Implementación de un nodo minero institucional en la red Ethereum 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 abierta y participativa de Argentina pensada para integrar servicios y aplicaciones sobre la Blockchain de Ethereum.

Las organizaciones, tanto públicas como privadas, pueden formar parte de Blockchain Federal Argentina, ejerciendo distintos roles de control dentro de la organización. También pueden desplegar aplicaciones sobre la plataforma.

El proyecto de investigación consiste en implementar un nodo Minero (en adelante nodo Sellador) en la Universidad Nacional de La Matanza, dentro de la red Blockchain Federal Argentina, para lo cual se celebrará un contrato de colaboración público-privada entre la UNLaM, representada por el Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) y el consorcio Blockchain Federal Argentina.

Este contrato hará a la UNLaM parte del mencionado consorcio y permitirá montar un nodo Sellador dentro de la infraestructura Blockchain-BFA. En el marco de este proyecto, se desarrollará e implementará una dApp (Aplicación Distribuida) que quedará disponible para su uso libre para toda la comunidad académica.

La relevancia de este trabajo radica en la importancia que tiene para una institución formar parte de una red con las características de BFA. Hasta el momento, la UNLaM, no forma parte de BFA ni de otras plataformas similares.

Palabras clave:
Ethereum. Blockchain. Nodo Sellador. Contrato Inteligente. BFA.

CONTEXTO

Este proyecto de investigación está siendo presentado como un Programa de Incentivos a Docentes Investigadores de la Secretaría de Políticas Universitarias (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 implementación de un nodo sellador en la UNLaM dentro de la red Blockchain Federal Argentina y de una dApp para uso académico.

1. INTRODUCCIÓN

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 [1].

Una Blockchain puede ser vista como un gran libro contable. Allí solo pueden ingresarse nuevas entradas y las entradas anteriores no pueden ser modificadas ni eliminadas. Esas entradas se llaman transacciones, las cuales se van agrupando en bloques que se agregan sucesivamente a una cadena [2].

Cada uno de los bloques hace referencia al bloque inmediatamente anterior de modo que, si alguna transacción intenta ser modificada, esa referencia cambia y ese bloque y todos los posteriormente agregados son inválidos.

Por lo anteriormente dicho, si quisiéramos corregir información ya registrada, solo lo podemos hacer mediante el agregado de nueva información. Los datos originales siempre van a permanecer en la cadena y pueden ser inspeccionados en cualquier momento.

Blockchain puede ser vista también como una base de datos pública y distribuida que contiene un histórico irrefutable de información. La Blockchain (esa cadena de nodos compuesta por transacciones) no se encuentra almacenada en un solo servidor centralizado, sino que se encuentra replicada en un gran conjunto de dispositivos conocidos como nodos que conforman lo que se conoce como red de pares.

Cada vez que se agrega una nueva transacción, ésta se integra a un bloque y posteriormente se agrega a la cadena y ésta es actualizada en todas las réplicas de los nodos. Blockchain no solo está protegida por este modelo de red descentralizada, sino que también está validada por métodos criptográficos que garantizan que nada pueda ser borrado o alterado sin que todos los usuarios puedan darse cuenta de ello.

Blockchain permite garantizar la identidad de las partes involucradas, ya que todas las transacciones son firmadas criptográficamente. Se puede certificar la fecha y hora de cada transacción. La información es inmutable e inalterable. Además, toda la información almacenada en la cadena es completamente auditable. Blockchain funciona sin intermediarios, esto es, no hace falta una persona, empresa o institución que legitime la información guardada en la cadena.

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].

Ethereum provee una criptomoneda que se llama “ether”. Se pueden intercambiar ether entre cuentas diferentes (es decir, puede ser utilizado como intercambio de valor). Pero existe una bifurcación de la cadena de bloques de Ethereum a partir de julio de 2016, que dio como resultado dos líneas de Ethereum activas: Ethereum y Ethereum Clásico.

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 que realizan contratos inteligentes son escritos en lenguajes de programación de alto nivel de tipo Turing completos, como Solidity, que es un lenguaje de alto nivel orientado a contratos. Su sintaxis es similar a la de JavaScript y está enfocado específicamente a la EVM para crear los contratos inteligentes [5].

Un contrato inteligente (en inglés Smart Contract) 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.

Un contrato inteligente es un programa que “vive” en un sistema no controlado por ninguna de las partes, y que ejecuta un contrato automático el cual funciona como una sentencia

if-then (si-entonces) de cualquier otro programa de computadora. Cuando se dispara una condición preprogramada, no sujeta a ningún tipo de valoración humana, el contrato inteligente ejecuta la cláusula contractual correspondiente.

Los Smart Contract tienen como objetivo brindar una seguridad superior a un contrato tradicional y reducir los costos de transacción asociados a la contratación. La transferencia de valor digital mediante un sistema que no requiere confianza (por ejemplo, bitcoins) abre la puerta a nuevas aplicaciones que pueden hacer uso de los contratos inteligentes.

Los contratos inteligentes se componen de una interfaz de usuario y a veces emulan la lógica de las cláusulas contractuales.

Los desarrolladores pueden escribir la lógica de negocio y acuerdos en forma de contratos inteligentes, los cuales se ejecutan automáticamente cuando sus condiciones son satisfechas por ambas partes e informadas a la red. Estos contratos pueden almacenar datos, enviar y recibir transacciones e incluso interactuar con otros contratos, independientemente de cualquier control.

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 [4]. 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 hace el proceso de verificar 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 [7].

Remix es un entorno de desarrollo, compilación y despliegue de contratos inteligentes basado en un navegador web.

Una dApp es una aplicación distribuida sobre la Ethereum Blockchain. Esta tiene múltiples capas y componentes y no depende de un sistema centralizado, sino que depende de la comunidad de usuarios que la utiliza. 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].

Blockchain Federal Argentina es una plataforma multiservicios abierta y participativa pensada para integrar servicios y aplicaciones sobre blockchain [9]. 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 estudiarán y analizarán los derechos y obligaciones emanados de la firma del contrato de colaboración público-privada que se debería celebrar 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 dApp (Aplicación Distribuida) en los servidores de la UNLaM. Esto se hará mediante el desarrollo de un Contrato Inteligente (Smart Contract), siguiendo con el desarrollo de una API y por último el diseño, desarrollo e implementación de una aplicación Front-end.

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.

Se redactará un informe integral final con el contrato y el software implementado y desarrollado acompañado de recomendaciones y buenas prácticas 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.

El objetivo principal incluye la celebración de un contrato de colaboración público-privada entre la Universidad Nacional de La Matanza, representada por el Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) y el consorcio Blockchain Federal Argentina (BFA). Esto otorgará los permisos necesarios por parte de Blockchain Federal Argentina para montar un nodo Sellador sobre su red, perteneciente a la UNLaM. Luego se procederá a su implementación.

El objetivo secundario incluye el desarrollo e implementación de una dApp (Aplicación Distribuida) perteneciente a la UNLaM. Dicha dApp funcionará sobre la Blockchain de BFA.

4. FORMACIÓN DE RECURSOS HUMANOS

El equipo está integrado por docentes-investigadores que pertenecen a distintas cátedras de la carrera de Ingeniería en 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 su tutor es el Mg. Jorge Eterovic, integrante del proyecto de investigación.

5. BIBLIOGRAFÍA

[1] Albert Szmigielski; Bitcoin Essentials; ISBN 978-1-78528-197-6; Ed. Packt Publishing Ltd.; Birmingham, UK. 2016

[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; 2020. https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[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