



Código	FPI-002
Objeto	Protocolo de presentación de proyectos de investigación SIGEVA UNLaM
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	4
Vigencia	12/11/2021

Unidad Ejecutora:
Departamento de Ingeniería e Investigaciones Tecnológicas

Programa de acreditación:
CyTMA2

Título del Programa de Investigación¹:

Director del Programa:

Título del proyecto de investigación:
Desarrollo de Smart Contracts e interacción con eventos de Blockchain

PIDC:

PII

Director del proyecto:
Lic. Gigante, Nora

Co-Director del proyecto:

Integrantes del equipo:
Ing. Uran Acevedo, Jonatan
Lic. Rusticcini, Héctor Alejandro

Fecha de inicio:
01-01-2022

Fecha de finalización:
31-12-2023

¹ Completar solo en caso de que el presente proyecto se encuadre en el marco de un Programa de Investigación

1-Cuadro resumen de horas semanales dedicadas al proyecto por parte de director e integrantes del equipo de investigación:²

Rol del integrante	Nombre y Apellido	Cantidad de horas semanales dedicadas al proyecto
Director	Nora Gigante	4
Co-director		
Director de Programa		
Docente-investigador UNLaM	Jonatan Uran Acevedo Héctor Alejandro Rusticcini	4 4
Investigador externo ³		
Asesor-Especialista externo ⁴		
Graduado de la UNLaM ⁵		
Estudiante de carreras de posgrado (UNLaM) ⁶		
Alumno de carreras de grado (UNLaM) ⁷		
Personal de apoyo técnico administrativo		

2-Plan de investigación

2. Tipo de actividad I+D:

Investigación Aplicada.

2.1. Resumen del Proyecto:

El proyecto consiste en crear una Aplicación distribuida y sobre ésta crear y desplegar varios smart contracts (contratos inteligentes) a medida.

Se mostrará la interacción desde la web con los eventos causados por los smart contracts dentro de la Blockchain y la respuesta a dichos eventos.

También se desarrollará una capacitación para ser impartida a un grupo de alumnos de la Universidad Nacional de La Matanza (UNLaM), con determinados conocimientos previos.

2.2. Palabras clave:

Contrato inteligente, Cadena de bloques, eventos

2.3 Resumen del Proyecto (inglés):

The project create a Distributed Application and create and deploy some custom smart contracts.

It show the interaction from the web with the events caused by the smart contracts within the Blockchain.

² Incluir todos los integrantes del equipo de investigación, agregando tantas filas para cada rol de integrante del equipo de investigación como sea necesario.

³ Deberá adjuntar FPI 28, 29 y 30 debidamente firmados.

⁴ Idem nota 2.

⁵ Idem nota 2

⁶ Adjuntar certificado de materias aprobadas de estudiantes de carrera de posgrado.

⁷ Adjuntar certificado de materias aprobadas de estudiantes de carrera de grado.

Training will also be developed to be given to a group of students from the Universidad Nacional de La Matanza (UNLaM).

2.4 Palabras clave (inglés):

Smart Contract, Blockchain, events

2.5 Disciplina desagregada:

1705 – Informática – Redes de Computación, Teleprocesamiento

2.6 Campo de aplicación

12 – Otros campos

2.7 Especialidad:

-

2.8 Estado actual del conocimiento:

La correcta implementación de un Smart Contract y el desarrollo de una Aplicación Distribuida, implican un profundo conocimiento sobre desarrollo de software utilizando técnicas y herramientas informáticas

Hoy en día existe una gran demanda de expertos a nivel mundial con conocimientos sobre arquitectura de Aplicaciones Distribuidas.

Existen casos conocidos de arquitecturas de dApps mal diseñadas y con un pobre desarrollo que han resultado en la pérdida de millones de dólares.

También sucede que existe actualmente una falta de información detallada en esta temática, sobre todo en idioma español y aún más, procedente de ámbitos académicos.

2.9. Problemática a investigar:

En primer lugar, se creará e implementará una Aplicación Distribuida (dApp) y junto con ésta, un conjunto de Smart Contracts.

Por otra parte, se desarrollará una capacitación para ser impartida a un grupo de alumnos de la Universidad Nacional de La Matanza (UNLaM), con determinados conocimientos previos.

2.10. Objetivos:⁸

Objetivo principal: creación e implementación de una dApp y un conjunto de Smart Contracts.

Objetivo secundario: desarrollar una capacitación para ser dictada en la Universidad Nacional de La Matanza (UNLaM).

2.11. Marco teórico:

¿Qué es una Blockchain?

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.

⁸ Detallar objetivo general y objetivos específicos.

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.

Cada uno de los bloques hace referencia al bloque inmediatamente anterior de modo que, si alguna transacción pudiera 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 agrega 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 atravesada 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.

¿Qué es Ethereum?

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).

Ethereum provee una criptomoneda que se llama ether. Se puede intercambiar ether entre cuentas diferentes (es decir, puede ser utilizado como intercambio de valor).

