

Sistema de premiación de logros basado en insignias digitales

Alberca Agustín¹ y Borrelli Juan Ignacio¹

Patricia Bazán² y Nicolás del Río²

¹ Alumnos Tesina de Licenciatura en Sistemas - Facultad de Informática - UNLP

² Directores de la Tesina. LINTI- Facultad de Informática – UNLP

aa.fi.unlp@gmail.com, nacho2911@hotmail.com,
pbaz@info.unlp.edu.ar, ndelrio@info.unlp.edu.ar

Palabras Clave: blockchain, token, gamificación, insignias digitales.

1 Motivación

La tecnología blockchain ha experimentado un auge sin precedentes en los últimos años, gracias a su capacidad para mejorar la seguridad, transparencia, eficiencia y descentralización de datos y transacciones en diferentes sectores y aplicaciones.

A pesar de su enorme potencial, en nuestra sociedad aún existe un gran desconocimiento acerca de su funcionamiento y alcance. Aún en los ámbitos académicos y educativos sigue resultando una tecnología nueva y en la que recién se está incursionando. Por esta razón, la normalización del uso de la tecnología blockchain y la formación de profesionales capacitados se ha convertido en una necesidad imperante.

El hecho de que esta propuesta utilice la blockchain representa un paso importante hacia la democratización y popularización del uso de esta tecnología en diferentes contextos y aplicaciones.

La aplicación de esta herramienta alcanza a cualquier ámbito que en que los usuarios requieran obtener una insignia digital.

Una insignia o certificado es un elemento que permite validar un hecho ante terceros, dado que garantiza la veracidad de lo obtenido como, por ejemplo, la aprobación de un curso, la asistencia a un evento, el logro obtenido en una competencia.

Una insignia digital es una insignia que puede disponibilizarse en línea y que puede contener metadatos que explica el contexto, el significado, desarrollo y resultados del hecho o actividad que representa. No tiene una representación tangible, por lo tanto, debe ofrecer un mecanismo para validar su autenticidad, mediante blockchain.

La utilización de contratos inteligentes basados en blockchain para la creación y gestión de las insignias digitales garantiza la inmutabilidad, la transparencia y la seguridad de la información, al tiempo que ofrece una solución innovadora y escalable para la gestión de logros y reconocimientos.

El objetivo general de la tesina es la creación de una herramienta tecnológica innovadora e integrable que permita premiar a usuarios con insignias digitales

intransferibles, en formato de tokens en blockchain, como reconocimiento al cumplimiento de logros predefinidos en diferentes ámbitos.

El trabajo diseña una arquitectura y flujos de trabajo de una plataforma alineada al objetivo general, haciendo uso de la blockchain como fuente de datos principal y sistemas tradicionales (backend, frontend) como acompañamiento para cubrir las funcionalidades. Basándose en el diseño mencionado, se busca implementar la herramienta de una manera funcional y consistente, integrable a otras plataformas ya existentes bajo estándares de comunicación bien definidos. Por último, se realiza una prueba de concepto a modo de validación en la cual, mediante un prototipo operativo de una aplicación externa, se integra la herramienta y se muestra la interoperabilidad con diferentes plataformas además de su correcto funcionamiento en torno a los parámetros esperados.

2 Aporte y desarrollo del trabajo

El sistema de premiación de logros propuesto en este trabajo, que se denomina TBAP (Token Based Achievements Protocol), implementa una api para integrarse a blockchain y se basa en la generación de tokens, que son unidades digitales que tienen un valor, gestionadas dentro de la blockchain con contratos inteligentes y legitimadas mediante billeteras virtuales.

TBAP se define sobre la base de tres componentes principales: 1- la blockchain que contiene los contratos inteligentes para gestionar tokens y billeteras virtuales, 2- un backend que alberga una base de datos y los servicios que resuelven la autenticación de los usuarios del sistema y la gestión de sus roles y 3- un frontend que resuelve tanto la comunicación con el backend como con la blockchain (esto último resuelto con Meta-mask [3]).

TBAP resuelve tres funcionalidades principales: autenticación de usuarios, lectura en la blockchain y escritura en la blockchain, cuyo diseño arquitectónico y flujo de trabajo se muestran en las Figuras 1, 2 y 3.

TBAP permite crear cursos, desafíos, así como roles de usuario jerarquizados entre encargados y usuarios regulares que pertenecen a una organización.

