Emisión y verificación descentralizada de microcredenciales universitarias
Decentralized issuance and verification of university micro-credentials

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

Resumo—**En este artículo, se presenta una propuesta de un modelo descentralizado de gestión de confianza para la emisión y verificación de microcredenciales en el ámbito educativo. El enfoque propuesto utiliza la tecnología blockchain como solución a los desafíos que involucran la transparencia, seguridad y autenticidad en los procesos de acreditación. El modelo se compone de la definición una ontología y la estructura técnica basada en Blockcerts.**

***Palabras clave*—Blockchain, microcredenciales, educación abierta, education 4.0, credenciales**

Abstract—**In this paper, a proposal for a decentralized trust management model for issuing and verifying micro-credentials in education is presented. The proposed approach uses blockchain technology as a solution to the challenges involving transparency, security and authenticity in credentialing processes. The model is composed of the definition of an ontology and the technical structure based on Blockcerts.**

***Keywords*—Blockchain, microcredentials, open education, education 4.0, credentials**

I. Introducción

Las microcredenciales son una forma flexible y específica de certificar los resultados de los aprendizajes adquiridos a través de experiencias de corta duración, como por ejemplo un curso o una formación breve. Este tipo de acreditación permite a las personas desarrollar sus conocimientos, habilidades y competencias, promoviendo su crecimiento personal y profesional.

Generalmente, si los cursos se imparten en la misma institución educativa, la gestión de créditos y la asignación de los resultados de aprendizaje es un proceso sencillo. Sin embargo, este proceso se vuelve más complejo cuando los cursos se extienden fuera de la institución educativa principal, y aún más, cuando las oportunidades de estudio se encuentran en instituciones educativas o empresas de formación profesional extranjeras.

La falta de estandarización en el desarrollo y emisión de microcredenciales reduce su valor, exposición, transfronterización, adopción, portabilidad y potencial.

El presente manuscrito tiene como objetivo principal abordar una cuestión crítica en el ámbito de las credenciales digitales: *¿Cómo se pueden utilizar las microcredenciales universitarias emitidas mediante estándares abiertos en procesos de aprendizaje de formación continua?* Para lograr este objetivo, se realizará un análisis de las estructuras técnicas de Blockchain disponibles y se propondrá un modelo de gestión de confianza descentralizado que permita la emisión y verificación de microcredenciales de manera eficiente y segura.

Este artículo está organizado de la siguiente manera: la Sección I proporciona una introducción a la temática central del documento y esboza su estructura general. En la Sección II, se lleva a cabo una revisión de la literatura relevante, enfatizando los conceptos clave relacionados. La Sección III plantea la adopción de un modelo basado en el estándar Blockcerts para la emisión y validación de microcredenciales. La Sección IV explica el proceso de implementación de un prototipo en la Universidad Técnica Particular de Loja para la gestión de las microcredenciales OPENCAMPUS y se exploran las implicaciones de la introducción de esta clase de tecnologías. Por último, en la Sección V, se presentan las conclusiones y se proponen recomendaciones para futuros trabajos en este ámbito.

II. Antecedentes

A. Revisión de la literatura existente

A fin de determinar el estado actual de las implementaciones de modelos de emisión y verificación de microcredenciales basadas en Blockchain, se realizó una revisión sistemática de la literatura existente y trabajos relacionados. La revisión se realizó empleando el procedimiento definido por [1].

*1) **Microcredenciales**:* En relación a microcredenciales, varios autores han desarrollado marcos de referencia para su creación. Por ejemplo, [2] propone un marco para abordar el diseño de un programa de credencialización, dividiendo el proceso en cuatro fases: diseño del sistema, diseño de las credenciales, publicación y gestión del cambio. Además, se

señala que a través de este marco, las credenciales abiertas podrían ayudar a reducir las brechas entre el aprendizaje informal y el formal, y entre la educación profesional y la académica.

