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)

ÍNDICE

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.

OBJETIVO

El objetivo del proyecto es construir una aplicación descentralizada que brinde a empresas o personas físicas un medio para administrar dinero, el cual puede ser aportado por varias partes diferentes, de forma totalmente transparente y trazable. Para ello, la aplicación web, que será la interfaz con la que un usuario interactúa, permitirá comunicarse con el backend (un contrato inteligente) y de esta manera configurar diferentes parámetros a la instancia de dicho smart contract que regularán las reglas de la administración del fondo. Los principales ítems configurables son:

- Si se permitirá a cualquier usuario de la red de Ethereum aportar dinero al fondo o si dicha acción sólo estará restringida a personas específicas (address).
- Cómo se realizará el proceso de extracción/transferencia del dinero del smart contract:
    - Si solo puede realizarlo el/los dueño/s del contrato inteligente.
    - Si cualquier persona que haya aportado al fondo puede retirar/transferir dinero del mismo.
    - Si cualquier persona que haya aportado al fondo puede retirar/transferir dinero del mismo con previa autorización del dueño del fondo o mediante una solicitud que será votada por las personas que hayan aportado dinero al mismo.

MARCO

La aplicación surge debido a que es habitual que cuando varias personas aportan dinero para una cierta causa común ocurran irregularidades con el manejo y la utilización de la misma por las personas que se encargan de administrarla. Esto es particularmente importante cuando la cantidad de personas involucradas en la causa es muy grande, pero también puede ocurrir en grupos más reducidos (por ejemplo cuando se junta dinero en un grupo de amigos).
Por lo tanto, la aplicación busca solventar y brindar transparencia en la utilización de este dinero, siendo una gran herramienta tanto para empresas como para personas individuales.

Definiciones:

- **Aplicación descentralizada o dApp:**
    - Las aplicaciones descentralizadas, también conocidas como "dApps" o "dapps", son aplicaciones digitales que se ejecutan en una red blockchain de computadoras en lugar de depender de una sola computadora. Podemos hacer una analogía de la comparación entre las apps tradicionales y las dApps haciendo alusión a las diferencias que existen entre un sistema centralizado y un sistema distribuido. El hecho de ser descentralizadas hace que estén libres del control y de la interferencia de una sola autoridad.

- **Blockchain:**
    - Blockchain es un libro mayor compartido e inmutable que facilita el proceso de registro de transacciones y de seguimiento de activos en una red de negocios. Un activo puede ser tangible (una casa, un auto, dinero en efectivo, terrenos) o intangible (propiedad intelectual, patentes, derechos de autor, marcas). Prácticamente cualquier cosa de valor puede ser rastreada y comercializada en una red de blockchain, reduciendo el riesgo y los costos para todos los involucrados.

- **Web 2.0**:
    - El término Web 2.0 se utiliza para referirse a sitios web que permiten a las personas colaborar y compartir información en línea de formas que antes no eran posibles. Este tipo de sitios web suelen considerarse interactivos, colaborativos o con contenidos generados por los usuarios. Sitios web como Facebook, Twitter, YouTube y Wikipedia son ejemplos de la web 2.0. La web

2.0 también se considera una forma de cultura participativa, lo que significa que adopta muchas formas, como el activismo social de base para el cambio global, la colaboración.

- **Web 3.0**:
    - La Web 3.0 es la tercera generación de servicios de Internet para páginas web y aplicaciones. Se centrará en el uso de una comprensión de datos basada en máquinas para proporcionar una Web semántica y datificada. El objetivo final de la Web 3.0 es crear sitios web más inteligentes, conectados y abiertos.

- **Ethereum:**
    - Ethereum en sí mismo es una plataforma digital que se basa en la tecnología blockchain o cadena de bloques. Su objetivo es convertirse en una blockchain capaz de ejecutar aplicaciones descentralizadas. Para lograr esto, este proyecto cuenta con una blockchain y una criptomoneda con características únicas. Entre ellas la capacidad de usar y crear smart contract y nuevos tokens. Ambas son poderosas funcionalidades, que permiten que se erija como una de las blockchain más completas y poderosas del criptomundo.

