Arquitectura de Aplicaciones

Trabajo Práctico de Investigación

DApps

INTEGRANTES - GRUPO 4

- Barrera, Elizabeth Gabriela (LU 1034506)
- Basteiro, Fernando (LU 1061120)
- Fuentes, Gonzalo Ariel (LU 1048232)
- Josevich, Danila Nancy (LU 1068313)
- Martínez Saucedo, Ana Carolina (LU 1078889)

PROFESORES

- González, Pablo Daniel
- Inchausti, Pablo Ezequiel

Índice de Contenidos

¿Qué son las DApps?

Introducción

Una DApp o aplicación descentralizada es aquella que se ejecuta un sistema informático descentralizado, específicamente dentro de una red de computadoras P2P. La mayoría de las DApps se ejecutan sobre una red blockchain, aunque existen otras que se ejecutan sobre otras redes P2P, como Tor o BitTorrent.

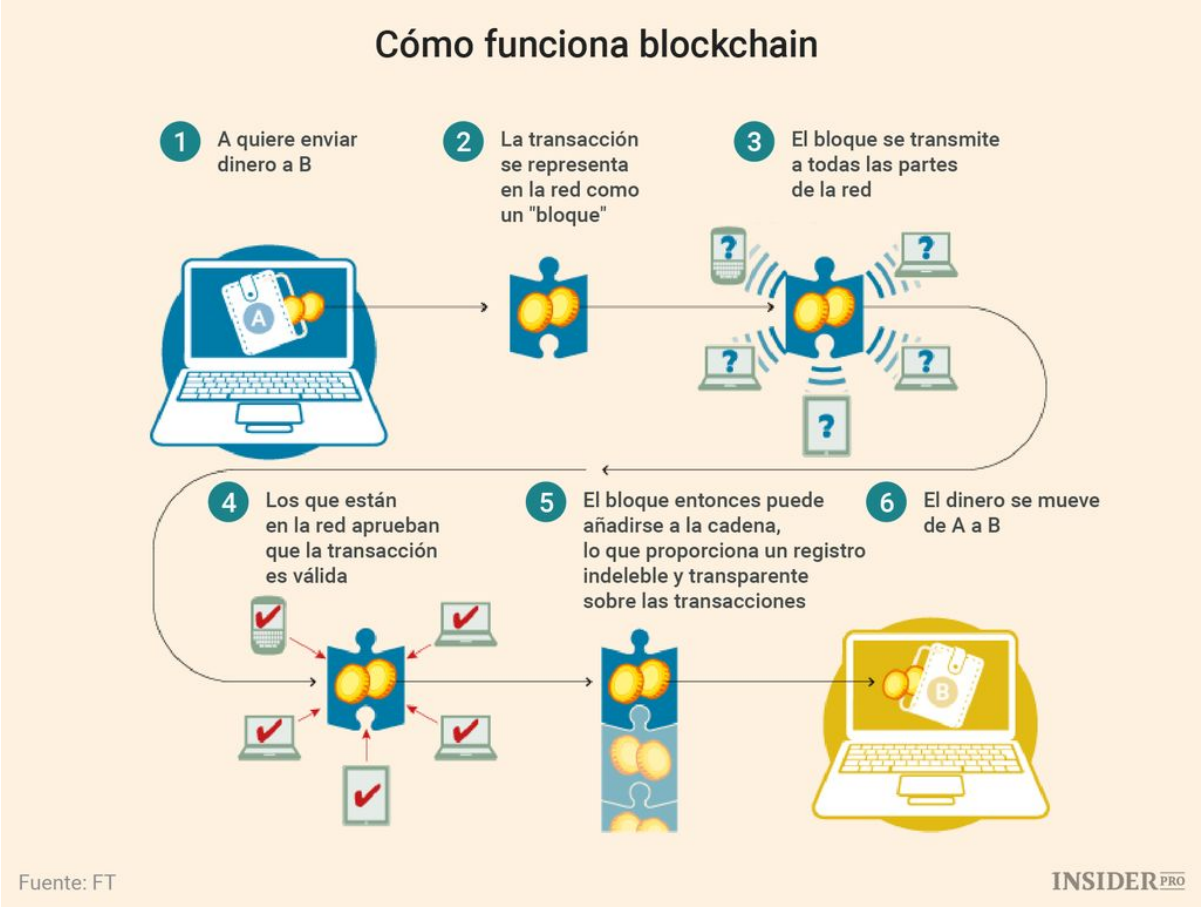
Existe una serie de requisitos que debe cumplir una aplicación para que pueda considerarse como una DApp, entre ellos:

- El código fuente de la aplicación debe ser abierto y poder operar sin una entidad que administre los tokens que gestione.
- La aplicación debe contar con un token criptográfico que permita el acceso a la aplicación y transaccionar con ese token. Algunos ejemplos de tokens criptográficos son Bitcoin o Ethereum.
- La aplicación deberá generar tokens mediante un algoritmo estándar.

Blockchain

Blockchain es una red P2P de computadoras o nodos que comparten toda la información y código de la red. Análogamente se puede decir que es un gran libro de registros organizados en bloques, “encadenados” entre sí mediante validaciones criptográficas que otorgan seguridad y privacidad a las transacciones que se realicen en ella. De esta manera, se prescinde de un servidor central, ya que cada computadora conectada tiene una copia de toda la información de blockchain.

El control de las transacciones que se realizan en blockchain es descentralizado y corre por parte de los usuarios, utilizando un mecanismo de consenso que previene el duplicado de transacciones y también su alteración. Toda transacción agregada a blockchain se hace de forma irreversible, y las transacciones realizadas a lo largo del tiempo son preservadas para siempre.



Ethereum

Ethereum es una red blockchain que tiene un lenguaje de programación integrado y una computadora blockchain que permite a los desarrolladores escribir smart contracts y aplicaciones descentralizadas. La criptomoneda de Ethereum es Ether, siendo esta el incentivo que reciben los desarrolladores para que escriban DApps de calidad y la recompensa que reciben aquellos usuarios que proveen recursos a blockchain.

Como los recursos computacionales son escasos a través de los nodos de Ethereum, existe una unidad fundamental de computación llamada Gas. A fin de evitar el uso innecesario de recursos computacionales por bucles infinitos accidentales, hostiles o errores de programación en las DApps, cada transacción que se realice debe establecer un número de pasos computacionales de ejecución que puede usar. Generalmente se establece en 1 gas el valor de un paso computacional, aunque otras transacciones son más costosas debido a que necesitan más procesamiento computacional o almacenamiento.

Ethereum posee su propio lenguaje de programación para smart contracts que usan la máquina virtual de Ethereum (EVM): Solidity.

Características

- Código abierto: el código fuente de las DApps es abierto y está disponible para todos los usuarios. Ante cualquier cambio que se quiera realizar, la mayoría debe llegar a un consenso para efectivamente aplicar ese cambio.
- Consenso descentralizado: todas las transacciones que realicen las DApps deben ser almacenadas en una blockchain pública y descentralizada, siempre con una validación previa realizada por la mayoría de los nodos.
- Moneda interna: para alocar recursos escasos en una red (como el procesamiento computacional) se usa un appcoin. Por ejemplo, en la red Bitcoin los mineros son quienes proveen de estos recursos a la red y cobran una cuota por cada transacción que los usuarios efectúan.
- Punto de fallo central inexistente: una DApp no puede estar fuera de servicio porque no hay un servidor central que pueda estar fuera de servicio. Esto se logra mediante la descentralización de las DApps a través de nodos independientes.
- Seguridad: el código de las DApps está en blockchain, una vez desplegada es imposible modificarla. De esta forma se garantiza que el entorno de ejecución es inmutable, sumado a que toda acción que se realiza quedará registrada en blockchain. Además, los datos que maneja una DApp están bajo posesión del usuario siempre, ya que las transacciones que realice el usuario sólo pueden efectuarse si se tienen las claves públicas y privadas correctas.

