Desarrollo de una criptomoneda con Blockchain

Sara Pérez García

29 de marzo de 2022

Resumen

Blockchain es una palabra es que escuchada en nuestro dia a dia cada vez más. Con este proyecto he querido aprender a utilizar esta tecnología con aplicaciones reales. Me he centrado en la implementacion de una criptomoneda con Node.js, Express, PubNud, React (si hago el frontend) y Git.

1. Introducción

1.1. Descripción del problema

1.1.1. ¿Qué es Blockchain?

Blockchain es de un conjunto de tecnologías que permiten llevar un registro seguro, descentralizado, sincronizado y distribuido de las operaciones digitales, sin necesidad de la intermediación de terceros [7]. 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 [3].

Con el Blockchain se consigue tener un control de acceso sobre los datos que se almacenan, seguridad de que esos datos no van a ser modificados en posibles ataques; transparencia, ya que todo el mundo puede acceder directamente a la cadena de bloques y consultar la informacion que contenga. Se almacena un historial de las transacciones lo que mantiene la tracabilidad de estas. Dado que se encuentro distribuido no existen intermediarios y nadie puede ser dueño de la informacion que esta cadena contiene. Esto genera una reducción de costes, más eficiencia y que cada uno pueda ser dueño de sus datos.

1.1.2. ¿Qué es la cryptoconcurrencia?

Una criptomoneda (o 'cripto') es un activo digital que puede circular sin necesidad de una autoridad monetaria central como un gobierno o un banco. En cambio, las criptomonedas se crean utilizando técnicas criptográficas que permiten a las personas comprarlas, venderlas o intercambiarlas de forma segura mediante el uso del Blockchain [4].

1.2. Objetivos

Los objetivos de este proyecto es familiarizaerse con la tecnologia del Blockchain mediante la programacion de una criptomoneda. Ser capaz de crear e implementar las

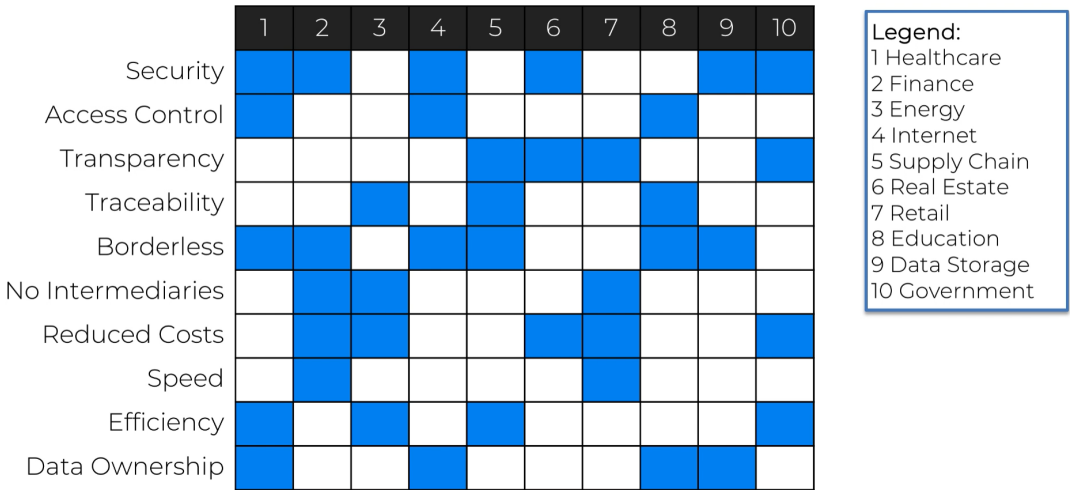

Figura 1: Caracteristicas del Blockchain más relevantes a diferentes aplicaciones industriales.

caracteristicas que diferencian al blockchain. Aprender cómo generar una red peer-to-peer (P2P) y que los usuarios accedan y modifiquen la informacion de la cadena de bloques. Asegurar que las transaciones que se llevan a cabo no están duplicadas y se sincronizan en todas las copias de las cadenas de la red distribuida. Ser capaz de desarrollar carteras digitales para los usuarios que almecenen las transacciones de estos. Desarrollar e implimertar el minado de bloques de la cadena y generar los API endpoints necesarios para la comunicacion entre peers.