- **Ether:**
    - La moneda de la red se denomina Ether (ETH), y al igual que Bitcoin (BTC), el Ether se caracteriza por ser una criptomoneda que puede ser usada como método de pago entre pares. Otra de las semejanzas con Bitcoin y otras criptomonedas es que no está controlada por ningún gobierno u organismo regulador. Su desarrollo está marcado por la Ethereum Foundation, su Core Team y la comunidad que soporta y apoya. Otro punto importante, es que utiliza el protocolo de consenso Proof-of-Work (PoW), usando el algoritmo Ethash. Aunque esto puede cambiar en el corto plazo con el lanzamiento de Ethereum 2.0 y el salto a ser una criptomoneda usando el protocolo Proof of Stake (PoS).

- **Exchange:**
    - Son plataformas o mercados digitales que permiten intercambiar monedas digitales por dinero fiat y/u otras criptomonedas o mercancías.

- **NFT:**
    - Son las siglas en inglés de token no fungible (Non Fungible Token). Los NFT son un activo "inimitable" en el mundo digital que puede ser comprado y vendido como cualquier otro tipo de propiedad, pero no tienen forma tangible en sí mismos.

- **Solidity:**
    - Solidity es un lenguaje de programación orientado a objetos para escribir contratos inteligentes. Se utiliza para implementar contratos inteligentes en varias plataformas blockchain, la más destacada, Ethereum.

- **Contratos inteligentes o Smart Contracts:**
    - Los contratos inteligentes son líneas de código autoejecutables con los términos de un acuerdo que se establece entre un comprador y un vendedor verificados y ejecutados automáticamente a través de una red informática.
    - Nick Szabo los define como “protocolos de transacción computarizados que ejecutan los términos de un contrato”. Así, al ser implementados en cadenas de bloques hacen que las transacciones sean rastreables, transparentes e irreversibles.

- **Dirección cripto o Crypto Address:**
    - Una dirección cripto (de bitcoin, ether u otra criptomoneda) es un código alfanumérico que indica un posible destino para un pago de la criptomoneda que estés operando. Cada criptomoneda tiene su propia estructura de direcciones, por lo que no es posible abonar, por ejemplo, ethers en una dirección Bitcoin.
    - Todas las direcciones tienen asociada una llave privada y una llave pública: la **llave privada** corresponde a la contraseña con que firmas una transacción. Por lo tanto, es el acceso a los fondos que haya en una dirección. Quien tenga acceso a la llave privada tendrá acceso a las criptomonedas que haya en ella. Por su parte, la **llave pública** permite que la red pueda corroborar que una transacción cualquiera fue, efectivamente, firmada por la llave privada asociada a una dirección específica, y así corroborar que la transacción es válida.

Matriz FODA

Fortalezas

- **Descentralización de operaciones**: La aplicación correrá en la blockchain, lo que representa que las operaciones no dependen de un único ente (por ejemplo un banco) y las transacciones son directas entre usuarios.
- **Transparencia de transacciones**: Las operaciones realizadas en la blockchain quedan en un registro por lo que permite realizar un seguimiento de la utilización de los fondos.
- **Escalable y no dependiente de un único servidor**: La aplicación escala ya que no depende de un único nodo, lo que además agrega robustez y estabilidad.
- **Cada transacción puede ser pública y/o anónima**: Las transacciones quedan registradas pero no necesariamente se sabe quién es el usuario que la realiza, a menos que el usuario anuncie la Address que le corresponde.

Oportunidades

- **Nuevas oportunidades de negocio no exploradas**: Mucha gente todavía no tiene conocimientos del sector por lo que el nivel de utilidad que tiene la blockchain actualmente es desconocido.
- **Ser líderes en un área no desarrollada**: Debido a la cantidad de aplicaciones centralizadas, es posible marcar una impronta en lo que se conoce como Web 3.0.