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 LISP, ensamblador y bitcoin script.

Los programas que realizan contratos inteligentes son escritos en lenguajes de programación de alto nivel de tipo Turing completos, como Solidity, que siguen la metodología de diseño por contrato para crear los contratos inteligentes.

Ethereum utiliza como criptomoneda al ether, esta sirve como intercambio de valor y también sirve como "combustible" para ejecutar los contratos inteligentes.

¿Qué es un Smart Contract?

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). 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 ordenador. Cuando se dispara una condición pre-programada, 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 costos de transacción asociados a la contratación. La transferencia de valor digital mediante un sistema que no requiere confianza (ej. 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.

¿Qué es Solidity?

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.

Solidity es un lenguaje de scripting tipado estáticamente (esto quiere decir que las variables deben ser declaradas junto con su tipo antes de ser utilizadas) que hace el proceso de verificar y hacer cumplir las restricciones en tiempo de compilación (antes de que se ejecute el programa).

Solidity es un lenguaje Turing Complete

Esto significa que es un lenguaje de programación que puede simular una Máquina de Turing Universal. En resumen, es capaz de realizar cualquier cálculo computacional con los recursos adecuados.

Solidity cuenta con un IDE oficial llamado Remix. Un IDE (Integrated Development Environment), entorno de desarrollo integrado, es una aplicación que proporciona servicios para facilitar al programador el desarrollo de software.

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

¿Qué es una dApp?

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. Una dApp puede ser web o mobile.

en pocas palabras, una dApp es una aplicación que tiene su backend construido sobre contratos inteligentes, en contraposición con los backend tradicionales.

Las dApps pueden ser categorizadas en base a su función financiera:

Puramente financieras: Se ocupan de cuestiones puramente monetarias (ej. Ayudan a los usuarios a administrar su dinero)

Semi-financieras: Se ocupan de intercambio de dinero por artículos o servicios.

No financieras: No involucran dinero, por ejemplo, sistemas de votación, gubernamentales, etc.

BLOQUES

Los bloques son lotes de transacciones con un hash del bloque anterior en la cadena. Esta vincula bloques juntos (en una cadena) porque los hashes derivan criptográficamente de los datos del bloque. Esto previene el fraude, porque un cambio en cualquier bloque del historial invalidaría todos los siguientes bloques; asimismo, todos los hashes subsecuentes cambiarían y todos los que ejecutasen la blockchain lo notarían.

Organizamos las transacciones en bloques para garantizar que todos los participantes en la red Ethereum mantienen un estado sincronizado y están de acuerdo sobre el historial preciso de las transacciones. Esto significa que decenas (o cientos) de transacciones se confirman, acuerdan y sincronizan a la vez.

Al separar los commits (formación exitosa de una cadena), damos a todos los participantes de la red el tiempo suficiente para llegar a un consenso: aunque las solicitudes de transacción ocurren docenas de veces por segundo, los bloques en Ethereum se confirman aproximadamente una vez cada 15 segundos.

Para preservar el historial de transacciones, los bloques se ordenan estrictamente (cada nuevo bloque creado contiene una referencia a su bloque predecesor) y las transacciones dentro de los bloques también se ordenan de manera estricta. Excepto en casos raros o en un momento determinado, todos los participantes en la red están de acuerdo en el número exacto y en el historial de los bloques. Además, están trabajando para agrupar los requerimientos de transacción en tiempo real en el próximo bloque.

Una vez que un minero ensambla un bloque en la red, este se propaga al resto de la red; todos los nodos agregan este bloque al final de su blockchain y la minería continúa. El proceso exacto de ensamblaje de bloques (minería) y el proceso de compromiso/consenso se especifican actualmente mediante el protocolo denominado "Prueba de trabajo" de Ethereum.

Prueba de Trabajo

Los nodos de minería tienen que gastar una cantidad variable y sustancial de energía, tiempo y potencia computacional para producir un "certificado de legitimidad" por un bloque que ellos proponen para la red. Esto ayuda a proteger a la red de ataques de spam/denegación de servicios, entre otras cosas*, ya que los certificados son costosos de producir.

Otros mineros que se enteran de la existencia de un nuevo bloque con un certificado válido de legitimidad deben* aceptar el nuevo bloque como el siguiente bloque canónico en la blockchain.

La cantidad exacta de tiempo que necesita cualquier minero para producir este certificado es una variable aleatoria con alta variabilidad. Esto garantiza que es improbable que dos mineros produzcan validaciones para un nuevo bloque propuesto simultáneamente; cuando un minero produce y propaga un nuevo bloque certificado, los demás pueden estar casi seguros de que el bloque será aceptado por la red como un nuevo bloque canónico en la blockchain sin conflicto (aunque hay un protocolo para resolver los conflictos, así como en el caso de que dos blockchains certificadas se produzcan casi simultáneamente).

¿Qué hay en un Bloque?

Timestamp: Es el horario en el que el bloque se minó.

Número de bloque: Es la longitud de la blockchain en bloques.

