2023 WICC
UNNOBA | JUNÍN

LIBRO DE ACTAS

XXV Workshop de Investigadores en Ciencias de la Computación

Buenos Aires, abril del 2023
UNNOBA – Red de Universidades de Carreras de Informática RedUNCI

RedUNCI ITT Instituto Transferencia Tecnología ESCUELA DE TECNOLOGÍA UNNOBA 1983 - 2023 40 años EN DEMOCRACIA Universidad Nacional Noroeste • Buenos Aires

Diseñar una solución de identidad auto-gestionada para acceso a servicios de calidad con redes Blockchain multipropósito en la Universidad Nacional de Río Negro

Mauro Cambarieri[1], Alejandra Viadana[1], Nicolás Garcia Martinez[1], Luis Vivas[1], Carlos Lugani[1]

[1] Universidad Nacional de Rio Negro. Sede Atlántica
Laboratorio de Informática Aplicada
{mcambarieri,caviadana,ngarciam, lvivas, clugani}@unrn.edu.ar

RESUMEN

El objetivo de este proyecto es diseñar la Identidad Digital Autogestionada en la UNRN adoptando el nuevo paradigma de producción de software, basado en tecnologías descentralizadas.

Se utilizarán tecnologías blockchain aportando a la transformación digital en el ámbito universitario y desarrollo de servicios públicos digitales innovadores. Se desarrollarán componentes de software para optimizar procesos y servicios utilizando tecnologías descentralizadas, es decir, las redes de web 3, ofrecen una alternativa al deterioro del status quo digital. La introducción de Blockchain, plantea una revolución tecnológica que repercute directamente en cambios organizacionales, económicos y políticos.

La Identidad Digital le da la posibilidad a cada individuo la administración de sus datos, como los certificados analíticos y la forma en que serían presentados a terceros a través de billeteras digitales.

El reto de las redes descentralizadas es que son bienes públicos. Al no haber una entidad central que controle las decisiones y obtenga beneficios, es difícil incentivar su mantenimiento y desarrollo. La criptografía ayuda a resolver este problema mediante la coordinación descentralizada y la provisión de incentivos económicos para el desarrollo.

Como resultado se espera la sensibilización a la comunidad, autoridades, entre otros, además de, divulgar los resultados, formación de recursos humanos y transferencia tecnológica.

Palabras clave: Web 3, Blockchain, LACChain, Wallet, descentralización

.

CONTEXTO

El presente trabajo se enmarca en el proyecto de investigación PI 40-C-875 “Herramientas Informáticas de Dominio Específico para el Desarrollo de Servicios Digitales Innovadores para Comunidades Urbanas y Rurales en el Marco de Ciudades y Regiones Inteligentes” desarrollado en el Laboratorio de Informática Aplicada, Sede Atlántica, Universidad Nacional del Río Negro (UNRN). Se pondrá especial énfasis en la utilización en tecnologías blockchain aportando a la transformación digital en el ámbito universitario y desarrollo de servicios públicos digitales innovadores. Se enfocará en la necesidad de instituciones universitarias nacionales e internacionales. Se desarrollarán componentes de software para optimizar los procesos, políticas y servicios utilizando tecnologías descentralizadas, teniendo en cuenta la relevancia de la tercera era de internet, es decir, las redes descentralizadas de web 3.

Contamos con una fortaleza para el desarrollo de este proyecto, ya que en el año 2022 el LIA se sumó a un proyecto liderado por el BID Lab con el objetivo del desarrollo del ecosistema blockchain en América Latina y el Caribe. Como resultado nace la alianza LACChain que se encuentra compuesta por un grupo de organizaciones que están activamente participando en el desarrollo de aplicaciones blockchain y su uso real por la sociedad, cuyo objetivo se centra en materializar las oportunidades que representa la tecnología blockchain para la región, haciéndola viable.

Esta Alianza Global, permitió realizar el despliegue de un nodo escritor en los servidores del LIA, en el cual es posible realizar transacciones de información sensible sobre la Blockchain, permitiendo sumar integrabilidad al proyecto de investigación 40-C-875, además de contar con un entorno de prueba para el despliegue y desarrollo de aplicaciones descentralizadas que se pretende llevar a cabo en la presente propuesta.