Debilidades

- **Tecnología relativamente nueva**: Genera una necesidad de conocimiento que muchas veces es difícil encontrar.
- **Los costos pueden ser impredecibles**: Los costos son impredecibles debido a que el precio del “gas” o “fee” depende de la cantidad de transacciones que se estén dando en la blockchain al momento de querer realizar una operación, esto será resuelto con el lanzamiento de ETH 2.0, la cual se estipula llegará para finales de 2022.
- **Experiencia de Usuario limitada**: Las transacciones actualmente no son instantáneas, por lo que a veces se puede reflejar cierta demora entre el envío y la recepción de fondos

Amenazas

- **Mercado debilitado por volatilidad**: Los usuarios tienen mucha incertidumbre sobre el estado de la blockchain debido a un mercado volátil donde el precio de los activos es determinado por oferta y demanda de sus propios usuarios.
- **Estafas e incertidumbre en el "entorno cripto"**: Se han dado a conocer muchas estafas lo que genera cierto escepticismo sobre las nuevas aplicaciones dentro de la Web 3.0, por lo que es necesario trabajar en una marca transparente y confiable.

VENTAJA COMPETITIVA

Actualmente existen múltiples plataformas de gestión de fondos en la Web 2.0, entre ellas aplicaciones muy conocidas como pueden ser Kickstarter e Indiegogo, aunque éstas no están basadas en la blockchain, por lo que resta transparencia y descentralización.

- **Kickstarter**
- **Indiegogo**
- **AirFunding**
- **DonorPerfect**
- **Cafecito**

Aún no es un sector muy explorado en la blockchain ya que la mayoría de las aplicaciones están focalizadas en Exchanges y NFTs, aunque sí podemos considerar a BitGive, la cual es una DAO para realizar donaciones.

- **BitGive**

Buscamos combinar lo mejor de ambos mundos, en el caso de BitGive el enfoque está dado en donaciones sin fines de lucro, pero aplicaciones como Kickstarter o Indiegogo buscan potenciar no sólo proyectos sin fines de lucro, sino también financiar startups o proyectos indie que requieren de un capital inicial del cuál quizás sus fundadores no disponen, pero no cuentan con las ventajas de transparencia y solidez que provee la Blockchain.

Con este proyecto deseamos implementar las ventajas que nos provee la Web 3.0 para poder colaborar y desarrollar un mundo más descentralizado y transparente en el que no debemos depender de una organización externa o las limitaciones de un gobierno de turno para poder fondear un proyecto o realizar donaciones a una organización sin fines de lucro además de irrumpir en un mercado en el que todavía no se ha realizado tanto énfasis y no se han descubierto las grandes ventajas que hoy encontramos gracias a las nuevas tecnologías.

INFRAESTRUCTURA

Hardware

No se requerirá de ningún tipo de Hardware propio para implementar la aplicación en producción debido a que el backend, escrito en Solidity, será desplegado en la red descentralizada de Ethereum mediante la conexión con un nodo de la red, la cual se podrá implementar utilizando una herramienta gratuita como es Infura.
Por otro lado, el frontend (aplicación web) será desplegado en el sistema de archivos distribuido IPFS, el cual nos brindará la principal ventaja de que dicha aplicación será almacenada en varios nodos (computadoras de la red) descentralizadas.
De esta manera, tendremos una aplicación descentralizada completa, la cual no podrá ser atacada a través de un servidor centralizado.

Software

Los programas o softwares necesario para realizar el proyecto serán:

