Diseño y Prototipado de un Simulador Modular Blockchain de Código Abierto y Uso Libre para Investigación

William Ricardo Cadenas Mantilla
wcadenas@uninorte.edu.co

Yennifer Paola Herrera Ariza
yenniferh@uninorte.edu.co

David Andrés Cuentas Martinez
dacuentas@uninorte.edu.co

Asesor
Pedro M. Wightman, Ph. D.
pwightman@uninorte.edu.co

Asesor
Ricardo Villanueva Polanco, Ph. D.
rpolanco@uninorte.edu.co

1. INTRODUCCIÓN

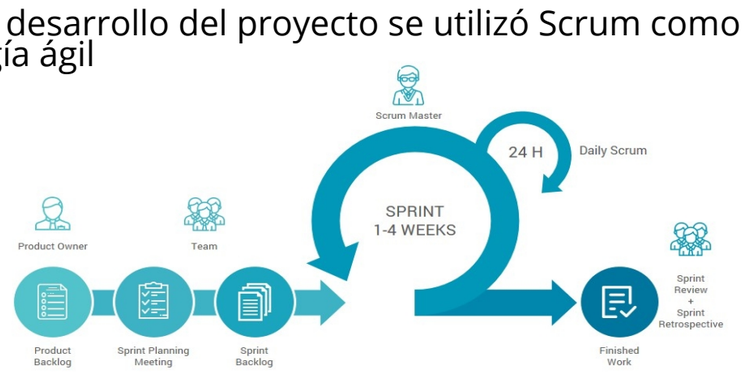
El uso de la Blockchain como tecnología para preservar datos de forma inmutable y descentralizada ha tenido un auge en los últimos años, puesto que las tecnologías o implementaciones más famosas como Bitcoin y Ethereum han demostrado su valor con el incremento de los bienes que se intercambian en dichas plataformas [1]. Se propone un proyecto de código abierto disponible en Github que cumple y sienta las bases para conformar un simulador robusto que pueda servir para investigación y simulaciones en el ámbito académico.

2. DESCRIPCIÓN DEL PROBLEMA

En el desarrollo y análisis de Blockchain existen muchas combinaciones posibles. Sin embargo, la cantidad de herramientas que permiten ver el funcionamiento y que faciliten el estudio de estas combinaciones es muy baja [2]. El problema principal es la falta de un simulador Blockchain modular que permita al desarrollador poder combinar, agregar e incluso editar las configuraciones del sistema para ver su comportamiento ante

3. METODOLOGÍA

Durante el desarrollo del proyecto se utilizó Scrum como metodología ágil



La implementación de esta metodología ayudó para realizar los objetivos de forma ordenada y secuencial, además promovió una buena comunicación entre los involucrados para alcanzar el éxito de este proyecto.

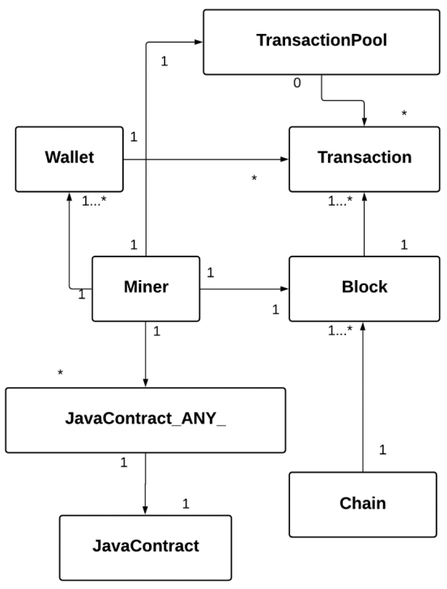
4. OBJETIVO GENERAL

Diseñar y prototipar un sistema Blockchain modular que en primera instancia pueda simular el comportamiento de intercambio de moneda como Bitcoin, pero su estructura lógica le permita evolucionar y poder implementar un sistema más complejo como Ethereum con contratos inteligentes e intercambiar otros bienes digitales o registrar información en la cadena de bloques, dejando el código desarrollador como código abierto.

5. OBJETIVOS ESPECÍFICOS

1. Identificar las variables y componentes claves para el diseño del simulador de Blockchain a través de la revisión sistemática de la literatura.
2. Diseñar la arquitectura del sistema modular que permita la integración de los diferentes componentes para simular un intercambio de monedas tipo Blockchain.
3. Desarrollar una comunicación Peer To Peer para la conexión de los nodos a la red de Blockchain.
4. Desarrollar el prototipo del simulador Blockchain con una estructura basada en contenedores.
5. Publicar la implementación del prototipo de código abierto, para que siga siendo mejorada y sirva de ejemplo para futuras investigaciones.

