Desarrollo de una DApp académica en la red Blockchain Federal Argentina

Jorge Eterovic; Jonatan Uran Acevedo; Alejandro Rusticcini; Nora Gigante

Programa PROINCE / Departamento de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza
Florencio Varela 1903 (B1754JEC), San Justo, (5411) 4480-8900

eterovic@unlam.edu.ar; juran@unlam.edu.ar; arusticcini@unlam.edu.ar; ngigante@unlam.edu.ar

RESUMEN

Blockchain Federal Argentina (BFA) es la primera plataforma multiservicios sólida, transparente, confiable, abierta y participativa de Argentina, desarrollada para integrar servicios y aplicaciones sobre la Blockchain de Ethereum.

Este trabajo se desarrolló en el marco de un proyecto de investigación que consiste en implementar un nodo Minero (en adelante nodo Sellador) de la Universidad Nacional de La Matanza (UNLaM), dentro de la red Blockchain Federal Argentina.

La UNLaM ha firmado un contrato de colaboración público-privado con BFA, y actualmente forma parte de este consorcio. El mismo permitirá montar un nodo Sellador dentro de la infraestructura de la universidad que formará parte de la red de nodos de BFA.

Uno de los objetivos del proyecto de investigación es desarrollar e implementar una Aplicación Distribuida (DApp) que estará disponible para su uso libre y gratuito para toda la comunidad académica. Esta DApp está siendo desarrollada para las emisiones seguras de actas de examen, certificados de materias aprobadas y títulos académicos, entre otras.

La relevancia de este trabajo radica en la importancia que tiene para una institución académica formar parte de una red con las características de BFA que le permitirá emitir en formato digital distintos tipos de documentos académicos de manera confiable.

Palabras clave:
Blockchain. DApp. Contrato Inteligente. Blockchain Federal Argentina.

CONTEXTO

Este proyecto de investigación fue presentado como un Programa de Incentivos a Docentes Investigadores de la Secretaría de Políticas Universitarias del Ministerio de Educación - PROINCE en el Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza.

El presente proyecto es del tipo “investigación aplicada” y consiste en el desarrollo e instalación de un nodo sellador en la UNLaM dentro de la red Blockchain Federal Argentina y de la implementación de una DApp para uso académico.

1. INTRODUCCIÓN

Blockchain se están integrando cada vez más en la sociedad. Su gran potencial y su tecnología revolucionaria se están abriendo cada día más hacia las personas. Su modelo seguro, descentralizado y público permite el funcionamiento independiente de autoridades bancarias u otras instituciones.

Una de las criptodivisas con mayor potencial que usan la tecnología blockchain es Ethereum. El objetivo de Ethereum es crear una blockchain programable que cambie el modelo de internet, donde los programas almacenados en su interior sirvan como columna vertebral a futuras aplicaciones descentralizadas (dAps). Estos programas se conocen como smart contracts.

Una Blockchain, contiene un conjunto de tecnologías informáticas y criptográficas que permiten crear una estructura de datos en forma de cadena de bloques cifrados y enlazados entre ellos que a su vez forman una base de datos distribuida y sincronizada.

Una Blockchain, dada su arquitectura y funcionamiento, permite almacenar información de forma verificable, que no puede ser modificada.

Una Blockchain no consiste en una única base de datos, ya que cada nodo tiene una copia de esta y están en constante sincronización. En lugar de confiar en una entidad central, la confianza en la integridad de esa base de datos se consigue mediante las interacciones de los participantes, es decir, el sistema está basado en una confianza descentralizada. Las plataformas que más utilizan este tipo de tecnología actualmente son las criptomonedas.

El ejemplo más famoso de una plataforma de criptomonedas que utiliza la cadena de bloques es Bitcoin, pero hay otras muy populares, como Ethereum, que utiliza su blockchain de manera distinta. La diferencia más significativa entre ambas es que Bitcoin pretende generar un sistema de economía digital y Ethereum, aparte de servir también como red de pago utilizando su propia moneda (Ether), es una plataforma cuyo propósito general es crear un blockchain programable.

Ethereum pretende crear una cadena de bloques donde los programadores puedan crear y subir código para que los participantes de la red puedan usarlo a través de los smart contracts. Estos contratos inteligentes son piezas de código que viven dentro del blockchain y que pueden ser utilizados de forma autónoma por los usuarios.

La existencia de contratos inteligentes permite realizar tareas autoejecutables que responden a una condición pre-programada en el contrato, es decir, en un acuerdo registrado previamente entre partes donde se cumpla una condición existente en el contrato, se ejecutaría la cláusula correspondiente a esa condición.