- Remix: Remix es un entorno integrado de desarrollo (IDE) basado en un navegador que integra un compilador y un entorno en tiempo de ejecución para Solidity sin los componentes orientados al servidor.
- Visual Studio Code: Editor de código fuente independiente que se ejecuta en Windows, macOS y Linux. Cuenta con una gran cantidad de extensiones que nos ayudarán en nuestro desarrollo.
- Infura: Es un conjunto de herramientas para que cualquiera pueda crear una aplicación que se conecte a la cadena de bloques Ethereum. Interactúa con la cadena de bloques Ethereum y ejecuta nodos en nombre de sus usuarios.
- IPFS: InterPlanetary File System, es un sistema de archivo descentralizado que busca garantizar la seguridad, privacidad y resistencia a la censura de tus datos.
- Ganache: Ganache es un software que nos proporciona una red de pruebas local súper sencilla e intuitiva.
- Rinkeby Testnet: es una red de prueba de Ethereum que nos permitirá desplegar nuestra aplicación en la misma para hacer diferentes pruebas sin gastar dinero (ethers) real.
- Truffle: Truffle es un conjunto de herramientas que nos permitirá crear aplicaciones sostenibles y profesionales utilizando la Máquina Virtual Ethereum (Ethereum Virtual Machine, EVM).

- Hardhat: Es un entorno de desarrollo para compilar, desplegar, testear y depurar un software de Ethereum. Nos ayudará a gestionar y automatizar tareas recurrentes.
- MetaMask: MetaMask es un software de criptomoneda que es instalado como extensión de un navegador web. Este es utilizado para interactuar con la plataforma de blockchain Ethereum.

REQUERIMIENTOS

Requerimientos funcionales

- El sistema permitirá a un usuario de la red de Ethereum crear un nuevo fondo común (instanciar un contrato inteligente) del cual será el administrador.
- El sistema permitirá a un usuario de la red de Ethereum que desea crear un nuevo fondo configurar una serie de parámetros iniciales del mismo que determinarán las reglas del contrato inteligente que se instanciará.
- El sistema permitirá a un usuario de la red de Ethereum ingresar dinero (ether) en un fondo común particular.
- El sistema permitirá a un usuario de la red de Ethereum autorizado retirar/transferir dinero (ether) de un fondo común al que haya aportado anteriormente.
- El sistema permitirá a un usuario de la red de Ethereum realizar una solicitud de retiro de dinero de un fondo al que haya aportado anteriormente.
- El sistema permitirá a un usuario de la red de Ethereum votar el retiro de dinero de un fondo por parte de otro contribuidor que lo haya solicitado.
- El sistema permitirá a un usuario de la red de Ethereum administrador de un fondo delegar la administración del mismo a otras personas.
- El sistema permitirá a un usuario de la red de Ethereum administrador de un fondo autorizar a otras personas a realizar aportes al contrato y poseer los privilegios para realizar votaciones de retiro.
- El sistema mostrará un registro de todas las operaciones del contrato inteligente del fondo realizadas.

