Adoptando el nuevo paradigma de producción de software con redes Blockchain multipropósito para el diseño de una solución de Identidad Digital Autogestionada en la Universidad Nacional de Río Negro

Mauro Cambarieri[1], Claudia Alejandra Viadana[1], Rached Sofia[1], Michelle Jauge[1]

[1] Universidad Nacional de Río Negro (UNRN), Laboratorio de Informática Aplicada LIA, Sede Atlántica, Viedma, Río Negro
{mcambarieri,caviadana}@unrn.edu.ar, msofiarached@gmail.com, michellejauge@gmail.com

Resumen. El objetivo de este proyecto es diseñar una solución de Identidad Digital Auto gestionada en la UNRN adoptando el nuevo paradigma de producción de software, basado en tecnologías descentralizadas y la Web 3. Con la intención de promover y diseñar la formación y capacitación de recursos humanos para que puedan desarrollar proyectos bajo estas tecnologías, 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. 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 que consolidó, permitió realizar el despliegue de un nodo escritor en los servidores del LIA. La identidad auto-gestionada es un sistema que se apoya en repositorios personales, cuya capacidad de administración es total por parte de los usuarios, en cuanto a todos sus documentos y datos, de manera segura y transparente. El término "billeteras digitales" es usado para identificar estos repositorios personales, donde se administran y comparten, por ejemplo, los certificados analíticos y la forma en como estos son presentados a terceros. La tecnología Blockchain, plantea una revolución que repercute directamente en cambios organizacionales, económicos y políticos. Las redes descentralizadas son bienes públicos. La criptografía ayuda a resolver este problema con coordinación descentralizada. provisión de incentivos económicos para el desarrollo. El resultado esperado es sensibilizar a la comunidad, autoridades, entre otros, divulgar resultados, formación de recursos humanos y transferencia tecnológica.

Palabras clave: Blockchain LACChain, Identidad Autogestionada, Web3, Billeteras digitales.

1 Introducción

La responsabilidad de identificar a los ciudadanos es de los diferentes Estados

nacionales, ellos emiten una credencial única para cada ciudadano que sirve como válido para acreditar la identidad de los mismos. Los gobiernos registran información que va desde nuestra fecha y lugar de nacimiento, domicilios que están asentadas en una oficina estatal que recaba todo información civil de los ciudadanos de un país.

Podemos establecer algunas diferencias en la web 2 en la que se requería de la instalación de diferentes aplicaciones de acuerdo a los servicios que se quisiera acceder incorporando información personal en las mismas de manera obligatoria, en la Web 3 se espera una web descentralizada en la que cada usuario esté en condiciones de compartir información autónoma de manera segura y sin intervención de terceros

Una de las características destacables de esta nueva era de internet es: 1) Identidad digital autogestionada (según Sovrin, "identidad autogestionada (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 [1], 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).

Otro objetivo de este proyecto es llevar adelante un análisis del aporte de esta tecnología en los diferentes niveles de gobierno. La aplicación de la misma permite entender de manera precisa el funcionamiento de la tecnología blockchain y su aporte en la educación. Uno de los beneficios fundamentales es que ayuda a realizar un seguimiento y asegura la inmutabilidad de cada elemento académico individual de una manera escalable. Otro cambio sustancial de la implementación es que ayuda a reducir los niveles de riesgo, elimina posibles fraudes y malas prácticas tanto en lo público como en lo privado, potencia la transparencia, y aumenta la seguridad y transparencia.

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. En esta nueva era digital, la confianza parece ser uno de los problemas a enfrentar día a día. Las transacciones monetarias, el registro de datos personales, los movimientos de contribuyentes del estado, el seguimiento de trámites importantes, son solo algunos de los ejemplos que se pueden mencionar en los que necesitamos que la información brindada sea transparente y honorable.

2 Conceptos utilizados

2.1¿Qué es Blockchain?

