dirección.

```
function balanceOf(address tokenOwner) public view returns (uint balance) {  
    return balances[tokenOwner];  
}
```

Función allowance

La función allowance puede ser empleada junto con approve. Cuando le has otorgado permiso a un contrato para que gestione tus tokens, puedes utilizar esta función para comprobar cuántos de ellos puede retirar todavía. Por ejemplo, si tu suscripción ha utilizado doce de los veinte tokens que has aprobado, llamar a la función allowance debería retornar un valor total de ocho.

```
function allowance(address tokenOwner, address spender) public view returns (uint remaining) {  
    return allowed[tokenOwner][spender];  
}
```

Función approve

es otra función útil desde un punto de vista de la programabilidad. Con dicha función, puedes limitar el número de tokens que un smart contract puede retirar de tu balance. Sin ella, corres el riesgo de un mal funcionamiento del contrato (o de que sea explotado) y robe todos tus fondos.

```
function approve(address spender, uint tokens) public returns (bool success) {
    allowed[msg.sender][spender] = tokens;
    emit Approval(msg.sender, spender, tokens);
    return true;
}
```

Función TransferFrom

La función transferFrom es una alternativa cómoda a transfer que permite un poco más de programabilidad en las aplicaciones descentralizadas. Igual que transfer, se emplea para mover tokens, pero éstos no han de pertenecer necesariamente a la persona que llama al contrato.

```
function transferFrom(address from, address to, uint tokens) public returns (bool success) {
    balances[from] = safeSub(balances[from], tokens);
    allowed[from][msg.sender] = safeSub(allowed[from][msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    emit Transfer(from, to, tokens);
    return true;
}
```

Función Transfer

transfiere tokens de un usuario a otro de manera idónea. En esta, proporcionas la dirección a la que quieres hacer el envío y la cantidad a transferir.

```
function transfer(address to, uint tokens) public returns (bool success) {
    balances[msg.sender] = safeSub(balances[msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    emit Transfer(msg.sender, to, tokens);
    return true;
}
```


Función SendPoints

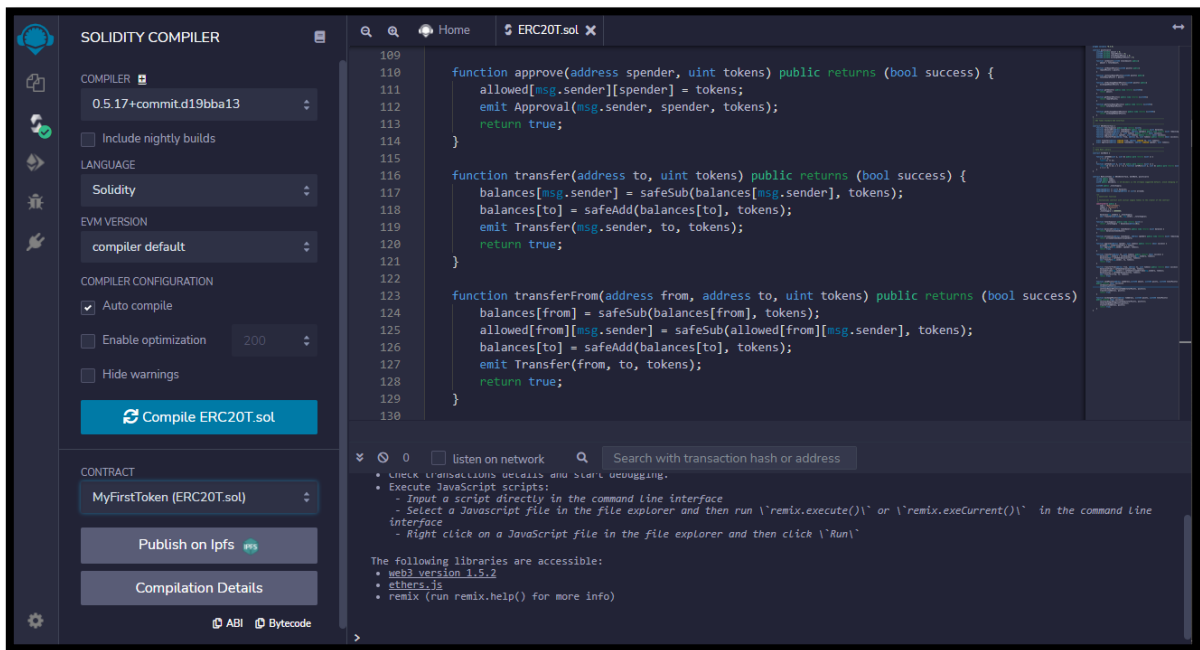
```
function sendPoints(address toAddress,uint256 amount, uint256 points, uint256 totalPoints)
public returns (bool success){
    setAmount(amount);
    setRewardPoints(points);
    setTotalRewardPoints(safeAdd(totalPoints, points));
    transfer(toAddress, points);
    return true;
}
```

