Programa de Acreditación y Financiamiento de Proyectos de Investigación

Formulario Guía para la presentación de proyectos

I. Identificación del Proyecto

1.1. Datos Generales del Proyecto

Título:

Blockchain Aplicada a las Organizaciones Públicas y Privadas

Título abreviado:

BAOPP

Unidad Académica Ejecutora

CRUC – IUA – Facultad de Ingeniería

Responsable:	Decano de la FI del IUA Dr. VCom. José Cuozzo						
Dirección:	Calle:	Av. Fuerza Aérea				Nº :	6500
Localidad:	Córdoba		C.P.:	5016	Provincia:	Córdoba	
Tel.:	4435000	Correo Electrónico:		jcuozzo@iua.edu.ar			

Datos de contacto Director de Proyecto

Nombre:	Eduardo Casanovas						
DNI:	14.142.537						
Dirección:	Calle:	Av. Fuerza Aérea				Nº :	6500
Localidad:	Córdoba		C.P.:	5016	Provincia:	Córdoba	
Tel.:	4435000	Correo Electrónico:		ecasanovas@iua.edu.ar			

Otras Facultades de UNDEF u otras instituciones que intervienen

Responsable:							
Dirección:	Calle:					Nº :	
Localidad:			C.P.:		Provincia:		
Tel.:		Correo Electrónico:					

Tipo de línea de investigación[1]

Este proyecto se trata de una línea de investigación que es prioritaria para el Departamento de

[1] Aclarar e identificar si se trata de la continuidad de una línea de investigación o una línea prioritaria

Programa de Acreditación y Financiamiento de Proyectos de Investigación

Formulario Guía para la presentación de proyectos

Computación e Informática en las áreas de Seguridad Informática, Gestión de proyectos, Redes, aplicados a los desarrollos de software en el ámbito científico-técnico de la Universidad de la Defensa.

Características del Proyecto:

Tipo de Actividad[2]	Investigación Aplicada
Disciplina	Ciberdefensa y ciberseguridad
Campo de Aplicación	Ingeniería y Tecnología

Palabras clave

Blockchain, nodo, contrato inteligente

1.2. Dirección del Proyecto

Director: (Acompañar CVar o SIGEVA actualizado)

Apellido y Nombres	Categoría				Grado académico alcanzado
	UNDEF	Incentivos	CONICET	RPIDFA	
Eduardo Casanovas	Clase Id Grupo C Cat. 3				Maestría en Ciencias de la Ingeniería

Codirector: (Acompañar CVar o SIGEVA actualizado)

Apellido y Nombres	Categoría				Grado académico alcanzado
	UNDEF	Incentivos	CONICET	RPIDFA	
Fernando Boiero					Especialista en Seguridad Informática

1.3. Duración del Proyecto:

Fecha de Inicio	**Octubre 2018**
Fecha de Finalización	**Octubre 2019**
Duración prevista en meses (máximo 12 meses)	**12**

II. Integrantes Equipo de Trabajo

2.1 Recursos Humanos

[2] Investigación Básica / Investigación Aplicada / Desarrollo Experimental / Innovación Tecnológica.

Programa de Acreditación y Financiamiento de Proyectos de Investigación

Formulario Guía para la presentación de proyectos

Integrantes Equipo de Trabajo (Acompañar CV abreviado de c/u)

Apellido y Nombres	Docente/Investigador (cargo/área de trabajo/facultad)	Estudiante (condición/nivel de carrera)	Personal de Apoyo y Técnico (función/lugar)	Otra Facultad UNDEF	Otras Instituciones (especificar)
Carlos Tapia	Docente en Ing en Informática y Esp. en Seguridad Informática - Depto. Computación e Informática – FI – CRUC – IUA	Especialista en Seguridad Informática			
Sofía Pérez	Docente Investigador en Ing en Informática - Depto. Computación e Informática – FI – CRUC – IUA	Ingeniera de Sistemas			
Jose Ignacio Casanovas	Docente Adscripto Ing. en Informática - Depto. Computación e Informática – FI – CRUC – IUA	MSc in management ESSEC Business School			
Adrián Lezama	Docente Adscripto Ing. en Informática - Depto. Computación e Informática – FI – CRUC – IUA	Alumno Regular Esp. Seguridad en Informática			
Serafín Fernández		Alumno Regular Ingeniería Informática			
Franco Geller		Alumno Regular Ingeniería Informática			
Jeremías		Alumno			