Además, el autor menciona que es esencial tener en cuenta que, a medida que la educación abierta continúa evolucionando, es necesario fortalecer la calidad de creación de contenido abierto y explorar nuevas estrategias de aprendizaje centradas en habilidades, distribuidas, flexibles y adaptadas a las exigencias del mundo laboral actual.

De igual manera, [3] describe un estándar de metadatos para microcredenciales e insignias digitales. Un estándar de metadatos para microcredenciales es esencial para garantizar la confiabilidad y la validez de las mismas, y para facilitar su uso en diferentes contextos. El estándar descrito incluye experiencias de aprendizaje, sistemas de acreditación y evaluación, y evidencias de las calificaciones.

De forma general, se han identificado los siguientes elementos que componen a una microcredencial [6]:

- **Distintivo**: es la parte visual de la insignia. Se compone de la imagen que representa a la insignia. Incluye un nombre único, una descripción y también puede incluir una etiqueta sobre cómo obtener las insignias.
- **Lógica de cumplimiento**: son los requisitos para obtener el distintivo. Consiste de:
  1) Desencadenador: indica lo que debe hacer la persona para obtener la credencial.
  2) Prerrequisito: el requisito que se debe cumplir antes de activar el desencadenador
  3) Condiciones para obtener la insignia.
  4) Multiplicador: indica cuántas veces tiene que cumplir el requisito para obtener el distintivo.
- **Recompensa**: indica lo que obtendrá el usuario después de lograr la insignia. La insignia digital también contiene un hipervínculo en el que se puede hacer clic para ver más información (metadatos). Los metadatos se pueden agregar mediante la notación de objetos de JavaScript para datos vinculados (JSON-LD).

*2) **Arquitecturas**:* La revisión de los estudios seleccionados sugiere que el diseño del ecosistema educativo es esencial al momento de desarrollar arquitecturas para la emisión de microcredenciales basadas en Blockchain. [6], por ejemplo, presenta un ecosistema en el que se integran diferentes elementos como instituciones educativas, proveedores de contenido educativo, plataformas tecnológicas, empresas, organizaciones sin fines de lucro y reguladores gubernamentales. Este ecosistema se basa en la adopción de estándares abiertos y promueve la colaboración e interoperabilidad para garantizar su efectividad.

La revisión de los estudios seleccionados permitió identificar dos propuestas relevantes para la implementación de sistemas emisores y validadores de microcredenciales. La primera, presentada por [7], es una implementación llevada a cabo en la Universidad Fernando Pessoa, que utiliza Blockcerts como estándar y combina el uso de dos plataformas Blockchain: Bitcoin y Ethereum. Esta propuesta busca aprovechar las ventajas de ambas plataformas para lograr un sistema robusto y confiable para la emisión y validación de microcredenciales.

La segunda propuesta arquitectónica, presentada por [8], se centra en la utilización de contratos inteligentes para permitir la creación de aplicaciones descentralizadas. Esta propuesta se apoya en tecnologías como Ethereum, IPFS y Solidity para su estructura técnica, con el objetivo de ofrecer un sistema robusto y seguro para la emisión y validación de microcredenciales. Los autores concuerdan en que una de las características esenciales de la estructura técnica para la emisión de microcredenciales en Blockchain es la adopción de técnicas avanzadas de criptografía, lo que garantiza la seguridad y privacidad de los datos. Además, destacan la utilización de arquitecturas descentralizadas, que permiten la creación de sistemas autónomos, y la adopción de estándares abiertos, lo que facilita la interoperabilidad entre diferentes entidades. Otro aspecto importante mencionado es la escalabilidad, pues es necesario que el sistema gestione un gran volumen de transacciones de usuarios.

*3) **Estándares**:* La revisión literaria muestra que varios autores han destacado la importancia de adoptar estándares en la implementación de Blockchain para la emisión de microcredenciales. En este sentido, [7], [9] y [10] mencionan que uno de los estándares más idóneos es Blockcerts. Este estándar se caracteriza por su capacidad de ofrecer una solución segura y confiable para la emisión y verificación de microcredenciales. Blockcerts ha demostrado ser escalable y fácil de implementar, lo cual lo convierte en una opción atractiva para las instituciones educativas.