Una organización tiene el control total. No tiene registro público, sino que es creada por el administrador de la plataforma. Es la responsable de gestionar a los encargados, verificar los nombres de los cursos creados, habilitar a los encargados a crear insignias digitales y a agregar usuarios regulares.

Los encargados crean y administran cursos con usuarios regulares y registran las insignias digitales que estos pueden reclamar.

Los usuarios regulares se registran a través de un registro público y son los únicos que pueden acceder a obtener las insignias digitales que la plataforma ofrece, una vez que un administrador o encargado los haya inscripto en un curso y habilitado dichas insignias.

3 Conclusiones y trabajos futuros

Como resultado del trabajo se obtuvo una aplicación enteramente funcional que le permite a distintos usuarios poder administrar y obtener insignias digitales y poder compartirlas en sus redes. A su vez, se realizó un relevamiento de herramientas similares y cómo nuestra herramienta puede aportar algo más. También se realizó un análisis de todas las tecnologías que permitieron el desarrollo de TBAP, haciendo hincapié en las insignias digitales, la blockchain y las otras tecnologías que derivan de esta última.

Los usuarios pueden obtener insignias digitales compatibles en sus redes, permitiendo validar distintos logros los cuales son certificados por una entidad competente. Distintas empresas u organismos pueden hacer uso de esta herramienta para motivar a su personal a seguir creciendo profesionalmente a la vez que consiguen distintos logros personales.

Entre los trabajos futuros que pueden abordarse para mejorar las prestaciones de la herramienta, se detectan la validación de organizaciones y de usuarios. Se analizan a continuación alternativas de solución a estas dos funcionalidades.

3.1 Validación de organizaciones

La validación de la identidad de las organizaciones emisoras de insignias es crucial para evitar la creación y emisión de insignias falsas por parte de entidades no legítimas. Si no se realiza esta validación, se corre el riesgo de que se generen insignias fraudulentas, lo que podría resultar en la falsificación de credenciales y fraude en el sistema. En consecuencia, la confianza de los usuarios en el sistema se vería afectada, ya que no podrían verificar la autenticidad de los tokens emitidos. Esto podría desmotivar a los usuarios a reclamar las insignias, al percibir que no son confiables.

Una posible solución técnica sería implementar un sistema de autenticación en dos pasos. Bajo este sistema, las organizaciones emisoras primero proporcionarían información clave, como su nombre, dirección y número de identificación fiscal. Luego, se requeriría que confirmen su identidad a través de una verificación de contacto o un proceso de revisión manual por parte del equipo encargado. Esta capa adicional de seguridad ayudaría a garantizar que solo las entidades legítimas puedan emitir insignias en la plataforma.

Sin embargo, es importante tener en cuenta que este sistema es poco escalable al ser manual. Esto se debe a que implica un contacto directo con las entidades, lo que puede derivar en múltiples envíos de documentación si estas no son las correctas en el primer intento. Como resultado, puede ser difícil implementar este sistema en una plataforma grande con una gran cantidad de organizaciones emisoras.

Otra posible implementación para solucionar esta problemática podría ser una función de reputación para las organizaciones emisoras. Esto permitiría a los usuarios y receptores de insignias evaluar y comentar sobre la autenticidad y calidad de las credenciales emitidas por diferentes organizaciones. Esta retroalimentación contribuiría a la transparencia y ayudaría a fortalecer la confianza en el sistema.

Por otro lado, es importante destacar que esto no soluciona el problema de raíz, ya que la función de reputación puede ser subjetiva y difícil de medir.

Es posible que algunos usuarios o receptores de insignias dejen comentarios negativos sobre las organizaciones emisoras incluso si las credenciales son auténticas y de buena calidad, con el objetivo de perjudicarlas.

3.2. Validación de usuarios

La versión actual de TBAP priorizó la facilidad de integración de los usuarios antes que la validación de los mismos.

La registración de usuarios se realiza utilizando la dirección de mail como identificador, lo cual impide validar la relación unívoca persona-usuario ni permite comprobar la veracidad de los datos registrados para cada usuario.

Si bien la blockchain permite la “quema” de los tokens, es decir, la anulación del otorgamiento de la insignia, en caso que la organización detecte una anomalía en los datos, o un error se haya cometido, se analizan las alternativas de para evitar o minimizar estas eventualidades.