Dificultad: Es el esfuerzo que requirió minar el bloque.

mixHash: Un identificador único para el bloque.

Parent hash: Identificador único del bloque predecesor (así es como los bloques están enlazados en una cadena).

Lista de transacciones: Son las transacciones incluidas en el bloque.

State root: Es el estado completo del sistema; incluye los saldos de las cuentas, el almacenamiento de contratos, el código del contrato y los nonces de las cuentas.

Nonce: Es un hash que cuando se combina con un mixHash, comprueba que el bloque ha pasado por la Prueba de trabajo.

Los bloques tienen limitaciones de tamaño. Cada bloque tiene un límite de gas, que establecen colectivamente la red y los mineros: la cantidad total de gas consumida por todas las transacciones en el bloque debe ser inferior al límite de gas del bloque. Esto es importante porque garantiza que los bloques no pueden ser tan grandes como queramos. Si los bloques pudieran ser tan grandes como quisiéramos, los nodos completos de menor rendimiento poco a poco dejarían de estar al día con la red debido a los requisitos de espacio y velocidad. El límite de gas del bloque en el bloque 0 fue inicializado en 5000; cualquier minero que extraiga un nuevo bloque puede alterar el límite del gas hasta aproximadamente un 0,1% en cualquier dirección desde el límite de gas del bloque primario. El límite de gas a partir de noviembre de 2018 es de aproximadamente 8 000 000.

TRANSACCIONES

Las transacciones son instrucciones firmadas criptográficamente que se emiten desde cuentas. Una cuenta iniciará una transacción para actualizar el estado de la red Ethereum. La transacción más sencilla es transferir ETH de una cuenta a otra.

Una transacción de Ethereum hace referencia a una acción iniciada por una cuenta de propiedad externa, en otras palabras, una cuenta controlada por un humano, no un contrato. Por ejemplo, si Bob le envía 1 ETH a Alice, este debe debitarse de la cuenta de Bob y acreditarse en la cuenta de Alice. Esta acción modificadora del estado de la red tiene lugar en una transacción.

Las transacciones, que modifican el estado de la EVM, se deben transmitir a toda la red. Cualquier nodo puede transmitir una solicitud de una transacción que se va ejecutar en la EVM; a continuación, un minero ejecutará la transacción y propagará la modificación de estado que resulte de ello al resto de la red.

Las transacciones necesitan una comisión y deben minarse para convertirse en transacciones válidas. Para simplificar esta descripción general, abarcaremos las comisiones de gas y el minado por separado.

Una transacción enviada incluye la siguiente información:

destinatario: La transacción destinataria (en caso de que sea una cuenta de propiedad externa, la transacción transferirá valor. Si se trata de un contrato, la transacción ejecutará el código del contrato)

firma: Identificador del remitente. Se genera cuando, mediante la clave privada, se firma la transacción y se confirma que el remitente la ha autorizado

valor: Cantidad de ETH que el remitente transfiere al destinatario (en WEI, una denominación de ETH)

datos: Campo opcional en el que se incluyen datos arbitrarios.

LímiteDeGas: Cantidad máxima de unidades de gas que puede consumir la transacción. Las unidades de gas representan pasos computacionales

PrecioDeGas: La comisión que el remitente paga por unidad de gas.

El gas es una referencia al trabajo computacional que se necesita para que el minero procese la transacción.

Los usuarios tienen que pagar una comisión por ese trabajo computacional. El límiteDeGas y el precioDeGas determinan la comisión de gas máxima que se le paga al minero.

GAS Y TARIFAS

El gas es esencial para la red de Ethereum. Se trata del combustible que le permite operar, de la misma manera que un vehículo necesita gasolina para funcionar.

El gas hace referencia a la unidad que mide la cantidad de esfuerzo computacional requerida para ejecutar operaciones específicas en la red de Ethereum.

Como cada transacción de Ethereum requiere recursos computacionales para ejecutarse, cada transacción requiere una comisión. El gas hace referencia a la comisión necesaria para llevar a cabo una transacción en Ethereum con éxito.

En esencia, las comisiones de gas son pagadas en la moneda nativa de Ethereum, es decir, el ether (ETH). Los precios del gas están indicados en Gwei, que es una denominación de ETH; cada Gwei equivale a 0,000000001 ETH (10⁻⁹ ETH). Por ejemplo, en lugar de decir que el gas cuesta 0,000000001 Ether, puedes decir que cuesta 1 Gwei.

En resumen, las comisiones de gas ayudan a mantener la red de Ethereum segura. Al requerir una comisión para cada cálculo computacional ejecutado en la red, evitamos que algunas personas envíen spam a la red. Para prevenir la generación de hostiles bucles infinitos o accidentales, así como de otros desperdicios computacionales generados en el código, cada transacción debe establecer un límite del número de pasos computacionales de código que puede utilizar. La unidad fundamental del cálculo computacional es el "gas".