*4) **Soluciones actuales**:* [4] y [11] destacan varios proyectos en el ámbito educativo que han utilizado Blockchain para la emisión de microcredenciales. Un ejemplo de esto es el desarrollo llevado a cabo por la Universidad de Nicosia donde se implementó un sistema de certificación que va más allá de solo emitir credenciales, sino que también se diseñó un sistema de organización del currículo que está vinculado a las credenciales emitidas. Proyectos similares fueron desarrollados por las Universidades de Cumbria y Ateneo de Manila.

Otro proyecto mencionado por los autores es Open Badges de Mozilla, el cual es un innovador sistema emisor de credenciales educativa que se basa en un estándar abierto. Este proyecto ha sido pionero en permitir la emisión y verificación de credenciales educativas mediante el uso de una plataforma tecnológica. Además, lo que lo hace especialmente relevante es que permite validar habilidades y conocimientos adquiridos fuera del sistema de aprendizaje tradicional, por ejemplo a través de experiencias laborales o proyectos personales, permitiendo una mayor flexibilidad en el reconocimiento de las competencias y habilidades.

Además, se menciona el proyecto Blockcerts del MIT, una plataforma que permite a las instituciones emitir y verificar credenciales de manera estandarizada. Estos proyectos son un ejemplo de cómo Blockchain puede ser utilizado para mejorar el proceso de emisión de credenciales educativas.

*5) **Beneficios y retos**:* [12] destaca que la implementación de Blockchain en procesos educativos ofrece numerosos beneficios debido a las características intrínsecas de esta tecnología, tales como arquitecturas descentralizadas, confiabilidad y seguridad en las transacciones. Esto permite una mayor transparencia y confianza en la gestión de la información, así como una mayor eficiencia en los procesos educativos.

Según [6], una de las principales ventajas de utilizar la tecnología Blockchain para la emisión de microcredenciales es su capacidad para proporcionar una implementación eficiente, económica y con cortos tiempos de desarrollo, si se diseña de forma adecuada. Además, esta tecnología permite el reconocimiento de habilidades adquiridas a través de cursos no tradicionales, lo que brinda a los estudiantes mayores oportunidades para obtener cursos específicos según sus necesidades y a las universidades para desarrollar una oferta educativa competitiva.

En la implementación de Blockchain para la emisión de microcredenciales, se han identificado varios desafíos. Uno de ellos es garantizar la seguridad y privacidad de la información manejada en las transacciones realizadas en las cadenas de bloques, tal como menciona el trabajo de [13]. Además, es esencial desarrollar avances en escalabilidad para poder gestionar un gran volumen de transacciones simultáneamente. En este trabajo también se destaca la importancia de encontrar un equilibrio entre la estructura técnica y los costos de implementación de estas soluciones.

Otro desafío es lograr una colaboración y compartición de datos entre las organizaciones educativas involucradas, lo que requiere cambios en las culturas organizacionales de estas instituciones. Además, según el trabajo de [7], es importante abordar cuestiones relacionadas con la revocación y los tiempos de expiración de las certificaciones emitidas.

El trabajo de [14] destaca un desafío clave para la implementación de microcredenciales basadas en Blockchain: la necesidad de adaptar las metodologías educativas tradicionales de las instituciones para impulsar programas de corta duración, los cuales han sido cada vez más populares entre los estudiantes de educación superior. En este contexto, las microcredenciales podrían tener un papel crucial al convertirse en componentes esenciales de rutas de aprendizaje personalizadas y flexibles.

III. Propuesta

A. *Diseño del modelo de gestión de confianza*

Con el propósito de abordar de manera eficiente la emisión y verificación descentralizada de microcredenciales universitarias, se propone un modelo de gestión de confianza. Esta propuesta establece las bases de un ecosistema colaborativo, donde las distintas instituciones educativas involucradas se enlazan armónicamente para trabajar con un objetivo común.