Una alternativa es que las organizaciones proporcionen los datos personales de los usuarios mediante el registro SSO existente, y delegando a ellos la verificación de los mismos, es decir, que se recarguen los datos de los usuarios en su registro.

Mientras esta solución le da más poder a las organizaciones, permitiéndoles tener control de los datos de los usuarios, también excluye a aquellas que no tienen un sistema existente, o que lo tienen, pero tampoco hacen un control exhaustivo de la veracidad de los datos de los mismos.

Una segunda alternativa, es utilizar un sistema de KYC (“Know Your Customer”, o conoce a tu cliente en su traducción) dentro de la plataforma para verificar la documentación identificativa del usuario para asegurar que es quien dice ser. De esta manera, se certifica que los datos sean verídicos y que el usuario no posee múltiples cuentas dentro del sistema.

Por último, se pueden considerar los sistemas KYC pero con tecnología blockchain, tales como Civic o SelfKey, que cumplen casi con las mismas características de los convencionales, pero agregando las características más importantes de la blockchain.

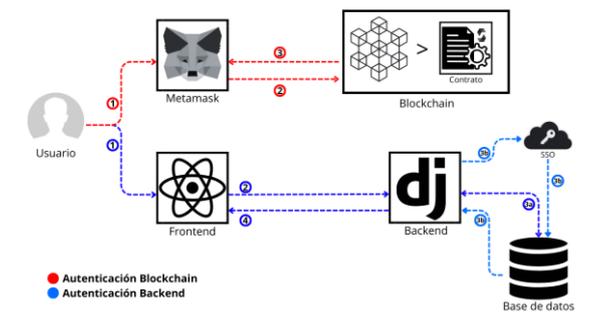


Figura 1- Flujo de trabajo de autenticación de usuarios en TBAP.

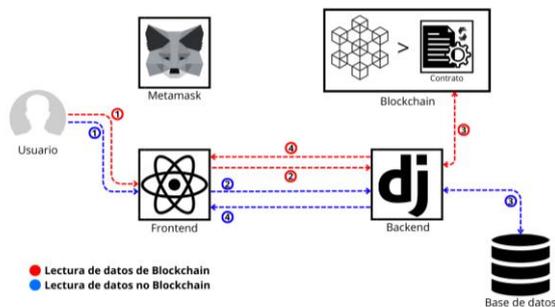


Figura 2- Flujo de trabajo para lectura desde la blockchain

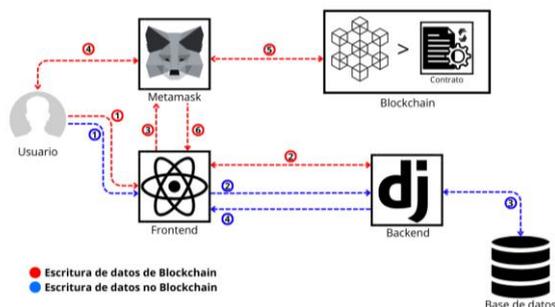


Figura 3- Flujo de trabajo para escritura en la blockchain.

Referencias

1. OpenTimeStamps, plataforma de sellado de tiempo estándar para blockchain <https://open-timestamps.org/>
2. Blockchain Federal Argentina. plataforma multiservicios abierta y participativa para integrar servicios y aplicaciones sobre blockchain. <https://bfa.ar/>
3. Metamask. Extensión de navegador web y una aplicación móvil para administrar sus claves privadas de Ethereum. <https://metamask.io/>
4. Gallardo, I., Bazán, P. A., & Venosa, P. (2019). Arquitectura de Certificados Digitales: de una arquitectura jerárquica y centralizada a una distribuida y descentralizada. *RISTI-Revista Ibérica de Sistemas e Tecnologías de Informação*.
5. Gómez, M., Bazán, P., Río, N. D., & Morandi, M. (2021, June). Routing Security Using Blockchain Technology. In *Conference on Cloud Computing, Big Data & Emerging Topics* (pp. 46-59). Cham: Springer International Publishing.
6. Mansoor, N., Antora, K. F., Deb, P., Arman, T. A., Manaf, A. A., & Zareei, M. (2023). A Review of Blockchain Approaches for KYC. *IEEE Access*.
7. Protocolo de finanzas descentralizadas de código abierto <https://www.ngi.eu/blockchains-forsocialgood/2019/12/20/alice/>