Aunque una transacción incluye un límite, el gas que no se utilice en la transacción se le devuelve al usuario.

2.12. Hipótesis de trabajo o los supuestos implícitos (según corresponda al diseño metodológico) :⁹

Se creará e implementará una Aplicación Distribuida (dApp) y junto con ésta, un conjunto de Smart Contracts.

También se desarrollará una capacitación para ser impartida a un grupo de alumnos de la Universidad Nacional de La Matanza (UNLaM), con determinados conocimientos previos.

2.13. Metodología:

Se estudiará y explicará la teoría que sustenta el desarrollo del presente trabajo.

Luego se procederá a instalar el hardware necesario para desarrollar y desplegar la App. Seguido a esto se implementará el software necesario.

Se implementará una dApp (Aplicación Distribuida) perteneciente a la UNLaM. Esto se hará mediante el desarrollo de un conjunto de Contrato Inteligentes (Smart Contracts), siguiendo por el desarrollo de una aplicación Frontend.

Se desarrollarán informes de avances que incluyan el progreso del proyecto y las conclusiones de cada una de las actividades que forman parte de este.

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.

2.14. Bibliografía:

Ethereum - <https://www.ethereum.org>

Solidity - <https://solidity-es.readthedocs.io/>

Contrato Inteligente - https://es.wikipedia.org/wiki/Contrato_inteligente

2.15. Programación de actividades (Gantt):¹⁰

Referencias de Responsables: Gigante Nora (1), Uran Acevedo Jonatan (2), Rusticcini ALejandro (3).

* Las referencias de responsables en la siguiente tabla se refiere a los responsables finales de la tarea, considerando que en determinadas tareas participan de forma grupal diferentes integrantes.

2022	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
ETAPA I	X	X	X	X	X	X	X	X	X	X	X	X
Análisis Inicial, Revisión bibliográfica	X (1) (2) (3)	X (1) (2) (3)	X (1) (2) (3)	X (1) (2) (3)								
Instalación del hardware					X (2)	X (2)						
Construcción de la dApp - Analisis							X (2) (3)	X (2) (3)	X (2) (3)			

⁹ En proyectos de desarrollo tecnológico puede ser reemplazada una hipótesis de trabajo por la propuesta de solución al problema de investigación mediante el diseño de un prototipo o elemento equivalente.

¹⁰ Definir la programación de actividades para cada objetivo específico, y las personas responsables de su ejecución.

Diseño										X (2) (3)	X (2) (3)	X (2) (3)
Redacción de Informe							X (1)(2)				X (1)(2)	X (1)(2)

2023	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
ETAPA I	X	X	X	X	X	X	X	X	X	X	X	X
Diseño	X (2) (3)											
Desarrollo		X (2) (3)	X (2) (3)	X (2) (3)	X (2) (3)	X (2) (3)	X (2) (3)					
prueba								X (2) (3)	X (2) (3)	X (2) (3)		
Implementación Final											X (2) (3)	X (2) (3)
Redacción de Informe							X (1)(2)				X (1)(2)	X (1)(2)

2.16. Resultados en cuanto a la producción de conocimiento:

El presente proyecto traerá a la UNLaM una serie de conocimientos hasta el momento no abordados por ninguna de sus cátedras debido al carácter actual e innovador de la rama del conocimiento que se tratará.

Como parte del proyecto se organizarán actividades de apoyo a la formación en la temática.

2.17. Resultados en cuanto a la formación de recursos humanos:

El equipo está integrado por docentes investigadores que pertenecen a distintas cátedras de la carrera de Ingeniería en Informática y Tecnicatura en desarrollo Web de la UNLaM.

Como parte del proyecto se organizarán actividades de apoyo a la formación en la temática.

Cabe destacar que el proyecto no tiene alumnos que colaboren en el mismo, debido a que no es una temática que se enseñe académicamente a los mismos aún. No se descarta en un futuro sumar colaboradores alumnos, una vez que la temática esté más trabajada académicamente.

2.18. Resultados en cuanto a la difusión de resultados:

Se pretende difundir los resultados en diferentes Congresos:

- WICC – Workshop de Investigadores en Ciencia de la Computación.
- CoNalISI – Congreso Nacional de Ingeniería Informática y en Sistemas de Información.
- CACIC – Congreso Argentino de Ciencias Informáticas y Computación.
- Otros Congresos relacionados con la temática.

2.19. Resultados en cuanto a transferencia hacia las actividades de docencia y extensión:

- Los resultados del trabajo de investigación aportarán conocimientos y material para esta nueva temática que aún no es abordada por la carrera Ingeniería en Informática y las Tecnicaturas Universitarias en Desarrollo Web y Móvil.
- Se brindarán charlas y jornadas de capacitación a alumnos, graduados y docentes de Ingeniería Informática, Tecnicaturas Universitarias en Desarrollo Web y para Dispositivos Móviles y carreras afines.

2.20. Resultados en cuanto a la transferencia de resultados a organismos externos a la UNLaM:

Se espera poder brindar cursos, charlas y jornadas de capacitación a organismos privados y públicos involucrados a la temática, de todo el país.