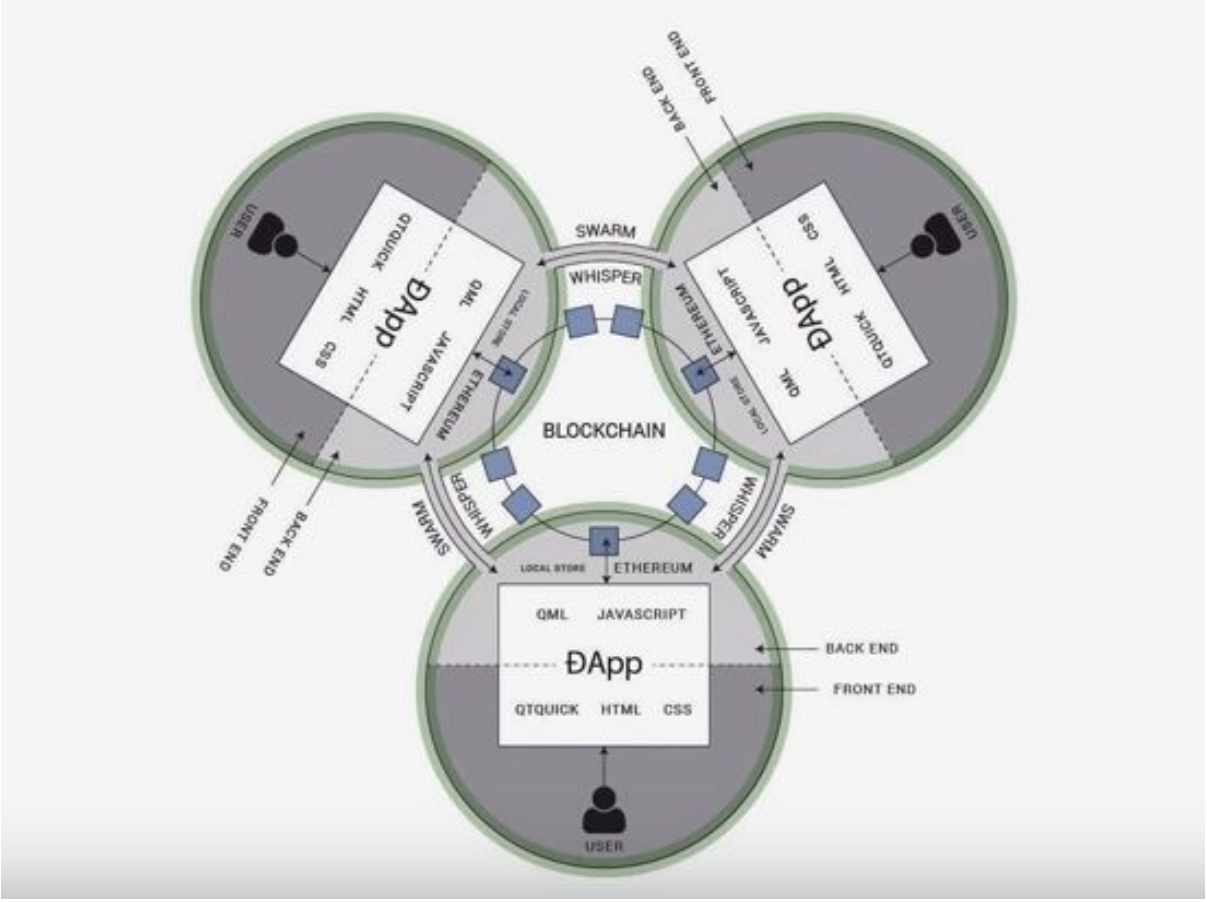
Arquitectura

El front end de una DApp está compuesto por cualquier tecnología que utiliza actualmente una aplicación tradicional, como puede ser HTML, JavaScript o CSS. Sin embargo, en contrapartida a las aplicaciones tradicionales Web2, las DApps son aplicaciones Web3 que necesitan conectarse a una blockchain administrada por un “wallet” o billetera que guarde las claves privadas y direcciones blockchain de forma tal que podamos gestionar nuestra identidad digital para poder transaccionar en blockchain. Las claves públicas sirven para identificar y autenticar un usuario, en vez de hacerlo mediante una API que consulta una base de datos.