Este modelo adopta la formación de un consorcio integrado por estas instituciones educativas, que asumen un compromiso colectivo de aceptar y respetar las condiciones y reglas establecidas para participar en el proceso de emisión de microcredenciales. Este consorcio no solo aporta una red de colaboración, sino que también simboliza un pacto de confianza entre las instituciones que deciden participar en el ecosistema de emisión y verificación de microcredenciales educativas.

La construcción de este consorcio desempeña una función crucial en el impulso de la transparencia, la confiabilidad y la interoperabilidad dentro del sistema. A través de la unión de esfuerzos y el establecimiento de estándares comunes, las universidades participantes contribuyen a la creación de un entorno colaborativo. Este entorno incentiva buenas prácticas y garantiza que los procesos de emisión y verificación de microcredenciales sean coherentes y fiables para todos los participantes.

Además, se plantea la definición de los criterios de calidad, los requisitos técnicos y los estándares de seguridad que deben regir en el ecosistema. Este objetivo no solo fortalece la confianza entre las partes involucradas, sino que también facilita la portabilidad y el reconocimiento de las microcredenciales en diversos entornos educativos y laborales. En la siguiente tabla, se listan los roles y responsabilidades de los integrantes del ecosistema.

TABLE I
ROLES Y RESPONSABILIDADES DE LOS INTEGRANTES DEL ECOSISTEMA

Rol	**Responsabilidad**
Junta Directiva	Encargados de establecer normas y estándares para la emisión de las microcredenciales. Además, definen las reglas de participación en el ecosistema.
Auditores de normas y estándares	Encargados de velar por el cumplimiento de las normas y estándares que fueron aprobados por la Junta Directiva.
Agencias de acreditación y regulación	Encargados de supervisar el correcto funcionamiento de los sistemas en conformidad con las normativas educativas de carácter local o nacional.
Instituciones educativas	Encargados de diseñar y ofertar los diferentes programas de formación. Además, son los encargados de verificar los aprendizajes y habilidades adquiridas por los estudiantes.
Proveedores de infraestructura tecnológica	Encargados de la administración de la infraestructura tecnológica que soporta el modelo.
Participantes	Individuos que adquieren aprendizajes y habilidades, que pueden ser verificadas gracias a la emisión de microcredenciales. Responsables de cumplir con los requisitos del programa de formación y fomentar la participación en el ecosistema.
Empleadores y Organizaciones	Encargados de utilizar las microcredenciales para validar las competencias de potenciales empleados. Además, son los responsables de definir las necesidades del mercado laboral.

El consorcio, al fomentar la colaboración y el establecimiento de estándares compartidos, se erige como un verdadero motor de cambio y desarrollo en el ámbito de las microcredenciales universitarias. Su participación activa y su influencia en la definición de las condiciones y reglas de emisión permiten consolidar un marco robusto que promueva la innovación y la adopción generalizada de este tipo de credenciales.