2.21. Vinculación del proyecto con otros grupos de investigación del país y del exterior:

Se espera vincular el proyecto con grupos de investigación de otras Universidades Nacionales y Privadas con temáticas relacionadas.

2.22. Destinatarios:

Tipo de destinatario		Subtipo de destinatario ¹¹	¿Cuál? Especificar	Demandante ¹²	Adoptante ¹³
Sector Gubernamental	Gobiernos	Del Poder Ejecutivo nacional			
		Del Poder Ejecutivo provincial			
		Del Poder Ejecutivo municipal			
	Otras Instituciones gubernamentales	Poder Legislativo en sus distintas jurisdicciones			
		Poder Judicial en sus distintas jurisdicciones			
Sector Salud		Hospitales, centros comunitarios de salud y otras entidades del sistema de atención			
Sector Educativo		Sistema universitario	X	X	X
		Sistema de educación básica y secundaria			
		Sistema de educación terciaria			
Sector Productivo		Empresas			
		Cooperativas de trabajo y producción			
		Asociaciones del Sector			
Sociedad Civil		ONG's y otras organizaciones sin fines de lucro			
		Comunidades locales y particulares			

¹¹ Marcar con una X

¹² Demandante: entidad administrativa de gobierno nacional, provincial o municipal constituida como demandante externo de las tecnologías desarrolladas, que determina la necesidad del proyecto por su importancia social. Marcar con una X

¹³ Adoptante: beneficiario o usuario en capacidad de aplicar los resultados desarrollados (organismos gubernamentales de ciencia y tecnología nacionales o provinciales; universidades e institutos universitarios de gestión pública o privada; empresas públicas o privadas; entidades administrativas de gobierno nacionales, provinciales o municipales; entidades sin fines de lucro; hospitales públicos o privados; instituciones educativas no universitarias; y organismos multilaterales. Marcar con una X

3-Recursos Existentes¹⁴

Descripción/ concepto	Cantidad	Observaciones

4-Recursos financieros¹⁵

	Rubro	Año 1	Año 2	Total
Gastos de capital (equipamiento)	a) Equipamiento (1)	\$ 10000,00	\$ 10000,00	\$ 20000,00
	b) Licencias (2)			
	c) Bibliografía (3)			
	Total Gastos de Capital	\$ 10000,00	\$ 10000,00	\$ 20000,00
Gastos corrientes (funcionamiento)	d) Bienes de consumo			
	e) Viajes y viáticos (4)	\$ 10000,00	\$ 10000,00	\$ 20000,00
	f) Difusión y/o protección de resultados (5)			
	g) Servicios de terceros (6)			
	h) Otros gastos (7)			
	Total Gastos Corrientes	\$ 10000,00	\$ 10000,00	\$ 20000,00
	Total Gastos (Capital + Corrientes)	\$20000,00	\$20000,00	\$40000,00

Ejemplos de equipamiento: Servidor en la Nube AWS.

Ejemplos de viáticos: CACIC, WICC.

Aclaraciones sobre rubros del presupuesto

1 Equipamiento: Equipamiento, repuestos o accesorios de equipos, etc.

2 Licencias: Adquisición de licencias de tecnología (software, o cualquier otro insumo que implique un contrato de licencia con el proveedor).

3 Bibliografía: En el caso de compra de bibliografía, ésta no debe estar accesible como suscripción en la Biblioteca Electrónica.

4 Viajes y viáticos: Viajes y viáticos en el país: Gastos de viajes, viáticos de campaña y pasantías en otros centros de investigación estrictamente listados en el proyecto. Gastos de viaje en el exterior: (no deberán superar el 20% del monto del proyecto).

5 Difusión y/o protección de resultados: Ej.: (Gastos para publicación de artículos, edición de libros inscripción a congresos y/o reuniones científicas).

6 Servicios de terceros: Servicios de terceros no personales (reparaciones, análisis, fotografía, etc.).

7 Otros gastos: Incluir, si es necesario, gastos a realizar que no fueron incluidos en los otros rubros.

4.1 Origen de los fondos solicitados

Institución	% Financiamiento
UNLaM	
Otros (indicar cuál)	

¹⁴ Antes de confeccionar el presupuesto del proyecto, será necesario que el Director incluya en esta tabla si dispone de recursos adquiridos con fondos de proyectos anteriores (equipamiento, bibliografía, bienes de consumo, etc.) a ser utilizados en el proyecto a presentar, y además se recomienda consultar en la Unidad académica la disponibilidad de recursos existentes factibles de ser utilizados en el presente proyecto.

¹⁵ Justificar presupuesto detallado. Para compras de un importe superior a \$15000.- se requieren tres presupuestos. (Resolución Rectoral N°177/2021.)