Leiton		Regular Ingeniería Informática			

Si correspondiera, consignar becas y/o pasantías relacionadas con el proyecto

Apellido y Nombres	Tipo de Beca / Pasantía	Institución otorgante / Unidad Académica	Período

III. Plan de Investigación

3.1. Elaboración del proyecto

Resumen Técnico[3]

Blockchain, en adelante, "BC" es una nueva forma para que las empresas, los sectores de la industria y los organismos públicos puedan realizar y comprobar transacciones de forma casi instantánea, lo que facilita los procesos de negocio, ayuda a ahorrar costos y reduce las posibilidades de fraude. Básicamente podemos decir que BC es una base de datos distribuida, NO modificable, Aplicable a todo tipo de transacciones, existiendo una réplica de toda la información en todos los nodos de la red. El objetivo de este proyecto es investigar y definir una solución para llevar a las organizaciones un sistema funcionando se desarrollará en la Facultad de Ingeniería del Centro Regional Universitario Córdoba.

Este trabajo involucra la creación de un modelo de referencia que provee un marco de trabajo tanto al área de finanzas por el manejo y gestión de las criptomonedas, sino también a áreas de desarrollo de software de las nuevas aplicaciones y las nuevas APIs (Application Programing Interface – Interfaz de programación de aplicaciones) requeridas para poder realizar la adaptación de los sistemas en funcionamiento a la red BC.

En este proyecto se construirá una arquitectura de nodos que permitirá realizar el despliegue de organizaciones validadoras de cadenas de bloques constituida para un objetivo determinado. Una cadena de bloques es una estructura de datos que se usa para crear un "libro de contabilidad" de transacciones digitales que, en lugar de pertenecer a un único proveedor, se comparte en una red distribuida de equipos. El resultado es un sistema más abierto y transparente que se puede comprobar de forma pública y que cambiará radicalmente nuestra forma de considerar el intercambio de valores y

[3] Hasta 500 palabras

activos, la ejecución de contratos y el uso compartido de datos entre los distintos sectores. Las aplicaciones que usan BC son prácticamente ilimitadas, desde préstamos, bonos, pagos, como así también todo tipo de registración en la que resulta de interés que la misma no pueda ser modificada ni cambiada, por lo tanto, cobra una particular importancia el concepto de "Transparencia" en cualquiera de las aplicaciones que implementen esta tecnología.
Surge entonces la necesidad de montar un laboratorio de pruebas que replique el ambiente de simulación que se utiliza para lograr visualizar la ejecución de los escenarios en las distintas transacciones y contratos inteligentes.
El resultado final que persigue el proyecto una vez finalizado, es acelerar los tiempos de desarrollo e implementación de cualquier tipo de contrato inteligente, siendo un factor diferenciador el hecho de que esto tiene una directa aplicaciones tanto para organizaciones u organismos públicos como en el sector privado.

Estado actual del conocimiento sobre el tema[4]

Un blockchain es una base de datos distribuida, no modificable, que se puede aplicar a todo tipo de transacciones. Consiste en una cadena de bloques, donde cada bloque está enlazado al anterior, y toda la cadena está replicada en todos los nodos que conforman la red.