1.3. Motivación

Considero que el Blockchain es una nueva forma de comprender el almacenamientos de datos y me intersa comprender cómo funciona esta tecnologia. Creo que hoy en día se confunden los conceptos de criptomonedas con el blockchain pero realmente esta segunda es el esqueleto en el que se sustenta la aplicacion de las 'cripto'. La mejor forma de aprender a es poniendo los conceptos aprendido en practica y la forma más sencilla que he encontrado para comprender el concepto del Blockchain es desarrollando una criptomoneda.

A futuro, me gustaría crear una pequeña prueba de concepto de un sistema de votaciones descentralizado, seguro y transparente, basado en el blockchain. Esto permitiria automatizar la votacion en unas elecciones haciendo que cada persona pueda votar de forma segura desde cualquier dispositivo. Existen muchas más aplicaciones que se le puede dar al blockchain pero actualmente la que he encontrado para aprender es el desarrollo de una criptomoneda.

2. Tecnologías y Herramientas utilizadas

- **Javascript**: es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos, basado en prototipos, imperativo, débilmente tipado y dinámico.
- **Node.js**: Ideado como un entorno de ejecución de JavaScript orientado a eventos asíncronos, Node.js está diseñado para crear aplicaciones network escalables [5].

- **Express**: Express es una infraestructura de aplicaciones web Node.js mínima y flexible que proporciona un conjunto sólido de características para las aplicaciones web y móviles. Lo usaré para el desarrollo de las API endpoints [1].
- **PubNud**: es una plataforma de comunicación en tiempo real. La utilizará para la generacion de la red p2p [2].
- **Postman**: Postman es una aplicación que nos permite realizar pruebas API. Es un cliente HTTP que nos da la posibilidad de testear 'HTTP requests' a través de una interfaz gráfica de usuario, por medio de la cual obtendremos diferentes tipos de respuesta que posteriormente deberán ser validados. Con esta aplicacion podre testear las API endopoint que vaya desarrollando [6].

3. Estimación de Recursos y Planificación

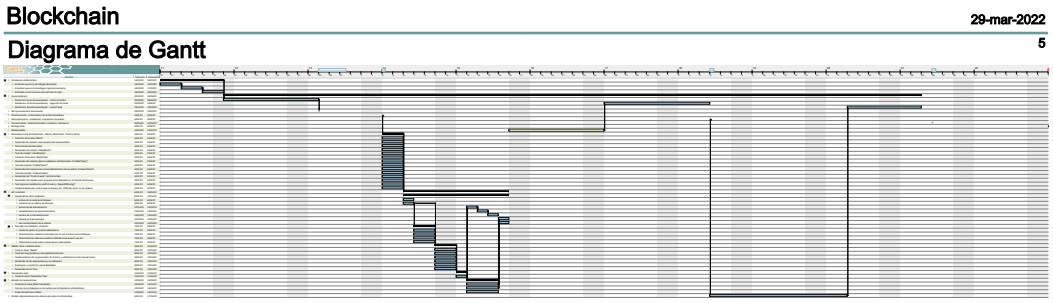

Figura 2: Gantt chart

4. Desarrollo

4.1. TODO

Referencias

[1] infraestructura de aplicaciones web node.js 2022, 2022.

[2] real-time in-app chat and communication platform 2022, 2022.

[3] IBM. ¿qué es la tecnología de blockchain? - ibm blockchain, 2021.

[4] nerdWallet. what is cryptocurrency? here’s what investors should know, 2022.

[5] Node.js. acerca de node.js 2022, 2022.

[6] postman. postman, 2022.

[7] Solunion. ¿qué es y para qué sirve la tecnología blockchain?, Oct 2021.