Estos contratos tienen gran cantidad de usos en la industria y en la vida diaria, como por ejemplo en la banca, Internet de las Cosas (IoT), autoría, derecho, etc.

Las DApps rompen los esquemas tradicionales al eliminar la necesidad de intermediarios en los servicios que ofrecen, ya que permiten a los proveedores interactuar directamente con los usuarios finales, lo cual brinda mayor flexibilidad y satisfacción para todos [1].

Las DApps se construyen sobre una cadena de bloques determinada, que cuenta con su respectivo protocolo. Las aplicaciones descentralizadas están compuestas por uno o varios contratos inteligentes (smart contract) que operan en la cadena de bloques y una plataforma front-end, que puede ser un sitio web, una aplicación web o móvil, entre otras posibilidades.

La comunicación entre el smart contract y el front-end se realiza mediante una interfaz de programación de aplicaciones (API, por sus siglas en inglés). Parte del procedimiento al crear una DApp es agregarla a un directorio o biblioteca de aplicaciones [2].

Blockchain, en español cadena de bloques, es una tecnología que permite administrar un registro de datos en la nube. Tiene como característica la transparencia y es prácticamente incorruptible.

A pesar de que Bitcoin fue la primera aplicación descentralizada que nació con el propósito de crear una alternativa a los medios de pagos tradicionales, las características de su blockchain

no facilitan la creación de DApps. Años más tarde surge Ethereum como un proyecto que busca superar algunas de las dificultades de Bitcoin.

Ethereum es una plataforma descentralizada de código abierto (open source), que permite la creación de contratos inteligentes sobre una blockchain. En diciembre de 2013, Vitalik Buterin comenzó el desarrollo de Ethereum, con la primera prueba de concepto (PdC) [3].

El enfoque de Ethereum es contar con un mecanismo de desarrollo más eficiente en cuanto a tiempo, seguridad y escalabilidad. Ethereum funciona de manera descentralizada a través de una máquina virtual llamada Ethereum Virtual Machine (EVM). Esta máquina ejecuta un código intermedio o bytecode el cual es una mezcla de lenguaje de programación LISP, un ensamblador y bitcoin script [4].

Los programas en Ethereum se escriben en lenguajes de programación de alto nivel, como Solidity, que es un lenguaje de alto nivel orientado a objetos que permite a los nodos de Ethereum almacenar y procesar datos. Su sintaxis es similar a la de JavaScript y está enfocado específicamente a la EVM para crear los contratos inteligentes [5].

Un contrato inteligente es un programa informático que ejecuta un flujo de trabajo que generalmente representa acuerdos registrados en una Blockchain, entre dos o más partes, por ejemplo, personas u organizaciones [6]. Dichos contratos se ejecutarán como resultado de que se cumplan una serie de condiciones especificadas previamente.

Solidity es un lenguaje de programación orientado a objetos utilizado para escribir contratos inteligentes en la plataforma Ethereum. Fue desarrollado por Gavin Wood y otros programadores.

Es un lenguaje de scripting tipado estáticamente. Esto quiere decir que las variables deben ser declaradas junto con su tipo antes de ser utilizadas. Se debe realizar el proceso de verificación y hacer cumplir las restricciones en tiempo de compilación, antes de que se ejecute el programa.

Cuenta con un IDE oficial llamado Remix. Un IDE (Integrated Development Environment, entorno de desarrollo integrado), es una aplicación que proporciona servicios para facilitarle al programador el desarrollo de software. Remix es un entorno de desarrollo, compilación y despliegue de contratos inteligentes basado en un navegador Web [7].

Una DApp es una aplicación distribuida sobre una Blockchain. Esta tiene múltiples capas y componentes y no depende de un sistema centralizado. Puede ser Web o Mobile. Una DApp es una aplicación que tiene su Back-end construido sobre contratos inteligentes, en contraposición con los Back-end tradicionales [8].

Finalmente, el desarrollo se hará en una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre la blockchain Ethereum, la Blockchain Federal Argentina [9]. Esta es una iniciativa confiable y completamente auditable que permite optimizar procesos y funciona como herramienta de empoderamiento para toda la comunidad.

2. LINEAS DE INVESTIGACIÓN Y DESARROLLO

En el presente proyecto de investigación, se estudiaron y analizaron los derechos, obligaciones y posibilidades emanados de la firma del contrato de colaboración público-privada celebrado con Blockchain Federal Argentina.

Luego de firmado el acuerdo, se procederá a instalar el hardware necesario para montar el nodo sellador. Seguido a esto, se implementará el software para el correcto funcionamiento del nodo.