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

Departamento: DIIT

Programa de acreditación:

CyTMA2

Programa de Investigación¹:

Código del Proyecto:

C2-ING-096

Título del proyecto

Desarrollo de Smart Contracts e interacción con eventos de Blockchain

PIDC:

Secretaría De Ciencia Y Tecnología

PII:

Ingeniería e Investigaciones Tecnológicas

Director:

Mst. Gigante, Nora C.

Director externo:

Codirector:

Integrantes:

Ing. Uran Acevedo, Jonatan

Lic. Rusticcini, Héctor Alejandro

Investigador Externo, Asesor- Especialista, Graduado UNLaM:

Alumnos de grado: (Aclarar si tiene Beca UNLaM/CIN)

Alumnos de posgrado:

Resolución Rectoral de acreditación: N°

118/323

Fecha de inicio:

01/01/2022

Fecha de finalización:

31/12/23

¹ Los Programas de Investigación de la UNLaM están acreditados con resolución rectoral, según lo indica la Resolución HCS N° 014/15 sobre **Lineamientos generales para el establecimiento, desarrollo y gestión de Programas de Investigación a desarrollarse en la Universidad Nacional de La Matanza**. Consultar en el departamento académico correspondiente la inscripción del proyecto en un Programa acreditado.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

A. Desarrollo del proyecto (adjuntar el protocolo)

A.1. Grado de ejecución de los objetivos inicialmente planteados, modificaciones o ampliaciones u obstáculos encontrados para su realización (desarrolle en no más de dos (2) páginas)

Con respecto al primer objetivo, crear una aplicación distribuida (DApp) que interactúe con contratos inteligentes (*Smart Contracts*), éste ha sido alcanzado. Puntualmente se ha diseñado y construido durante la presente investigación, una aplicación distribuida que interactúa con dos *Smart Contracts*, los cuales han sido desarrollados por el propio equipo de investigación.

Para el desarrollo de la aplicación se ha utilizado el *framework* Next de React (Javascript). La aplicación, del tipo *ToDo list*, permite gestionar ítems en una lista y específicamente, durante el proceso de inserción de nuevos ítems, la misma requiere la interacción con dos *Smart Contracts*.

Los *Smart Contracts* fueron desarrollados en *Solidity*, un lenguaje de programación Orientado a Objetos diseñado para desarrollar contratos inteligentes que se ejecutan en Ethereum y que han sido desplegados en una blockchain de Ethereum.

Cabe recordar que una de las características principales de una red blockchain consiste en que la información registrada en ella es validada por un sistema criptográfico descentralizado y en la práctica inalterable.

Durante la interacción entre la aplicación y los *Smart Contracts*, se solicita que el usuario proporcione ether, a modo de pago (puede no tener valor monetario realmente), para que la inserción sea aceptada. Una vez que el usuario proporciona el ether, la acción es aceptada y se procesa, dando como resultado la adición de un



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

nuevo ítem. Esta transacción queda registrada en la blockchain y es visible por todo aquel que ingrese a la red, además de ser inalterable en el tiempo.

Con el desarrollo y despliegue de esta aplicación distribuida se ha comprobado la factibilidad de implementar aplicaciones simples y performantes utilizando contratos inteligentes almacenados en una red de tipo Blockchain en este caso particular Ethereum.



Con respecto al segundo objetivo, construir un espacio de capacitación sobre las tecnologías investigadas, especialmente el uso de Blockchain y su aplicación práctica en aplicaciones distribuidas; con el objeto de ser impartida a Docentes y Alumnos de la Universidad Nacional de La Matanza (UNLaM), se diseñó y construyó un plan de capacitación destinado a al conjunto de Alumnos y Docentes de la Institución involucrados en carreras de Pre-Grado, Grado y Posgrado relacionada con Tecnología. En particular, se analizaron los planes de estudio de las carreras



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

Tecnicatura en Desarrollo Web, Tecnicatura en Desarrollo de Aplicaciones Móviles e Ingeniería en Informática, dictadas en nuestra casa de estudios, para indagar sobre la inclusión de las tecnologías involucradas en esta investigación. Como conclusión, se observó un espacio vacante en el tratamiento de conocimientos relacionados sobre la temática y se diseñó un espacio de capacitación para cubrirlo.

Dicha capacitación se programó para ser realizada en el marco del Conversatorio de Proyectos Tecnológicos evento que, a pedido del Departamento, se ha pospuesto para el Año 2024 por lo que, al momento de finalización del proyecto, su ejecución se encuentra planificada para realizarse en el Primer Cuatrimestre 2024.