- **Funcionamiento**

Cada bloque contiene el hash del bloque previo, por lo que si se modifica algún bloque, su hash no coincidirá con el hash que el siguiente bloque de la cadena tiene almacenado, y a su vez, todos los bloques esta replicados en todos los nodos que conforman la red. Por lo tanto, si se quiere modificar algún bloque de la red, debemos modificar todos los bloques subsiguientes para que haya una consistencia entre los hash de los bloques, y así mismo hay que modificar todos los bloques de todos los nodos de la red. Tarea que se vuelve más difícil entre más cantidad de nodos conforman la red. Cada nuevo bloque es creado por un solo minero, que compite mediante una prueba de trabajo o PoW (Proof of Work) o una prueba de participación o PoS (Proof of Stake) para poder hacerse de la transacción y poder subir un nuevo bloque a la red. Una vez generado el bloque, el nodo que lo mina, lo envía a todos los nodos de la red, y para poder ser confirmada la transacción, el nuevo bloque debe ser aprobado por al menos el 50% de los nodo de la red, que verificarán si cumple con las normas del blockchain. Todo lo descripto funciona en lo que se llama la Blockchain pública. Pero qué sucede si se quiere desarrollar una Blockchain privada.
Se puede crear una blockchain privada a través de herramientas como Geth. Esto permite crear contratos inteligentes y hacer transacciones a aplicaciones distribuidas, al igual que usando la blockchain pública, pero sin la necesidad de usar alguna criptomoneda real. Si por ejemplo se utilizará la red de Ethereum, además se puede crear ether propio, preasignar ether a una cuenta y usarlo para

[4] Hasta 2000 palabras

transacciones, transferencias o acciones de contratos inteligentes.
Para crear la blockchain privada se empieza creando el bloque génesis. Luego se debe crear la red privada donde se podrán minar los bloques que se añadirán a la blockchain privada. Esta red tiene un identificador networkid que permitirá identificar la red del blockchain.
Luego se deben crear cuentas para poder manipular la red del blockchain. Para minar los bloques de un blockchain privado no se necesita hardware especializado como sucede con el blockchain público, ya que el dueño del blockchain especifica la dificultad para minar.
La ventaja de implementar una blockchain privada es que disminuye el requerimiento de hardware tantos en nodos que copian el blockchain como en nodos que minan. Además, permite controlar quién utiliza el blockchain y que transacciones pueden usar, a través de permisos. También se pueden disminuir los tiempos de actualización del blockchain y de procesamiento de un bloque.
La diferencia con utilizar la blockchain pública es que la implementación de una privada requiere una inversión inicial mayor ya que es obligatorio crear al menos un nodo que comparta el blockchain, y se necesitan más si se va a procesar una mayor cantidad de transacciones desde muchos nodos. En cambio, si se utiliza la blockchain pública y no se replica todo el blockchain en cada nodo, no se requerirá ningún tipo de hardware especializado.
A modo de ejemplo podemos describir el siguiente caso.

- **Casos de uso**

IDEX: 25,000 transacciones x día.
IDEX es una plataforma de intercambio de transacciones de blockchain híbrida, semidescentralizada que permite a los usuarios operar continuamente sin esperar para transacciones a la mina. Funciona como una cola de transacciones.
Etheroll: 1,200 transacciones x día.
Etheroll es una dapp de Ethereum para realizar apuestas en juegos usando Ether, sin depósitos ni registros.
OpenSea: 600 transacciones x día.
OpenSea es una dapp de mercado para cripto coleccionables.

- **Por qué Ethereum y no otra**

Ethereum posee una gran cantidad de nodos y transacciones actualmente, lo que la vuelve muy segura. Además, existe la posibilidad de implementar un blockchain privado, lo cual no existe con alternativas como Nem. Además, alternativas como Nem no son completamente de código abierto, lo que limita la capacidad de saber qué realiza el software.

- **¿Qué es un smart contract o contrato inteligente?**

Un contrato inteligente es un programa informático que ejecuta acuerdos establecidos entre dos o más partes haciendo que ciertas acciones sucedan como resultado de que se cumplan una serie de

condiciones específicas.
Es decir, cuando se da una condición programada con anterioridad, el contrato inteligente ejecuta automáticamente la cláusula correspondiente.

- **Otros puntos a tener en cuenta**
  - En Mayo de 2018, el tamaño del blockchain de Ethereum pasó 1TB (para los full nodes, no los archival nodes).
  - Esto es un problema para el espacio de disco necesario, el tamaño del blockchain o la validación de todos los archivos del bloque génesis. Lo que hay que tener en cuenta es los datos por segundos que se deben procesar (ancho de banda)
  - El tiempo de sincronización actual del blockchain de Ethereum, desde cero es de aproximadamente 7 horas.
  - Existe un proyecto llamado "vipnode" que buscar incentivar económicamente a la gente que cree full nodes, ya que actualmente hay problemas con los slots para los light nodes.