Asimismo, se desarrollará e implementará una Aplicación Distribuida en la Blockchain de

BFA. Esto se hará mediante el desarrollo de un Contrato Inteligente, el desarrollo de una API, la implementación de la DApp sobre la Blockchain Ethereum de BFA y por último el diseño, desarrollo e implementación de una aplicación Front-end para entorno Web, y Mobile.

Se escribirán y presentarán informes de avances que incluyan el progreso del proyecto y las conclusiones de cada una de las actividades que forman parte del mismo.

Finalmente, se redactará un informe integral final con el contrato y el software implementado y desarrollado acompañado de recomendaciones y buenas prácticas de uso como conclusión del trabajo de investigación realizado.

3. RESULTADOS OBTENIDOS/ESPERADOS

El objetivo principal de este proyecto de investigación es implementar un nodo Sellador dentro de Blockchain Federal Argentina (BFA).

El objetivo secundario es desarrollar e implementar una DApp (Aplicación Distribuida) perteneciente a la UNLaM. Dicha DApp funcionará sobre la Blockchain de BFA.

Una DApp es una aplicación distribuida. Ésta se desarrollará sobre la blockchain Ethereum. Tendrá múltiples capas y componentes y no dependerá de un sistema centralizado. Podrá ser usada desde un front-end Web o Mobile.

Una DApp es una aplicación que tiene su Back-end construido sobre contratos inteligentes, en contraposición con los Back-end tradicionales [10] [11].

Blockchain Federal Argentina es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre blockchain. Una iniciativa confiable y completamente auditable que permite optimizar procesos y funciona como herramienta de empoderamiento para toda la comunidad.

4. FORMACIÓN DE RECURSOS HUMANOS

El equipo está integrado por docentes-investigadores que pertenecen a distintas cátedras de la carrera de Ingeniería Informática y de la Tecnicatura de Aplicaciones Web de la UNLaM, alguno de los cuales está haciendo sus primeras experiencias en investigación.

Uno de los miembros del equipo de investigación se encuentra desarrollando su trabajo de tesis de posgrado de la Maestría en Ciberdefensa y Ciberseguridad de la Universidad de Buenos Aires y de la Escuela Nacional de Inteligencia (ENI). El tutor de esta tesis es el Mg. Jorge Eterovic, integrante de este proyecto de investigación.

5. BIBLIOGRAFÍA

[1] Álvaro Santos García; Caracterización de Smart Contracts en Ethereum; Universidad Carlos III de Madrid; Leganés, España. 2019

[2] Mohammad Dabbagh, Mehdi Sookhak, Nader Sohrabi Safa; The Evolution of Blockchain: A Bibliometric Study; IEEE Access PP (99):1-1. 2019

[3] Vitalik Buterin; A Next Generation Smart Contract & Decentralized Application Platform; https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Última visita: diciembre de 2020.

[4] Gavin Wood; Ethereum: A secure decentralized generalized transaction ledger; Ethereum project yellow paper. 2014.

[5] Chris Dannen; Introducing Ethereum and Solidity; ISBN-13 (pbk): 978-1-4842-2534-9; Ed. Springer Science; New York, USA. 2017.

[6] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, Aquinas Hobor; Making Smart Contracts Smarter; CCS '16: Proceedings of the

2016 ACM SIGSAC Conference on Computer and Communications Security; Pages 254–269. 2016.

[7] Susan Elliott Sim, Rosalva E. Gallardo-Valencia; Finding Source Code on the Web for Remix and Reuse; ISBN 978-1-4614-6595-9: Ed. Springer Science; New York, USA. 2013.

[8] Andrea Pinna, Simona Ibba, Gavina Baralla, Roberto Tonelli, Michele Marchesi¸ A Massive Analysis of Ethereum Smart Contracts. Empirical study and code metrics. DOI: 10.1109/ACCESS.2019.2921936. IEEE Access. 2019.

[9] Blockchain Federal Argentina; 2020; htpps://www.bfa.org. Última visita: febrero de 2021.

[10] Cai, Wei; Wang, Zehua; Ernst, Jason B.; Hong, Zhen; Feng, Chen; Leung, Victor C. M.; Decentralized Applications: The Blockchain-Empowered Software System. IEEE Access. 6: 53019–53033. DOI: 10.1109/ ACCESS.2018. 2870644. ISSN 2169-3536. 2018.

[11] Corbyn, Zoë. "Decentralization: the next big step for the world wide web". The Observer Internet. United Kingdom. https://www.theguardian.com/technology/2018/sep/08/decentralisation-next-big-step-for-the-world-wide-web-dweb-data-internet-censorship-brewster-kahle. 2018.