B. Principales resultados de la investigación

B.1. Publicaciones en revistas (informar cada producción por separado)

Artículo 1:	
Autores	
Título del artículo	
N° de fascículo	
N° de Volumen	
Revista	
Año	
Institución editora de la revista	
País de procedencia de institución editora	
Arbitraje	Elija un elemento.
ISSN:	
URL de descarga del artículo	
N° DOI	



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

B.2. Libros

Libro 1	
Autores	
Título del Libro	
Año	
Editorial	
Lugar de impresión	
Arbitraje	Elija un elemento.
ISBN:	
URL de descarga del libro	
N° DOI	

B.3. Capítulos de libros

Autores	
Título del Capítulo	
Título del Libro	
Año	
Editores del libro/Compiladores	
Lugar de impresión	
Arbitraje	Elija un elemento.
ISBN:	
URL de descarga del capítulo	
N° DOI	

B.4. Trabajos presentados a congresos y/o seminarios

Autores	



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

Título	
Año	
Evento	
Lugar de realización	
Fecha de presentación de la ponencia	
Entidad que organiza	
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	

B.5. Otras publicaciones

Autores	
Año	
Título	
Medio de Publicación	

C. Otros resultados. Indicar aquellos resultados pasibles de ser protegidos a través de instrumentos de propiedad intelectual, como patentes, derechos de autor, derechos de obtentor, etc. y desarrollos que no pueden ser protegidos por instrumentos de propiedad intelectual, como las tecnologías organizacionales y otros. Complete un cuadro por cada uno de estos dos tipos de productos.

C.1. Títulos de propiedad intelectual. Indicar: Tipo (marcas, patentes, modelos y diseños, la transferencia tecnológica) de desarrollo o producto, Titular, Fecha de solicitud, Fecha de otorgamiento

Tipo	Titular	Fecha de Solicitud	Fecha de Emisión
------	---------	--------------------	------------------



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

C.2. Otros desarrollos no pasibles de ser protegidos por títulos de propiedad intelectual. Indicar: Producto y Descripción.

Producto	Descripción

D. Formación de recursos humanos. Trabajos finales de graduación, tesis de grado y posgrado.

Completar un cuadro por cada uno de los trabajos generados en el marco del proyecto.

D.1. Tesis de grado

Director (apellido y nombre)	Autor (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis

D.2 Trabajo Final de Especialización

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha / En curso	Título de la tesis

D.2. Tesis de posgrado: Maestría

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha / En curso	Título de la tesis
Eterovic, Jorge	Urán Acevedo, Jonatan	Universidad de Buenos Aires	10(diez)	05/05/23	Implementación de un nodo minero



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

					institucional en la red Ethereum-BFA

D.3. Tesis de posgrado: Doctorado

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha / En curso	Título de la tesis

D.4. Trabajos de Posdoctorado

Director (apellido y nombre)	Posdoctorando (apellido y nombre)	Institución	Calificación	Fecha / En curso	Título del trabajo	Publicación

E. Otros recursos humanos en formación: estudiantes/ investigadores (grado/posgrado/ posdoctorado)

Apellido y nombre del Recurso Humano	Tipo	Institución	Período (desde/hasta)	Actividad asignada ²

² Descripción de la/s actividad/es a cargo (máximo 30 palabras)



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

F. Vinculación³: Indicar conformación de redes, intercambio científico, etc. con otros grupos de investigación; con el ámbito productivo o con entidades públicas. Desarrolle en no más de dos (2) páginas.

G. Otra información. Incluir toda otra información que se considere pertinente.

A través del proceso de desarrollo de la aplicación distribuida construida durante el devenir de la presente investigación, pudimos establecer una serie de puntos respecto de la tecnología involucrada.

Como punto principal pudimos comprobar que la tecnología investigada es accesible y aplicable en el desarrollo de aplicaciones distribuidas, incluso mediante productos de tipo *OpenSource* (productos de código abierto) como los utilizados, lo que abre un abanico de posibilidades para su inclusión tanto en proyectos comerciales como académicos. Por otra parte, se pudo comprobar que la utilización de tecnologías de *blockchain* como almacenamiento de información permiten realizar registros de transacciones en forma segura, posibilitando la auditoría de estas por cualquier interesado, y asegurando su inalterabilidad en el tiempo.

Asimismo, es destacable que el proceso desarrollado mediante el uso de ether es altamente performante, tomando sólo unos pocos segundos el registro de la transacción, a diferencia de otros procesos relevados donde el registro puede ser oneroso en tiempo.