1. INTRODUCCIÓN

En los años '90 nació lo que se denominó Web 1, Tim Berners-Lee y Robert Cailliau juntos crearon la World Wide Web, en la que un sitio web típico de un usuario (autoalojado) que estaría formado por texto hipervínculo de, archivo, imágenes, aplicaciones y otros objetos digitales que pueden ser leídos y/o

descargados por los navegadores, es lo que se conoce como "Web 1.0" o "web de sólo lectura" [1]; luego llegaron las interacciones del usuario y las redes sociales, esta web marcó el agrupamiento, ordenamiento, la gran centralización y monopolio de algunos proveedores, La Web 2.0 (término acuñado por Tim O'Reilly en 2007 [2]) o "web de lectura y escritura" (término acuñado por Richard McManus en 2003) empezó a desarrollarse en la década del 2000, cuando surgieron plataformas como Facebook, Amazon, eBay, etc. Sin embargo, no refleja la idea inicial de que la Web como medio para el intercambio seguro y descentralizado de datos públicos y privados [3]. La Web 3 o internet del valor es la evolución de la Web 2 y lo que se espera de esta es que sea una red completamente descentralizada, sin "censura", donde los usuarios puedan compartir información de forma segura sin temor a que sea borrada o modificada [4]. Esto es posible gracias a blockchain, esta tecnología de registro distribuido que facilita una lista ampliada de registros transaccionales irrevocables ordenados cronológicamente y firmados criptográficamente que comparten todos los participantes de una red, además permite eliminar la necesidad de intermediarios y también garantiza la integridad de los datos al registrar el historial de todas las transacciones. Esto significa que la Web 3 será una internet más segura que la actual [5], proveyendo una plataforma libre, abierta, democrática.

La Tecnología blockchain, ha ido creciendo su interés de forma exponencial como resultado de las nuevas aplicaciones de uso potencial que ya se está viendo no sólo en el ámbito financiero donde tuvo su primer y más exitoso campo de aplicación con las criptomonedas, sino en el gran interés por parte de múltiples sectores económico-financieros y sociales -tales como la Academia, la Industria, el Agro-, por su potencial para ofrecer soluciones a gran escala [6]. Esta tecnología de registro distribuido (DLT- por sus siglas en inglés Distributed Ledger Technology) es una tecnología que facilita una lista ampliada y ordenada cronológicamente de registros transaccionales irrevocables y firmados criptográficamente que comparten todos los participantes de una red. Cualquier participante con los derechos de acceso adecuados puede rastrear un evento transaccional, en cualquier momento de su historia, perteneciente a cualquier actor de la red. La tecnología almacena las transacciones de forma descentralizada. Las transacciones de intercambio de valor se ejecutan directamente entre pares conectados y se verifican de forma consensuada mediante algoritmos a través de la red. La introducción de Blockchain, plantea una revolución tecnológica que repercute directamente en cambios organizacionales, económicos y políticos. Esta nueva era del internet del valor, blockchain y la Web 3, implicarán un gran desafío de adaptación y una gran oportunidad hacia la transición digital, económica, social y política de nuestras sociedades. La sociedad hoy cuenta con herramientas que permiten auto-organizarse como nunca antes y expresarse sin la necesidad de intermediarios [17]. La contribución de la web 3 en las primeras etapas de desarrollo, permitirá que las comunidades sean incentivadas y recompensadas por mantener y desarrollar la infraestructura de base(blockchain) [7].

La importancia de la tercera era de internet, las redes descentralizadas de web 3, ofrecen una alternativa al deterioro del status quo digital. Aunque la centralización ha ayudado a millones de personas a acceder a la tecnología, muchas de estas de uso gratuito, también ha "ahogado" a la innovación. En la actualidad, las empresas o corporaciones propietarias de las redes tienen un gran poder unilateral sobre cuestiones importantes como, por ejemplo: acceso a la red, datos de los usuarios, etc. Las plataformas centralizadas siguen un ciclo de vida predecible. Cuando empiezan, hacen todo lo posible por captar usuarios y terceras partes, como desarrolladores, empresas y medios de comunicación. Lo hacen para que sus servicios sean más valiosos, ya que las plataformas (por definición) son sistemas con múltiples intereses en la red. A medida que las plataformas ascienden en la curva de adopción, su poder sobre los usuarios y las terceras partes aumenta constantemente. Cuando llegan a la cima de la curva, sus relaciones con los participantes de la red pasan de ser de suma "positiva" a "cero". La forma y estrategia de seguir creciendo consiste en extraer datos de los usuarios y competir por la audiencia y los beneficios: Ejemplos históricos de ello son Microsoft contra Netscape, Google contra Yelp, Facebook contra Zynga y Twitter contra clientes de terceros. Esto dificulta que las empresas emergentes, los desarrolladores y otros grupos aumenten su presencia en Internet, ya que deben preocuparse de que las plataformas centralizadas cambien las reglas y puedan llevarse sus audiencias o beneficios [4][18].