Función ExchangePoints

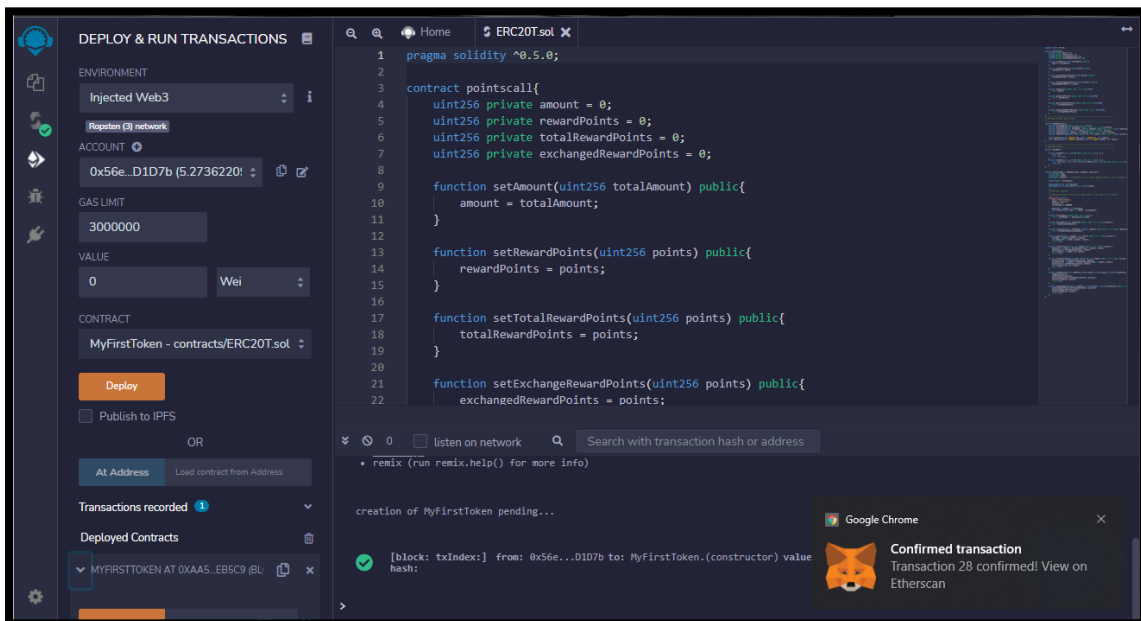
```
function exchangePoints(address toAddress, uint256 points, uint256 totalPoints)
public returns (bool success){
    setTotalRewardPoints(safeSub(totalPoints, points));
    setExchangeRewardPoints(points);
    transfer(toAddress, points);
    return true;
}
```

Evidencia en Remix

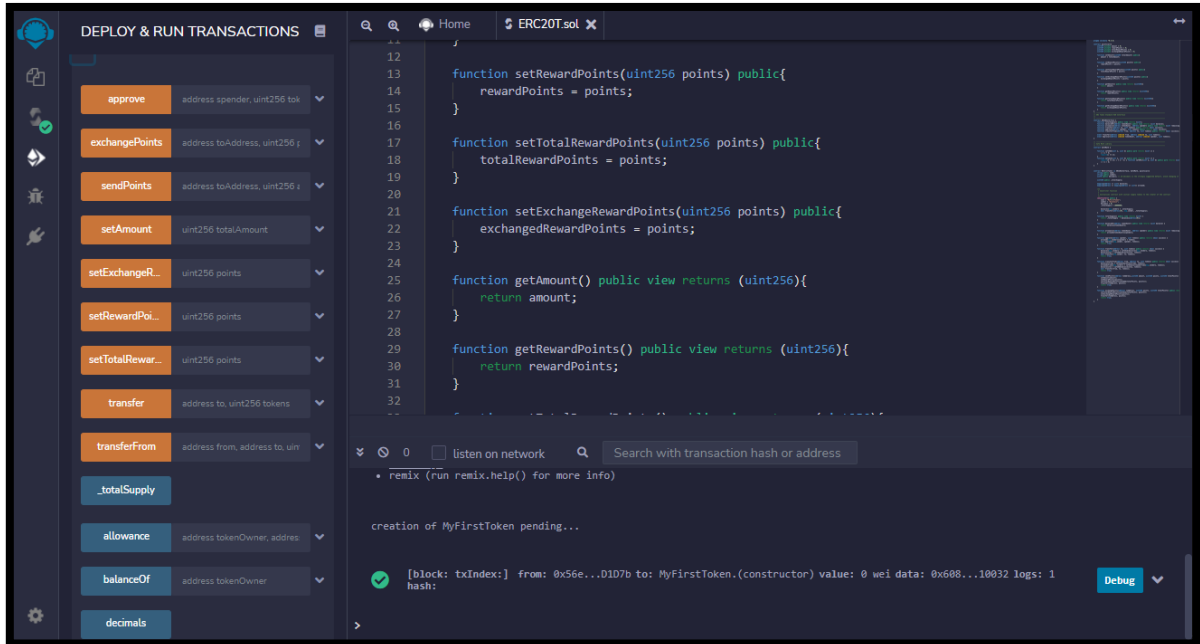
Dentro de remix se compilo el Smart contract para así obtener el abi y posterior a eso obtener el número de nuestro contrato.