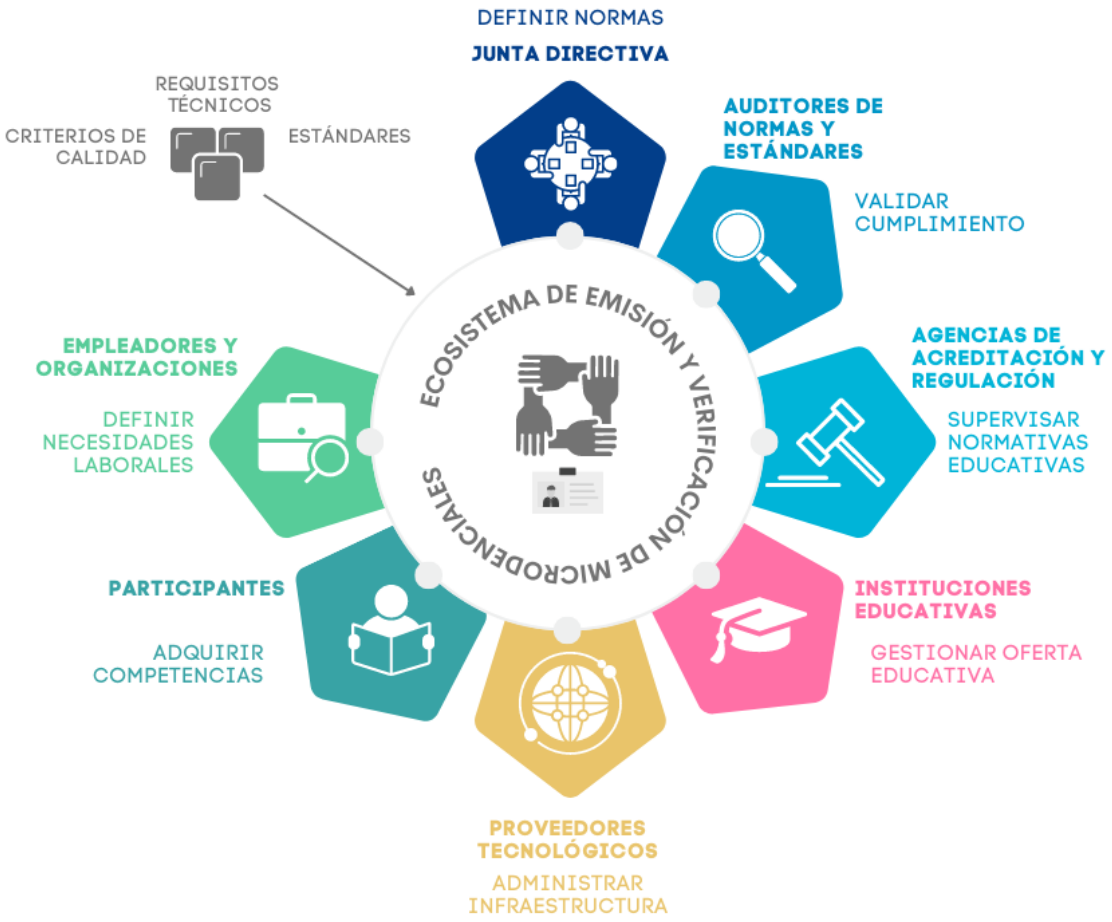

Fig. 1. Ecosistema de emisión y verificación de credenciales educativas

Esta iniciativa, por ende, beneficia a una amplia gama de actores, incluyendo estudiantes, instituciones educativas y empleadores, al facilitar el reconocimiento de logros y habilidades específicas en una variedad de contextos.

El establecimiento de las condiciones y reglas de participación del consorcio se llevará a cabo mediante un proceso detallado y transparente para garantizar que todos los miembros estén en la misma sintonía y se respeten los principios de equidad, transparencia y responsabilidad compartida.

Es necesario por lo tanto, el diseño de un marco de gobierno que describa la estructura del consorcio, defina los roles y responsabilidades de los miembros y establezca los procedimientos para la toma de decisiones. Este marco debe ser lo suficientemente flexible para adaptarse a las necesidades cambiantes del consorcio y lo suficientemente sólido para garantizar su funcionamiento eficaz y su integridad a largo plazo.

El consorcio también debe considerar el establecimiento de un mecanismo de control y seguimiento para garantizar el cumplimiento de las reglas y condiciones establecidas. Esto podría incluir el desarrollo de auditorías regulares, informes de cumplimiento y revisiones periódicas de las reglas y condiciones de participación para garantizar que sigan siendo relevantes y efectivas.

A continuación, se listan los elementos que componen el modelo basado en Blockchain para la emisión y verificación de microcredenciales (Figura 2), el cual está dividido en dos secciones principales: a) la ontología que soporta el modelo y b) la arquitectura técnica basada en Blockchain. En las siguientes páginas se profundizará en cada elemento.