El reto clásico de las redes descentralizadas es que son bienes públicos. Al no haber una entidad central que controle las decisiones y obtenga beneficios, es difícil incentivar su mantenimiento y desarrollo. La criptografía ayuda a resolver este problema mediante la coordinación descentralizada y la provisión de incentivos económicos para el desarrollo [8].

La Web 3 pondrá el poder en manos de las comunidades y no de las empresas. A continuación, se presentan algunas de las características claves que se incluyen en esta nueva internet: 1- la identidad digital autogestionada (según Sovrin, "identidad auto-gestionada (IAG) es un término utilizado para describir el movimiento digital que reconoce que un individuo debe poseer y controlar su identidad sin la intervención de las autoridades administrativas. La IAG permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el

mundo físico") [9] 2- Contratos inteligentes(método automatizado para realizar transacciones comerciales en línea); 3- Dapps (aplicaciones descentralizadas que se ejecutan en Web 3, ejecutan códigos basados en contratos inteligentes que permiten a los usuarios acceder a sus servicios a través del sistema) y 4- DAOs (Organizaciones descentralizadas, donde los participantes de un proyecto que se ejecuta en la Web 3 están a cargo del destino de su negocio, ya que les da más poder y más posibilidad de votación en cada decisión, que en las estructuras verticales tradicionales).

En el presente proyecto, se enfocará en uno de los aspectos claves antes mencionados. La Identidad Digital Autogestionada da la posibilidad a cada individuo la administración de sus datos y la forma en que serían presentados a terceros.

Entre esos datos (credenciales) a los cuales los usuarios tendrán acceso a su administración soberana podríamos enumerar: títulos académicos, certificados analíticos, certificados de alumnos regulares, rendimiento académico, etc. Para que esto sea posible se recurre al desarrollo de billeteras digitales que podrán disponer en sus dispositivos en forma de aplicaciones móviles.

Concepto de identidad digital

"La identidad es un conjunto de atributos relacionados con una entidad." – ISO/IEC 24760-1 [11]. Para definir la identidad digital se aclara que el dueño de dicha identificación tiene la posibilidad de elegir cuáles atributos quiere hacer públicos mostrando esta capacidad para mostrar el control que genera la condición de Descentralizada de esta nueva Identidad Digital (ID).

Otra característica importante de la ID es la inclusión de los ciudadanos, convirtiéndolos en ciudadanos digitales ya que a partir de esta tecnología permite usar estos servicios de forma remota y en tiempo real, incluyendo a pobladores de lugares a los que su ubicación y dificultad de acceso a la misma pueden acceder a sus credenciales que luego podrán administrar de forma personal sin la necesidad de la intervención de las entidades otorgantes.

Según el Banco Mundial, las identidades digitales se crean y utilizan como parte de un ciclo vital que se compone de cuatro etapas: (a) registro, incluyendo inscripción y validación, (b) emisión de documentos o credenciales, (c) autenticación de identidad y (d) autenticación para la prestación de servicios o transacciones. [10] [11].

La literatura sobre Identidad Digital Autogestionada ha aceptado como válidos los 10 principios establecidos por Christopher Allen en 2016 [12]. Los mismos hacen referencia al Acceso, Consentimiento para el uso de datos por terceros de ser necesario, Control de sus identidades, Existencia independiente de los usuarios, Interoperabilidad, Minimización de los reclamos de los usuarios y la difusión de los mismos, Persistencia en tanto las identidades deben ser sostenidas en el tiempo, Protección de los datos y derechos de los usuarios, Portabilidad tanto de la información y los servicios utilizados. Transparencia en los algoritmos utilizados.

