



Proyecto Final 2022

APLICACIÓN DESCENTRALIZADA

ETHEREUM

ADMINISTRADOR DE FONDOS COMUNES

Comisión: 503 ISI

Integrantes:

Romaniuk, Federico Nicolás - 45882 (federico.roma98@gmail.com)

Miño, Julián Mateo - 46206 (julian.m.mino@gmail.com)

Raselli, Gianfranco - 46472 (gianrase4@gmail.com)

RESUMEN

El sistema de administración de fondos comunes será una aplicación descentralizada que correrá en la cadena de bloques (Blockchain) de Ethereum.

La función principal de la aplicación será llevar un registro de los activos (Ether) que las diferentes cuentas de Ethereum ponen a disposición para una causa común. Los mismos serán gestionados mediante contratos inteligentes (Smart Contracts), que son porciones de código que residen en la cadena de bloques mediante los cuales se implementará la lógica de negocio.

La aplicación contará con distintos usos prácticos, la misma permitirá gestionar los fondos de donaciones, pensiones, seguros, campañas de inversiones, entre varios usos más que se le puede asignar en el uso diario de cada grupo de personas.

Por lo tanto, el alcance funcional comprende desde la creación de un fondo común (una instancia de un contrato inteligente) por parte de uno o más administradores del mismo, pasando por la inserción de fondos (Ether) en dicho smart contract por parte de las diferentes cuentas/personas interesadas, hasta la utilización de dichos recursos (lo cual tendrá diferentes usos dependiendo del tipo de fondo; es decir, sea un fondo de donaciones, seguro, campañas de inversión, entre otros).

Nuestro sistema contará con las ventajas de una Blockchain pública:

- **Descentralización:** Un blockchain descentralizado añade una red de igual a igual a las características de seguridad existentes típicas de las bases de datos de un blockchain. Los miembros de esta red no tienen que confiar ni conocerse entre sí, sino que cada integrante obtiene una copia del mismo registro de contabilidad del blockchain.
- **Transparencia:** La transparencia en blockchain se consigue publicando las reglas con las que se define el funcionamiento de blockchain. Esto se logra haciendo público el código del software necesario para ejecutar blockchain y generando una comunidad de nodos y desarrolladores que siguen este principio de transparencia.
- **Inmutabilidad:** Ningún participante puede cambiar o falsificar una transacción una vez grabada en el libro mayor compartido. Si el registro de una transacción incluye un error, se debe añadir una nueva transacción para revertir el error, pero ambas transacciones serán visibles.

- Privacidad: Las direcciones blockchain no están ligadas a las identidades de las personas que controlan cada una de las direcciones blockchain. Para poder operar en un blockchain público es necesario disponer del par de claves pública y privada que permiten controlar la dirección blockchain.
- Trazabilidad: Blockchain permite recorrer la cadena de bloques y trazar todas las operaciones que se han realizado sobre una determinada dirección; o retroceder en el tiempo y revisar las transacciones que se hicieron en una fecha determinada explorando todos los bloques generados en la fecha indicada.

Nuestro sistema seguirá los principios de dicha tecnología para escribir las reglas lógicas sobre las que se regirá nuestra aplicación. Las mismas serán escritas en un lenguaje de alto nivel orientado a contratos denominado Solidity. Dicha lógica de negocio interactúa con una aplicación Web/Mobile desacoplada, donde el frontend (cliente) interactúa con la API (servidor) utilizando la tecnología Web3, lo que permitirá también escalar dicha aplicación en base a la demanda de sus usuarios mediante auto-escalado de instancias.