Web3 se basa en Web2 e introduce elementos nuevos a nivel aplicación. Por ejemplo, del lado del backend Web3 se agrega una nueva capa de infraestructura para que las aplicaciones puedan interactuar en la blockchain. Para esto las DApps necesitan un componente que administre las claves privadas de un usuario, que luego serán las que se usan para firmar transacciones en blockchain.

El back end de una DApp está representado por uno o más contratos inteligentes o smart contracts que se ejecutan e interactúan con blockchain. Los contratos inteligentes son instrucciones almacenadas en la blockchain que se ejecutan automáticamente sin intermediarios, controlan y documentan eventos y acciones de acuerdo a un contrato entre dos o más partes. El código de los smart contracts es visible por todos y, como se explicó anteriormente, no puede cambiarse justamente por ser ejecutados en blockchain.

Los smart contracts representan la lógica de negocio de una DApp y son los encargados de procesar información proveniente de eventos, además de gestionar el estado de todos los nodos que componen la blockchain, leyendo y escribiendo información en ella.



Arquitectura conceptual de una DApp

A continuación, se presenta a modo sintético las principales diferencias entre una aplicación tradicional y una aplicación descentralizada.

Aplicación web tradicional

Aplicación compatible con Web3

Limitaciones

- No se puede explotar el potencial de hardware de los dispositivos de los usuarios, ya que las DApps se ejecutan en los nodos de la blockchain.
- Depurar smart contracts es difícil, pudiendo tener problemas de seguridad graves que no sean fácilmente encontrados.
- Tienen problemas de escalabilidad, ya que en blockchains como Ethereum o Bitcoin se optó por optimizar la seguridad y descentralización en detrimento de la escalabilidad.

Ejemplos

Golem

Golem es un proyecto que permite “alquilar” la potencia o almacenamiento de las computadoras de otros usuarios. Esto es especialmente útil para cuando necesitamos potencia computacional eventual y nuestra computadora no puede suplirlo.

Augur

Augur combina los conceptos de descentralización y predicción de mercados para predecir acontecimientos que ocurren en el mundo real mediante el comercio de acciones virtuales.

Aragon

Aragon busca eliminar intermediarios en los procesos de creación y mantenimiento de estructuras organizativas mediante blockchain. Para esto permite a los usuarios convertirse en empresarios y dirigir su propia organización, gestionando dicha organización de forma fácil y segura.

Crypto Kitties

Crypto Kitties es un juego que usa blockchain y tiene su propia criptomoneda para poder comprar, coleccionar y criar gatos digitales.

Fuentes

- *Decentralized Applications*. (Julio 2019). Shermin Voshmgir. Recuperado de http://blockchainhub.net/decentralized-applications-dapps/
- *The Ultimate Ethereum Dapp Tutorial* (Junio 2020). Recuperado de https://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial
- *Qué son las DApps y por qué serán cada vez más importantes.* (Septiembre 2018). Recuperado de https://www.bbva.com/es/que-son-las-dapps-y-por-que-seran-cada-vez-mas-importantes/
- *Decentralized Applications. Chapter 1. What Is a Decentralized Application?*. Siraj Raval. Recuperado de https://www.oreilly.com/library/view/decentralized-applications/9781491924532/ch01.html
- *¿Qué son las dApps o aplicaciones descentralizadas?* (Abril 2018). Recuperado de https://www.tucriptomoneda.com/que-son-las-dapps/
- *Qué es Ethereum (ETH)*. Recuperado de https://www.criptonoticias.com/criptopedia/que-es-ethereum-eth/
- *What Are Dapps? The New Decentralized Future.* Recuperado de https://blockgeeks.com/guides/dapps/
- *¿Qué son y para qué sirven las Aplicaciones Descentralizadas o Dapps?* Recuperado de https://www.miethereum.com/smart-contracts/dapps/