Blockchain (BC) es una forma de tecnología de contabilidad distribuida. Esta tecnología de registro distribuido (DLT- por sus siglas en inglés Distributed Ledger Technology) facilita una lista 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. [2].

2.2 - La evolución de la Web 3

La importancia de la tercera era de internet, las redes descentralizadas de la Web 3, ofrecen una alternativa al deterioro del status quo digital. En los inicios de la Web 1, Tim Berners-Lee y Robert Cailliau juntos crearon la World Wide Web, esta consistía en un sitio web formado por texto hipervínculo de, archivo, imágenes, aplicaciones y otros objetos digitales que podían ser leídos y/o descargados por los navegadores, y fue lo que se conoció como "Web 1.0" o "web de sólo lectura" [3]; La Web 2.0 (término acuñado por Tim O'Reilly en 2007 [4]) o "web de lectura y escritura" (término acuñado por Richard McManus en 2003) permitió la llegada de las interacciones del usuario y las redes sociales, empezó a desarrollarse en la década del 2000, agrupando, ordenando, y centralizando la información, lo que generó un monopolio de algunos proveedores (e.g Facebook, Amazon, eBay, etc). La Web 3 o internet del valor como evolución de la Web 2, se espera que sea una red completamente descentralizada, sin “censura", de forma segura sin temor de los usuarios para que puedan compartir información y que la misma no sea borrada o modificada [5]. La tecnología de registro distribuido, blockchain, da la facilidad de que una lista de registros transaccionales sea irrevocables, ordenados cronológicamente y firmados criptográficamente, compartido por todos los participantes de la red, “eliminando” intermediarios y garantizando la integridad y consistencia de los datos al registrar el historial de todas las transacciones. Como resultado de adoptar dicha tecnología, permitirá una internet más segura que la actual [6], proveyendo una plataforma libre, abierta, democrática. 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].

2.3 ¿Qué es la identidad Digital Autogestionada?

2.3.1 Identidad. La identidad se define como el conjunto de características que diferencian a un individuo/objeto/entidad/proceso de otro. En el caso de los individuos, este conjunto de características que los diferencian unos de otros, pueden ser físicas, de género, biométricas, o incluso un tipo de pertenencia. Los atributos que conforman esa identidad están en constante cambio y avances. Sin embargo, es posible que se defina un subconjunto limitado y exclusivo de atributos, para identificar concretamente a un individuo y también ser reconocibles, es decir, autenticarse frente a terceros. Para ello, debemos ser capaces de definir, recopilar, presentar y verificar estos subconjuntos de manera estandarizada. "La autenticación de una persona ante terceros consiste en convencerlos de que puede ser reconocida de manera confiable en base a un conjunto de identificadores y/o atributos." [8].

2.3.2 Identidad Digital (ID): extendiendo la definición anteriormente citada, la identidad digital, es aquella que consiste en un conjunto finito de atributos, y nos permite identificarnos y validarse electrónicamente con otros. Esta ID hace que la persona sea única dentro de un contexto específico. La verificación de la ID es un desafío, dado que la identidad ya no se compara visualmente entre las características físicas de un individuo con las de su documento de identidad para validar quién es. Sin embargo, plantea ventajas al permitir acceso a servicios digitales, de forma remota en un mundo cada vez más digitalizado. Contar con la identificación y autenticación electrónica, es relevante para que podamos saber con quién estamos interactuando y tengamos el control de nuestros datos pudiendo decidir en todo momento con quién, cómo y con qué fin los compartimos[8].

La Unión Europea (UE), señaló que *"sin una manera de identificarnos entre nosotros y nuestras posesiones, difícilmente podríamos construir grandes naciones o crear mercados globales. Desafortunadamente, existen problemas persistentes –y cada vez más serios– con la forma en que funciona la identidad digital. Debido a razones históricas y de otras índoles, la experiencia de identidad digital actual está fragmentada, con pocos estándares o interoperabilidad, es insegura, como nos recuerdan los informes casi diarios de piratas informáticos y violaciones de datos"* [9].