De acuerdo a Marcos Allende López [13]: "*Consideraremos que la identidad auto-gestionada es un modelo de identidad digital siempre que cumpla con los 16 principios siguientes.*

• *Las personas pueden generar sus propios identificadores únicos (control, existencia).*

• *Las personas tienen el control de sus autenticadores (acceso, control, existencia).*

• *Las personas tienen el control de sus credenciales y certificados digitales (acceso, control, existencia).*

• *Las personas pueden recuperar las credenciales y certificados en caso de pérdida o robo de sus autenticadores (acceso, control, existencia, persistencia y protección).*

• *Las personas administran y controlan los datos asociados con su identidad digital (acceso, control).*

• *Las personas pueden hacer divulgaciones selectivas de datos (consentimiento, control, minimización, protección).*

• *La información de identificación personal (IIP) de los individuos se minimiza (minimización, protección).*

• *Las pruebas criptográficas de la propiedad de los identificadores se pueden encontrar en una red pública descentralizada (interoperabilidad, persistencia, transparencia).*

• *Las pruebas criptográficas de la propiedad y la validez de las credenciales se pueden encontrar en una red pública descentralizada (interoperabilidad, persistencia, transparencia).*

• *El derecho al olvido está garantizado (protección).*

• *Las unidades de gestión de identidad (billeteras digitales) son portables (portabilidad).*

• *Los proveedores de billeteras digitales no tienen acceso a la información sobre el acceso de los individuos a los servicios o las interacciones con otros (acceso, control, protección).*

• *Las copias de seguridad garantizan los niveles máximos de seguridad y privacidad (persistencia, protección).*

• *Las implementaciones cumplen con las políticas regulatorias (protección).*".

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Es objetivo general de este proyecto:

Diseñar la identidad autogestionada en la UNRN adoptando el nuevo paradigma de producción de software, basado en tecnologías descentralizadas.

Sus objetivos específicos son:

1. Especificar los requerimientos funcionales utilizando un modelo metodológico y enfoque de construcción.
2. Diseñar una arquitectura de referencia que permita la adopción para la ID autogestionada.
3. Validar el diseño, pasible de ser implementado y transferido al medio.

Las principales actividades a desarrollar son:

A1- Investigar el estado del arte de las tecnologías descentralizadas y el paradigma de la Web 3 para la entrega e implementación de productos de software.

A2- Identificar herramientas, enfoques, metodologías y soluciones innovadoras emergentes en el área.

A3- Analizar el dominio de aplicación, en particular se estudiará el contexto de la Universidad Nacional de Río Negro, y otros gobiernos (municipal, provincial).

A4- Especificar requerimientos funcionales sobre el dominio planteado.

A5- Diseñar la solución en función de los requerimientos funcionales sobre el dominio planteado.

A6- Comunicar los resultados obtenidos.

Tareas a desarrollar:

Estudiar el estado del tema – conducir la revisión de bibliografía de trabajos publicados en congresos nacionales e internacionales y revistas de prestigio a fin de estudiar enfoques de desarrollo, marcos de trabajo, metodologías y soluciones tecnológicas adoptadas para el desarrollo de las tecnologías descentralizadas en el marco de ciudades y regiones inteligentes. (A1, A2)

Estudiar el dominio de aplicación – Conducir un relevamiento de los casos prácticos de desarrollo de soluciones de software con tecnologías descentralizadas y web 3, a fin evaluar las diferentes implementaciones. Comprender a través de un caso de estudio específico como se puede aplicar la tecnología blockchain y la Web 3 revisadas. (A2)

Especificar requerimientos- definir los aspectos funcionales y no funcionales para el diseño de la solución. (A3, A4)

Implementar prototipo(s) de solución – en base a los requerimientos especificados, seleccionar las tecnologías más adecuadas a utilizar para el desarrollo de las soluciones que mejor resuelvan las necesidades de los distintos actores o roles existentes en el contexto del caso de estudio. En esta tarea, las soluciones se implementarán bajo el nuevo paradigma Web 3 y blockchain. (A4, A5).

Identificar el gap entre investigación y práctica – analizar los desarrollos teóricos que no se aplican en la práctica y/o los desarrollos prácticos que no cuentan con sustento teórico que sean relevantes para el desarrollo de las tecnologías descentralizadas en el marco del desarrollo de ciudades inteligentes en la región, a fin de determinar un espacio de contribución científica y definir requerimientos específicos para las soluciones tecnológicas a proponer(A6)

Validar la implementación y adopción de la web 3 y blockchain - Se validará mediante pruebas de campo a coordinar, como caso testigo pasible de replicarlos en otros contextos. (A5, A6)

Divulgación de Resultados – publicar en congresos nacionales e internacionales y en revistas con referato los resultados de investigación producidos durante el proyecto(A6).