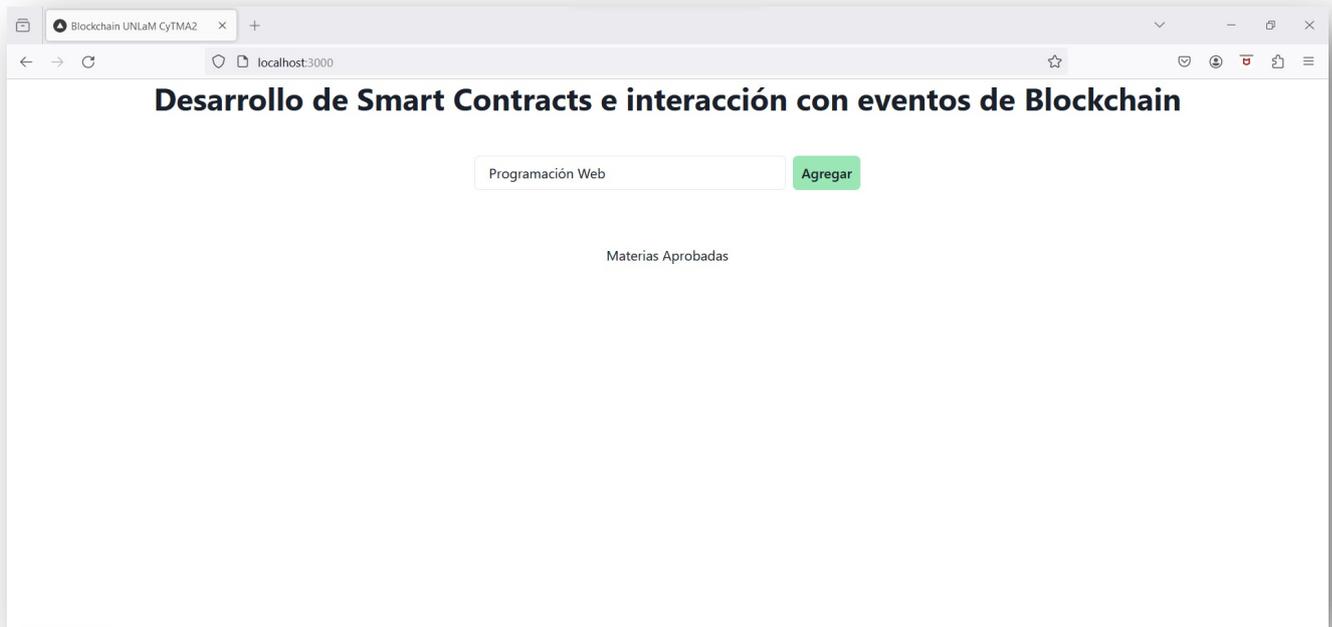
Por último, y no menos importante, el hecho de que los *Smart Contract* utilizados en la aplicación desarrollada han sido diseñados y codificados por los miembros de esta investigación, nos ha permitido establecer las bases prácticas y conceptuales necesarias para desarrollar la capacidad de gestionar la lógica aplicada en el proceso de aceptación de las transacciones.

³ Entendemos por acciones de “vinculación” aquellas que tienen por objetivo dar respuesta a problemas, generando la creación de productos o servicios innovadores y confeccionados “a medida” de sus contrapartes.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

Se adjunta captura del software funcionando:



La aplicación desarrollada se encuentra disponible a través de la siguiente URL:

<https://desarrollodesmartcontracts-8063861e2660.herokuapp.com/>

Además de lo expresado en el punto A1, y dada la conclusión acerca de la falta de la inclusión de estas tecnologías en el core curricular de las carreras ofrecidas por DIIT, se ha analizado la posibilidad de brindar un curso extracurricular.

Esto es, en función de la indagación sobre el nivel de inclusión de los temas de la presente investigación en los planes de estudio de las carreras relacionadas, se estableció el contenido temático mínimo necesario para introducir la tecnología tratada en los actores seleccionados y, por otra parte, los requisitos mínimos necesarios para que estos accedan a ellos y de esta manera establecer un piso de capacidades y/o conocimientos mínimos. A partir de esto se estableció que el curso se dirija a Docentes, Alumnos avanzados de Ingeniería en Informática y egresados de las carreras de las Tecnicaturas de Desarrollo Web y Móvil de la UNLaM.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

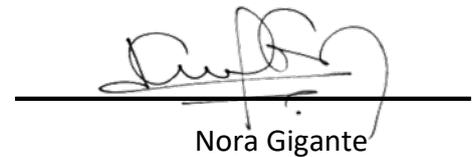
Este plan de capacitación se pensó con una duración establecida en 60 Hs. en opción didáctico-pedagógica a distancia, conformándose de 8 clases sincrónicas de 4 Hs de duración más actividades prácticas que insumen un mínimo de 28 Hs adicionales. Este curso tendrá un cupo de 25 participantes y está diseñado para ser dictado por un profesor disertante y un acompañante tutorial.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

H. Cuerpo de anexos:

- Anexo I: Copia de cada uno de los trabajos mencionados en los puntos B, C y D, y certificaciones cuando corresponda.⁴
- Anexo II:
 - FPI-013: Evaluación de alumnos integrantes. (si corresponde)
 - FPI-014: Comprobante de liquidación y rendición de viáticos. (si corresponde)
 - FPI-015: Rendición de gastos del proyecto de investigación acompañado de las hojas foliadas con los comprobantes de gastos.
 - FPI-035: Formulario de reasignación de fondos en Presupuesto.
- Anexo III: Alta patrimonial de los bienes adquiridos con presupuesto del proyecto (FPI 017)
- Nota justificando baja de integrantes del equipo de investigación.



Nora Gigante

Firma y aclaración
del director del proyecto.

Lugar y fecha: San Justo, 28 de febrero de 2024

⁴ En caso de libros, podrá presentarse una fotocopia de la primera hoja significativa o su equivalente y el índice.