Marcos Allende en su libro [8], señala que idealmente se deben reunir estas 7 características para identificación, autenticación y autorización:

- Escalabilidad: que sean adaptables y replicables.
- Interoperabilidad: que permitan acceso a todo tipo de servicios públicos y privados.
- Portabilidad: que permitan llevar los identificadores digitales y credenciales a cualquier lugar.
- Recuperación: que permitan recuperar claves y credenciales de manera fácil y segura.
- Seguridad: que protejan datos e información personal, incluidas claves privadas y credenciales.

- Seudónimo: que permitan interactuar sin revelar nuestra identidad real.
- Utilidad: generar valor a las personas y experiencia de usuario satisfactoria.

En la actualidad, los individuos no poseen el control de sus datos o de sus credenciales digitales, es decir, sus ID. "*No somos dueños de la información que existe en internet sobre nosotros; ni siquiera aquella información a la que accedemos con nuestro usuario y contraseña (como nuestra información bancaria o nuestros perfiles en redes sociales), pues se almacena en las bases de datos de terceros y son estos quienes nos proporcionan acceso a ella*".

La interacción se encuentra disponible por proveedores de servicios que nos dan acceso a aquellos datos e información que ellos mismos controlan, así como de proveedores de identidad de terceros que administran nuestros autenticadores.

2.3.3 Identidad Digital Autogestionada (IDA): La literatura sobre Identidad Digital Autogestionada ha aceptado como válidos los 10 principios establecidos por Christopher Allen en 2016 [10]. 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[2].

De acuerdo a Marcos Allende López [8]: "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).".

3 La importancia de la Identidad Autogestionada.

3.1 En el sector público

Como antecedente se puede tomar la Identidad Digital Europea, nace de un proyecto presentado por la Comisión Von der Layen que tiene como objetivo implementar una plataforma donde los ciudadanos de la Unión Europea estén en condiciones de gestionar sus datos personales y documentos de interés para los mismos y que llegue a ser implementado por todos los ciudadanos de los distintos países miembros de la UE.

Según la Comisión, las personas podrán elegir el tipo de datos personales que desean incluir y compartir. Útil para abrir cuentas bancarias, presentar declaraciones de impuestos e inscribirse en la escuela", entre otras cosas. Aunque no está previsto que sea obligatorio, la herramienta será gratuita y la Comisión Europea ha declarado que los ciudadanos, residentes y empresas de la UE tendrán derecho a obtener el documento. Según la Institución Europea, esta identidad será "fiable y segura", de acuerdo con el Reglamento General de Protección de Datos (RGPD).

"La identidad digital es el uso de tecnología para asegurar y probar identidad (FATF, 2020)[1]. Con la consolidación del gobierno y la economía digital, las interacciones y transacciones que solo se realizaban en forma presencial están ejecutándose a través de sistemas de información interconectados"

De este postulado se reconoce la importancia de la Identidad Digital en el que cada ciudadano pueda identificarse y autenticar información personal y demás documentos propios que se encuentren protegidos, impidiendo posibles fraudes.

Algo para destacar es que identifica que esta nueva tecnología hará necesario una actualización tecnológica y generar nuevos esquemas dentro de los ámbitos de los gobiernos aun en sus marcos normativos para adecuarlos a los nuevos desafíos que enfrentan.

[1] https://biblioguias.cepal.org/gobierno-digital/identidad-digital Desde el gobierno digital hacia un gobierno inteligente

3.2 En el sector educativo

Es posible contar con un proceso de acreditación que verifique las calificaciones de los titulares garantizando que la confidencialidad de la información no se ha visto comprometida con el tiempo. ¿Existe un sistema de acreditación que se apegue a los estándares? ¿Es posible mantener la confidencialidad de la información fuera de los momentos en que un ciudadano accede a proporcionar a un potencial empleador y al mismo tiempo certifica que las habilidades y destrezas que posee son genuinas?