- **Ontología**
  - Información del estudiante
  - Información de enrolamiento en cursos
  - Información de aprobación de cursos
  - Información del proceso de certificación
- **Arquitectura basada en blockchain**
  - **Frontend**
    - Frontal para la gestión de las entidades que interactúan en el modelo

Fig. 2. Modelo de gestión de confianza

- Frontal para la consulta y verificación de microcredenciales emitidas
- Aplicativo móvil para la consulta y verificación de microcredenciales emitidas

– **Backend**

- Lógica para la generación de microcredenciales en formato JSON-LD, en base al estándar Blockcerts
- Lógica para el envío y notificación de enlaces para consulta de microcredenciales
- Lógica para la definición de rutas de aprendizaje personalizadas
- Lógica para la creación de identificaciones descentralizadas (DIDs)
- Lógica para la creación de URLs de almacenamiento descentralizadas usando IPFS

B. Desarrollo de la ontología para microcredenciales universitarias

La ontología del modelo asegura una representación precisa y detallada de las microcredenciales, incorporando información relevante y significativa como detalles del estudiante, del curso, del proceso de emisión de la credencial, habilidades adquiridas, nivel de maestría, y otros aspectos pertinentes vinculados a la adquisición de nuevas competencias por parte del estudiante.

En la Tabla II, se describe el detalle de las clases principales que componen la ontología propuesta para la emisión y verificación de microcredenciales, ofreciendo una descripción exhaustiva de los elementos que la integran.

De igual manera, en la Tabla III se incluye un listado de las propiedades principales empleadas en el diseño de la ontología. Cada propiedad cuenta con un dominio y un rango asociados que especifican los tipos de entidades que pueden estar interrelacionadas por esa propiedad. Por ejemplo, la propiedad 'CoursehasCourseInstructor' tiene como dominio 'vivo:Course' y como rango 'vivo:FacultyMember', lo que significa que esta propiedad establece una relación entre un curso y su instructor.

Esta estructura coherente dota a las microcredenciales de una mayor comprensibilidad y verificabilidad, lo que potencia su reconocimiento y valor tanto en el ámbito académico como en el laboral. En la figura 3, se despliega una representación gráfica de la ontología propuesta, aportando una visión clara y sistemática de los principales elementos del modelo.

TABLE II
CLASES DE LA ONTOLOGÍA

Clase	Prefijo	Descripción
Microcredential	microcu	Subclase de Credential, representa una microcredencial.
Credential	vivo	Representa una credencial.
Consortium	vivo	Subclase de Organization, representa un consorcio.
Organization	foaf	Representa una organización.
OpenBadge	microcu	Subclase de Credential, representa una insignia abierta.
LearningOutcome	cs2013	Representa un resultado de aprendizaje.
Student	vivo	Subclase de Person, representa a un estudiante.
LearningPath	microcu	Representa un camino de aprendizaje.
Course	vivo	Representa un curso.
University	vivo	Subclase de Organization, representa una universidad.
LevelOfMastery	cs2013	Representa un nivel de dominio.
Instructor	vivo	Subclase de Person, representa a un instructor.
Person Organization Unit	vivo foaf	Representa a una persona. Representa un departamento académico.
Issuer	microcu	Subclase de Person, representa a un emisor.
University	microcu	Subclase de University, representa una universidad.

TABLE III
PROPIEDADES DE LA ONTOLOGÍA

Propiedad	Prefijo	Dominio	Rango
has CourseOffering	microcu	Organization Unit	Course
has LearningOutcome	vivo	Course	Learning Outcome
hasLevelOf Mastery	cs2013	Learning Outcome	LevelOfMastery
has CourseInstructor	vivo	Course	Instructor
IsPartOf	microcu	Course	Learning Path
issues	microcu	Issuer	Credential
holdsAccount	vivo	Student	Course
hasCredential	vivo	Student	Credential