La intención de este proyecto es contribuir a mejorar los procesos a los efectos de montar una Blockchain privada y que sea de aplicación a las distintas áreas involucradas investigando y construyendo soluciones tecnologías que garanticen la confiabilidad y transparencia de las operaciones.
El equipo de investigación pertenece al Departamento de Computación e Informática de la Facultad de Ingeniería y se desempeña en la línea de investigación de Seguridad Informática conformada en el año 2009.

Objetivos de la Investigación

- Entender el funcionamiento y significado de la tecnología de cadena de bloques.
- Comprender el sentido de porqué aplicar BC modificando paradigmas tradicionales
- Entender los elementos fundamentales del BC.
- Comprender los servicios relacionados con las tecnologías BC y validarlos en modelos
- asociados a los diferentes mercados objetivos.
- Prototipar los servicios de BC para organizaciones públicas y privadas.
- Dimensionar el impacto y esfuerzo de desarrollo de los servicios a proporcionar.

Metodología

La metodología a seguir en este plan de trabajo está basado en la metodología ágil SCRUM. Se justifica esta elección por tratarse de un proyecto en donde se integran diferentes conocimientos y el equipo de trabajo debe ser multidisciplinario para garantizar el éxito del proyecto. En el mismo participan expertos en el dominio de Seguridad Informática, desarrolladores de software científico técnico.
Teniendo en cuenta los valores imprescindibles del manifiesto ágil, que sugiere SCRUM, se adopta el

siguiente proceso de desarrollo que abarcará desde la etapa de requerimiento, diseño, desarrollo propiamente dicho y con una fuerte etapa des pruebas, las que incluirán: Planificación de las pruebas: la cual debe estar abarcada por la definición del alcance de la prueba, los tipos de prueba a realizar, la estrategia de prueba, criterio de salida, estimación de tiempos, roles y recursos que formarán parte del proceso y la preparación del entorno de pruebas entre otros. Diseño de las pruebas: que implica revisar toda la información del dominio relevado, se definen los casos de prueba o escenarios para evaluar cómo se comportan los diferentes componentes del sistema ante situaciones atípicas y permite verificar la robustez del sistema, atributo que constituye uno de los requerimientos no funcionales indispensable para este tipo de desarrollo de software. Implementación y Ejecución de las Pruebas: En esta etapa se ejecutan los escenarios o casos de prueba que puede realizarse de manera manual o automatizada; en cualquiera de los casos, cuando se detecte un fallo en el software, este debe ser documentado y registrado en una herramienta que permita gestionar los defectos. Una vez el defecto ha sido corregido, es necesario realizar un re–test que permita confirmar que el defecto fue solucionado de manera exitosa. Evaluación del criterio de salida: Los criterios de salida son necesarios para determinar si es posible dar por terminado un ciclo de pruebas. Por lo que es conveniente definir una serie de indicadores que permitirán comparar los resultados obtenidos contra los indicadores definidos, si los resultados obtenidos no superan los indicadores definidos, no es posible continuar con el siguiente ciclo de pruebas. Coexisten varios tipos de criterios de salida por ejemplo cubrimiento de funcionalidades en general, cubrimiento de funcionalidades críticas para el sistema, número de defectos críticos y mayores detectados, etc.
Cierre del Proceso: Principalmente en esta etapa se elabora un informe con del análisis de errores encontrados a lo largo del proceso de prueba como también una estadística de los errores más frecuentes dejando lecciones aprendidas para aplicar en futuros proyectos Además, se organizaron las funcionalidades a ser probadas en sprint para determinar

Indicadores (cuantitativos y/o cualitativos)

Indicadores de avance del proyecto:

- Porcentaje de los requerimientos identificados del dominio bajo análisis.
- Porcentaje de avance de las entrevistas realizadas para el estudio del relevamiento.
- Conocimiento del estado del arte por parte del equipo de trabajo.
- Cantidad y pertinencia de las tecnologías de Blockchain propuestas.
- Porcentaje de avance del diseño de la arquitectura de Nodos de la Red.
- Porcentaje de avance del montaje del laboratorio de BC.
- Estado de avance de la configuración de las herramientas de generación y programación de contratos inteligentes seleccionadas.
- Porcentaje de avance de la construcción del modelo de contrato inteligente.
- Porcentaje de avance de la ejecución de pruebas de funcionamiento e interrelación de los

nodos.
- Porcentaje de avance del informe de resultados.