6. MODELADO DE DATOS



La cadena Blockchain es una lista de bloques donde por lo menos siempre habrá un bloque (Génesis Block).

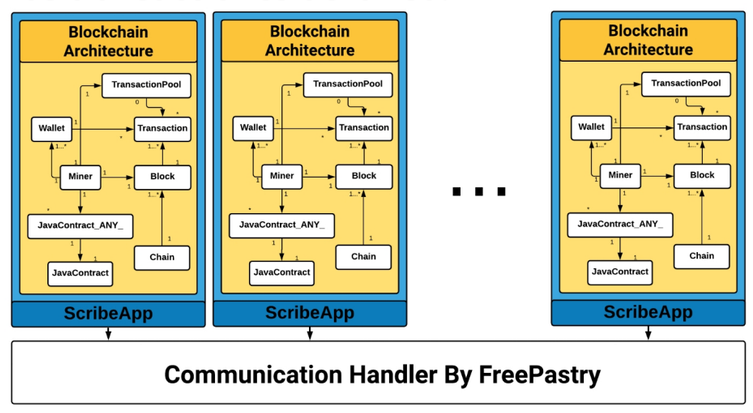
Los bloques son conformados por transacciones a guardar en la Blockchain y estas son generadas por medio de una Wallet y almacenadas en la TransactionPool que tienen los mineros que forman la red.

Los SmartContracts son ejecutados por los mineros. Estos contratos por motivos de modularidad son extendidos de una clase padre la cual tiene funciones que pueden ser editadas para ingresar lógica personalizada.

7. PROCEDIMIENTO

La red es iniciada por un primer nodo el cual si es el primero crear un canal de comunicación usando la librería FreePastry por medio de Scribe con el objetivo de usar este medio para la transferencia de datos entre todos los nodos de la red. Una vez que este nodo es iniciado procede a crear la cadena y el bloque génesis. Además, estará atento a identificar peticiones para distribuir dicha cadena que este tiene.

Cuando un nodo es añadido a la red hace una petición para sincronizar la cadena y una vez que la cadena haya sido sincronizada completa y exitosamente el nodo estará disponible para recibir las transacciones de la red.



Cuando una transacción es generada se procede inmediatamente a ser transmitida a toda la red y es almacenada en la TransactionPool que tiene cada minero.

Una vez que cierta cantidad de transacciones sean almacenadas el minero, este empieza a generar el bloque candidato iterando sobre cada una de ellas y ejecutando el Smart Contract asociado.

El minero añade su bloque a la cadena local y comparte a la red el bloque que ha generado. Además siempre estará escuchando los bloques propagados para validarlos y si son exitosos se añaden a la cadena de bloques.

8. RESULTADOS

1) Modularidad para desarrollar e implementar SmartContracts en la Blockchain desarrollada.
2) Archivo configurable para la variación de parámetros y cambiar el comportamiento de la Blockchain desarrollada.
3) Transferencia de información por medio de conexión Peer To Peer implementado la librería FreePastry con Scribe.
4) Despliegue de nodos a la red Blockchain por medio de Docker.

9. REPOSITORIO

El código desarrollado durante la elaboración de este proyecto es de carácter publico y abierto. Se puede encontrar en el siguiente enlace:
https://github.com/DavidCuentasMar/ModularJavaBlockchain

10. CONCLUSIONES

Inicialmente, debemos decir que desde la revisión sistemática de la literatura, se pudo obtener información muy importante y actual de cual es el uso más popular de las Blockchain hoy en día y su potencial a futuro, por tal motivo la idea del proyecto y su objetivo principal de aportar una implementación que se pueda progresar a través del tiempo se logró satisfactoriamente.

Dicho lo anterior, los objetivos específicos se llevaron a cabo y dejaron como precedente un repositorio de código abierto en la plataforma Github, el cual, si es progresado y mejorado a partir de las bases sentadas en este proyecto, tiene la capacidad de convertirse en una herramienta poderosa para probar e implementar nuevas funcionalidades y algoritmos que nos aporten datos y resultados para determinar parámetros óptimos de construcción para futuros sistemas basados en la tecnología de Blockchain.

REFERENCIAS

[1] R. Zhang, R. Xue, y L. Liu, «Security and Privacy on Blockchain», ACM Comput. Surv., vol. 52, n.o 3, pp. 1-34, jul. 2019, doi: 10.1145/3316481.
[2] B.-J. Butijn, D. A. Tamburri, y W.-J. Van Den Heuvel, «Blockchains: A Systematic Multivocal Literature Review», ACM Comput. Surv., vol. 53, n.o 3, pp. 1-37, jul. 2020, doi: 10.1145/3369052.