- Las clases *Credential*, *Microcredential* y *OpenBadge* representan la certificación como logro del aprendizaje adquirido por los estudiantes. Al haber incluido a la clase *Credential*, se podría adaptar la ontología no solamente al ámbito de las microcredenciales, sino a otro tipo de certificaciones, como por ejemplo en la utilización de OpenBadges.
- Las clases *Student*, *Instructor* y *Issuer* representan a los distintos roles que una persona puede ocupar en esta ontología. Estas clases representan al individuo que adquiere las competencias del curso (Estudiante), a quien imparte el curso (Instructor) y a quien emite las credenciales (Emisor) correspondientes a las habilidades adquiridas.
- La clase *Course* simboliza un curso dentro del marco de la formación continua. Esta entidad posibilita la representación detallada de la estructura del curso y está relacionada con los resultados de aprendizaje que los participantes pueden esperar alcanzar tras la culminación del mismo.
- Las clases *University* y *OrganizationUnit* permiten modelar la estructura organizativa dentro de la cual se lleva a cabo la formación continua. Estas entidades permiten definir y generar la oferta de cursos.
- Las clases *Organizations* y *Consortium* permiten modelar los distintos roles que ocupan las organizaciones en la ontología. La clase *Consortium* permite agrupar a distintas organizaciones educativas permitiendo definir un espacio colaborativo para impulsar el modelo propuesto.
- La clase *LearningPath* representa las rutas de aprendizaje, que se definen como los caminos o secuencia que puede seguir un estudiante para alcanzar una formación en un determinado campo del conocimiento.
- La clase *LevelOfMastery* permite representar el nivel de dominio o maestría que un estudiante está alcanzando respecto a un curso en específico.
- Finalmente, la clase *LearningOutcome* permite representar a los resultados del aprendizaje. Estas habilidades indican los conocimientos adquiridos fruto del proceso de aprendizaje y aprobación del curso de formación continua.

Fig. 3. Ontología diseñada en Protege

Para el diseño y validación de la ontología se utilizó la herramienta Protege, un software líder en la creación, edición y manejo de ontologías, brindando precisión y eficacia a todo el proceso.