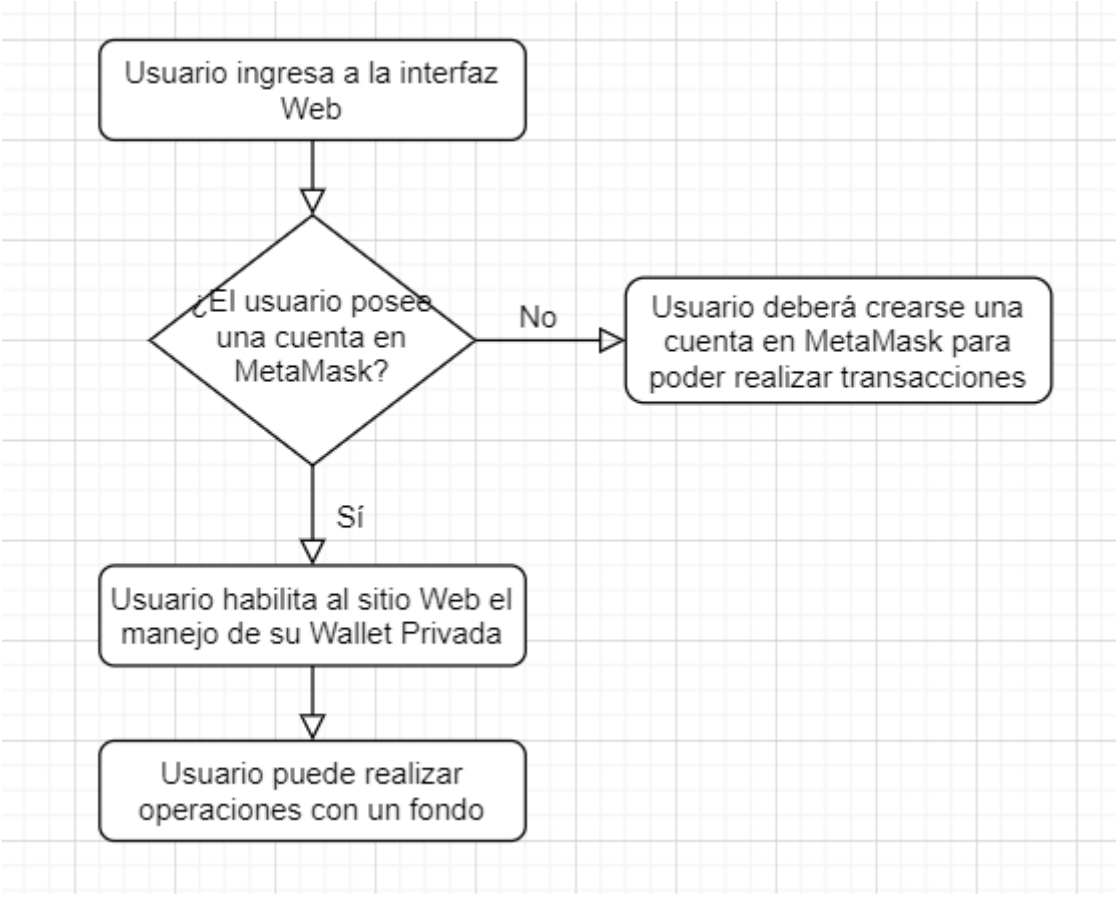
Requerimientos no funcionales

- La aplicación estará disponible siempre debido a que correrá en una red descentralizada y la misma estará distribuida en diferentes nodos (máquinas).
- La aplicación mantendrá la privacidad de cada usuario dado que los mismo solos estarán identificados en el mismo con una dirección de la red de Ethereum (anonimato).
- La aplicación no almacenará ningún dato o información de forma descentralizada.
- Toda la interacción de la interfaz web con el backend será llevada a cabo directamente por los usuario mediante la utilización de una wallet privada (MetaMask).

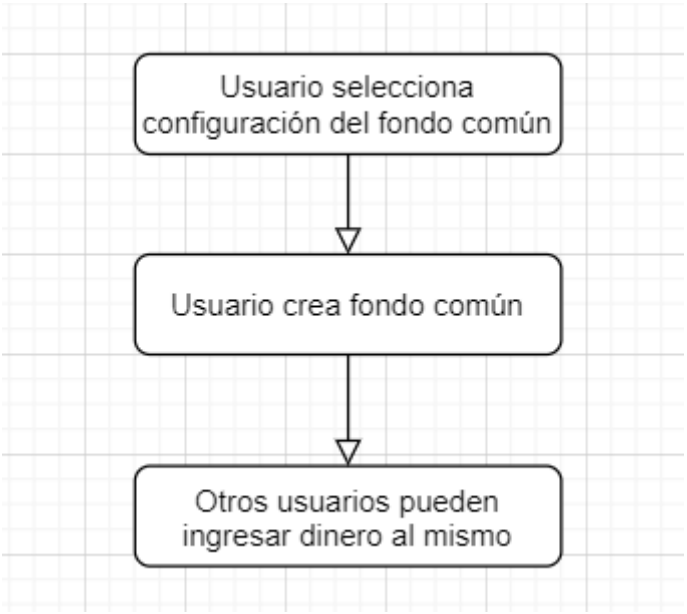
- Toda la actividad que realizan los usuarios con el contrato inteligente del fondo común será rastreable y nunca podrá ser eliminada de la red de Ethereum.

DIAGRAMAS DE ACTIVIDADES

Conexión con el sitio Web



Creación de un fondo común



Retiro de dinero del fondo