3.2. Impacto del proyecto

Contribución al avance del conocimiento científico y tecnológico y/o transferencia al medio

Este proyecto permitirá consolidar al grupo de seguridad informática específicamente acerca de esta nueva tecnología blockchain, adoptando un nuevo modelo de trabajo que le ayudará a interactuar con las áreas de desarrollo de software y de esta manera participar en el proceso de desarrollo de software desde los comienzos del mismo garantizando la calidad en el funcionamiento de cada Nodo y lo más importante garantizando el correcto funcionamiento de él o los contratos inteligentes desplegados en los nodos.
Manejar esta tecnología y disponer de un laboratorio en el que se puedan tener los distintos elementos que integran la red posicionará a la Facultad de Ingeniería como pionera en futuros desarrollos sobre Blockchain, más aún si pensamos en desarrollos sobre una Blockchain privada. Los beneficios obtenidos serán percibidos en la configuración de productos y soluciones tanto para el sector privado como público, que requieran mayor transparencia, confiabilidad y seguridad en su operación además de la reducción de costos.
Además el equipo de Blockchain obtendrá capacidades tecnológicas que le permitirá definir estrategias adecuadas de nuevos desarrollos y seleccionar las mejores técnicas y herramientas para adaptarse a las diferentes necesidades y aplicaciones con características específicas.
Teniendo en cuenta que el manejo de esta tecnología se encuentra en una etapa de absoluta expansión, las posibilidades de transferencia de conocimiento hacia el medio abre una puerta muy importante a la Facultad por la potencialidad de vinculación con organizaciones públicas y privadas.

Contribución a la formación de recursos humanos

Dentro del equipo de investigación existen conocimientos en las distintas tecnologías de Blockchain públicas pero se ha estimado capacitación externa para especializar estos conocimientos en el área de una Blockchain privada. En el proyecto se involucraron alumnos quienes están en los últimos años de la carrera y presentan interés en la especialidades asociadas a la Seguridad Informática y Blockchain, manifestando su motivación en la investigación de la temática, así mismo el proyecto propone variadas líneas para propiciar trabajos finales de carrera.

Beneficiarios/Usuarios directos e indirectos de la propuesta

Organizaciones Públicas y Privadas que requieran de servicios donde la seguridad y la transparencia de los datos e información sea un valor esencial.

3.3. Cronograma de Actividades

Actividades	Meses											
	1	2	3	4	5	6	7	8	9	10	11	12
Relevamiento	x	x	x	x								
Diseño				x	x	x						
Implementación						x	x	x	x			
Prueba									x	x	x	
Elaboración de informes técnicos												x

3.4. Conexión/Intercambio del proyecto con otros grupos de investigación de Facultades UNDEF y/u otras instituciones

IV. Presupuesto detallado del financiamiento solicitado y monto total que se necesita para viabilizar el proyecto

Rubros elegibles	*Concepto (desagregar gastos)*	*Monto Solicitado UNDEF*	*Otros aportes*	*Monto Total*
Insumos	Artículos de librería, insumos informáticos	$7.000		$7.000
Bibliografía	Material bibliográfico	$5.000		$5.000
Servicios y/o Asistencias Técnicas Especializadas	Servicios y/o asistencias técnicas especializados en lenguajes.	$25.000		$25.000
Viajes y Viáticos	Viajes y viáticos insumidos para el desarrollo del proyecto y asistencia de congresos y eventos	$20.000		$20.000
Inscripción a Congresos y eventos.	Inscripciones a congresos nacionales e internacionales	3.000		3.000
Equipamiento	Placa de video	$40.000		$40.000
Monto Total		**$100.000**		**$100.000**

Programa de Acreditación y Financiamiento de Proyectos de Investigación

Formulario Guía para la presentación de proyectos

(Nota: Los gastos de Viajes y Viáticos no podrá superar el 40% del presupuesto total solicitado)

Firma del Director

Aval Institucional