3. RESULTADOS OBTENIDOS/ ESPERADOS

Como resultado de este proyecto, se espera:

- Sensibilización a la comunidad sobre tecnologías descentralizadas.
- Elaboración de material para cursos de grado/posgrado
- Dictado de seminarios y/o cursos para desarrolladores de software.
- Definición de la Arquitectura para el desarrollo de las aplicaciones adoptando las tecnologías descentralizadas.
- Definición y selección de herramientas, enfoques, metodologías y soluciones innovadoras emergentes en el área.
- Se obtendrá mediante un Caso de estudio, una prueba de concepto (PoC, por sus ingles, Proof of Concept) para el diseño de una plataforma de servicios de ID autogestionada.
- Se transferirá la elaboración de este prototipo funcional a la Universidad Nacional de Río Negro.
- Se desarrollará estrategias para ingresar al Comité Nacional de Blockchain.

4. FORMACIÓN DE RECURSOS HUMANOS

El grupo de trabajo se encuentra formado por tres investigadores formados, dos investigadores en formación y tres alumnos avanzados de la carrera Licenciatura en Sistemas. En su marco se desarrolla

una tesis de Maestría en Ciencias de la Computación y se producirán tres trabajos finales de carrera de grado.

5. BIBLIOGRAFÍA

[1] Gaurish Korpal and Drew Scott: Decentralization and web3 technologies. The University of Arizona

[2] O'Reilly, Tim, What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Communications & Strategies, No. 1, p. 17, First Quarter 2007, Available at SSRN: https://ssrn.com/abstract=1008839.

[3] T. Berners-Lee, "SolidProject origin." disponible en: https://solidproject.org/origin07.

[4] Web 3.0 y blockchain, un cambio de paradigma para hacer negocios con los propios datos personales. Disponible en: https://www.cronista.com/columnistas/web-3-0-y-blockchain-un-cambio-de-paradigma-para-hacer-negocios-con-los-propios-datos-personales/

[5] Liguori, Walter. Web 3 -The Decentralized Future. October 2022 disponeble en: DOI: 10.13140/RG.2.2.20599.09129
Practices and Patterns. Addison-Wesley (2001).

[6] VEGA MAZA, Marina (2019). «El auge de blockchain y sus posibilidades reales de aplicación en los registros de las Administraciones Públicas». IDP. Revista de Internet, Derecho y Política. N.º 28, págs. 109-126. UOC Consultado: 20/12/2022. http://dx.doi.org/10.7238/idp.v0i28.3154.

[7] The web3 Landscape October 2021 disponible en: https://a16z.com/wp-content/uploads/2021/10/The-web3-Readlng-List.pdf.

[8] Globant. Blockchain un cambio de juego para todas las industrias.Disponible en: https://reports.globant.com/es/sentinel-report/blockchain/ Consultado el 01-02-2023

[9] SOVRIN FOUNDATION(2020). disponible en: https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-Spanish-v01.pdf. Consultado el 20-02-2023.

[10] World Bank. (2018). Technical standards for digital identification systems. Obtenido de http://documents.worldbank.org/curated/en/707151536126464867/ pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

[11] International Organization for Standardization. (2019). IT Security and Privacy — A framework for identity management - Part 1: Terminology and concepts. (ISO/IEC Standard No. 24760-1) Obtenido de https:// www.iso.org/standard/77582.html

[12] Christopher Allen. The Path to Self-Sovereign Identity" Disponible en: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[13] Allende Marcos. El futuro de la identidad digital: auto-gestión, billeterasdigitales y blockchain. Disponible en: https://publications.iadb.org/publications/spanish/viewer/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf

[14] Allende Marcos. Blockchain:Cómo desarrollar confianza en entornos complejos para generar valor de impacto social. BID disponible en: https://publications.iadb.org/publications/spanish/document/Blockchain-C%C3%B3mo-desarrollar-confianza-en-entornos-complejos-para-generar-valor-de-impacto-social.pdf.

[17] Jolías, L (2022): ""Identidad Digital Descentralizada: una guía de implementación de blockchain en gobierno "". Editorial OS City +. Disponible en https://plus.os.city/publicaciones/identidad-descentralizada.

[18] Chris Dixon (2018). ¿Por qué importa la descentralización? Disponible en: https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e.