La tecnología Blockchain ha sido aplicada en otros sectores como el financiero, es probable su aplicación en el ámbito académico en tanto Devine (2015) define esta tecnología como una transferencia universal de créditos entre diferentes instituciones. Estas credenciales verificadas podrían ser un instrumento usado por estudiantes para ser usado en casos de necesidad de ser presentados en otras universidades. Es esperable que dichas credenciales académicas verificadas por Blockchain sean propiedad de los usuarios y así generar inclusión y autonomía en el manejo de sus datos y documentos relevantes para su vida académica. [2]

4 Solución propuesta para el diseño de IAG en la UNRN.

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 Laboratorio de Informatica Aplicada (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 PI 40-C-875, además de contar con un entorno de prueba para el

[2] Devine, P.M. (2015). Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? En Proceedings of ALT Online Winter Conference 2015, 7-10 December 2015. http://oro.open.ac.uk/44966/

despliegue y desarrollo de aplicaciones descentralizadas que se pretende llevar a cabo en la presente propuesta.

BC reduce los riesgos a los que son propensos los sistemas centralizados, a través de la descentralización de datos. Sin embargo, existe el gran reto de introducir esta tecnología en la sociedad. En el marco del presente trabajo se tiene como objetivo el desarrollo para aplicación de blockchain en el ámbito de la educación específicamente en la Universidad de Rio Negro tratando de incorporar la misma para que los alumnos cuenten con sus propias billeteras ("wallets") donde puedan administrar sus propias credenciales surgidas de su paso por dicha institución.

Dentro de las etapas para el desarrollo sobre la tecnología Blockchain en la Universidad, esta se enfrenta a un conjunto de pasos como referencia para elaborar aplicaciones descentralizadas (DApps). Esta nueva tecnología permite la elección de herramientas utilizadas en diferentes propuestas de este ámbito. Para este proyecto será necesario desarrollar una arquitectura robusta que pueda ser implementada para diferentes DApps. Este desarrollo permite la validación en el caso de certificación académica por ejemplo y la gestión de propiedad intelectual de cada uno de los usuarios potenciales.

Como objetivos específicos del proyecto, se pueden enumerar los siguientes:

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 en revistas de divulgación científica, congresos, etc.

5 Conclusiones/Resultados

Como resultado de este proyecto, se espera: Sensibilización a la comunidad sobre tecnologías descentralizadas, la elaboración de material para cursos de grado/posgrado, incluyendo el dictado de seminarios y/o cursos técnicos para desarrolladores de software. Definición de una Arquitectura para el desarrollo de las aplicaciones adoptando las tecnologías descentralizadas, contando con la 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, que permitirá transferir el conocimiento y la tecnología mediante la elaboración de este prototipo funcional a la Universidad Nacional de Río Negro.

Referencias

[1] Sovrin Foundation(2020). Disponible en: https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-Spanish-v01.pdf. Consultado el 20-02-2023.

[2] Cambarieri M,, Viadana A, Vivas, L, Lugani C, Garcia M. N: "Diseñar una solución de identidad auto-gestionada para acceso a servicios de calidad con redes Blockchain multipropósito en la Universidad Nacional de Río Negro". WICC 2023. Disponible en; https://wicc2023.unnoba.edu.ar/2023/04/12/disenar-una-solucion-de-identidad-auto-gestionada-para-acceso-a-servicios-de-calidad-con-redes-blockchain-multiproposito-en-la-universidad-nacional-de-rio-negro/

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

[4] 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.

[5] 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/

[6] 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).

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

[8] 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

[9] The European Union Blockchain Observatory and Forum. (2019). Blockchain and digital identity. Disponible en https://www.eublockchainforum.eu/ sites/default/files/report_identity_v0.9.4.pdf Consultado el 27-03-2023.

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