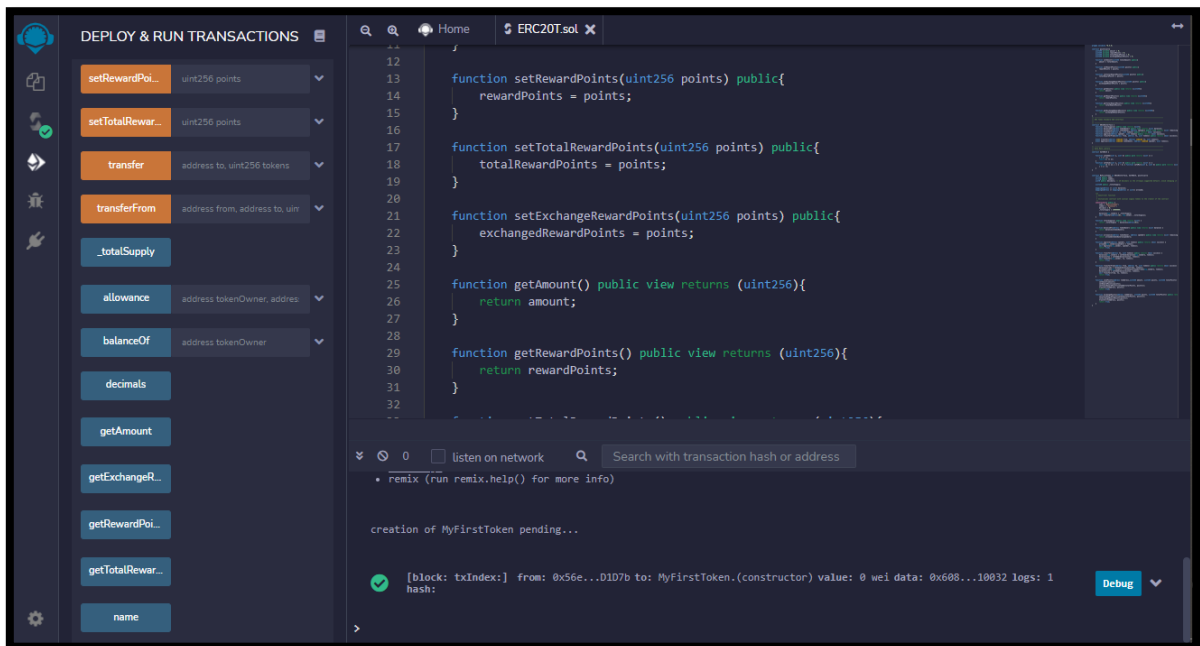
Corriendo nuestro Smart contract podemos observar la lista que se despliega del lado izquierdo una vez que se dio clic en “Deploy”.



Las funciones de color naranja son las de escritura.



Mientras que las funciones de color azul son las de lectura.



Como se observará en la página desplegada se hizo uso de la función de lectura de BalanceOf () para la consulta de saldo. Se utilizó TransferFrom () para la tranferencia de tokens de una cuenta a otra. Y por último se hizo uso de ExchangePoints () para la transferencia de puntos al Smart contract.

Conclusión

En la actualidad, las iniciativas para la gestión de la comunicación científica basadas en blockchain son muchas y muy variadas. La mayor parte de ellas están dirigidas a aspectos particulares, como la gestión de bases de datos garantizando la conservación y la fiabilidad de sus registros basándose en el consenso, o el almacenamiento de artículos de investigación, mediante la publicación de revistas o en repositorios. También se pueden encontrar interesantes y novedosas propuestas de sistemas de revisión por pares basados en esta tecnología, pero que, en general, podrían desarrollarse por otros medios. Las nuevas iniciativas que parecen más innovadoras son las plataformas de gestión integral de la investigación científica, que proponen sistemas organizativos completamente nuevos, basados algunos en el uso de criptomonedas.

Repositorio Github: <https://github.com/karla456/DAppDinoCoin.git>