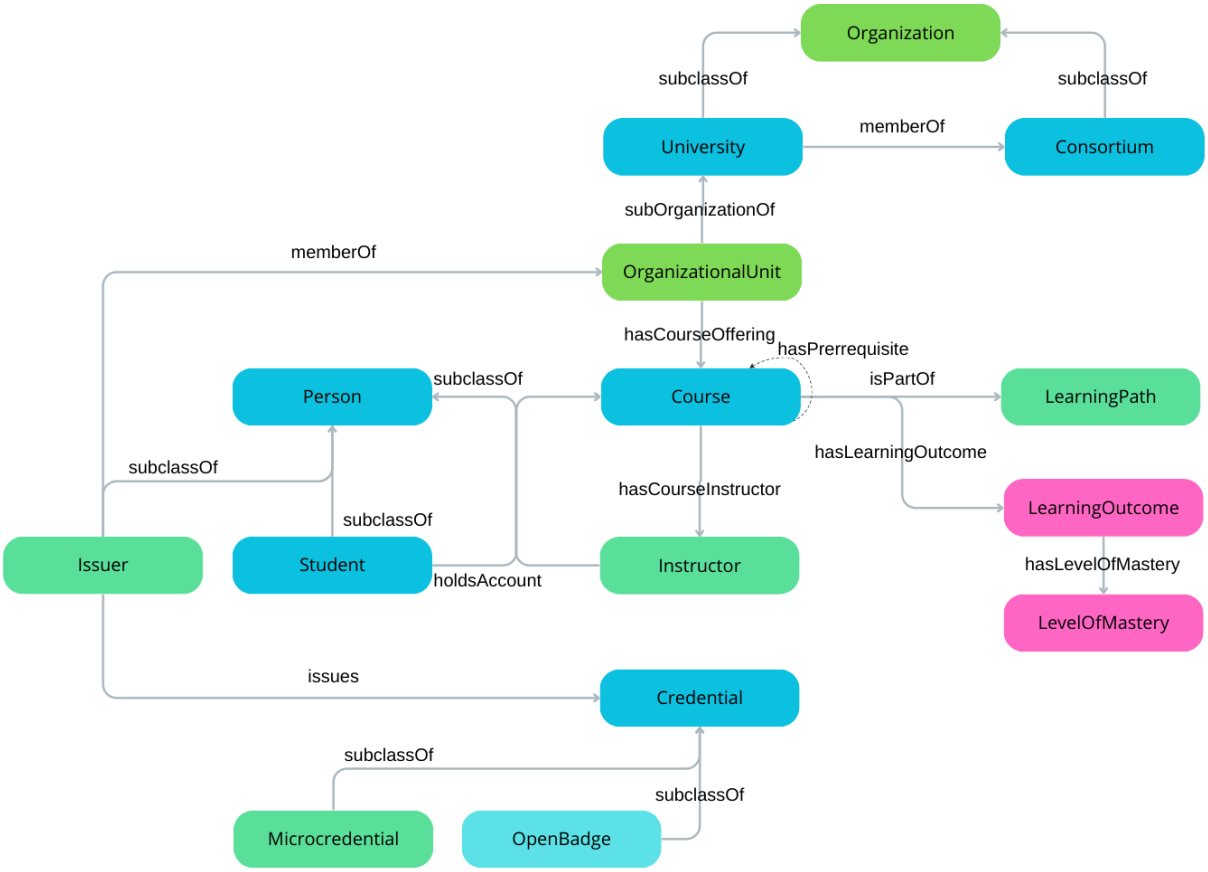

Fig. 4. Ontología propuesta

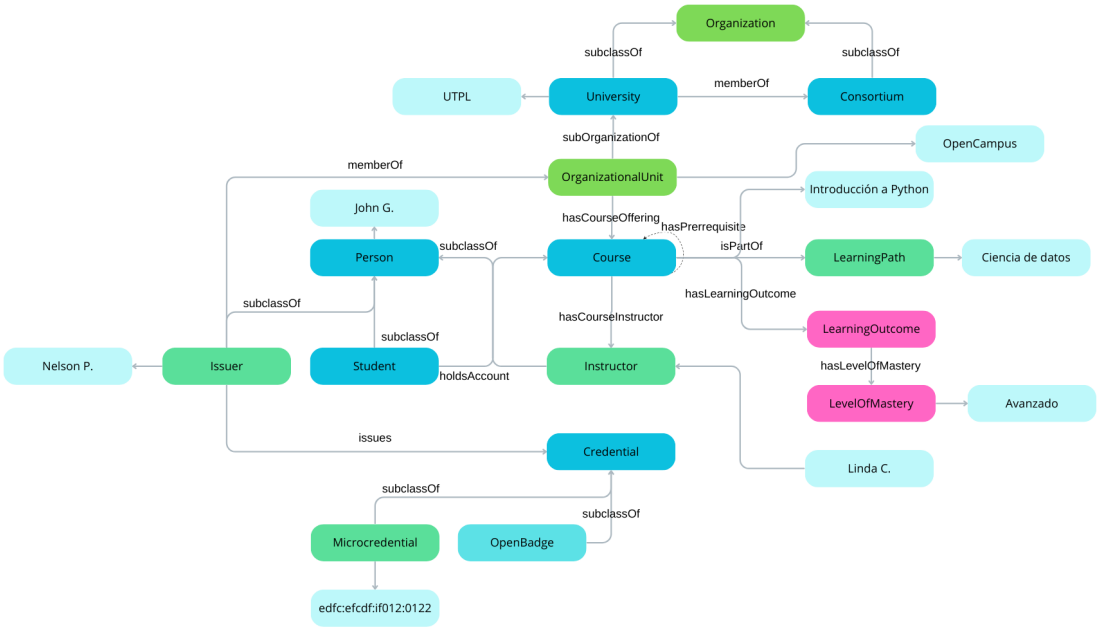

Fig. 5. Instanciación de clases de la ontología

C. *Estructura técnica basada en Blockchain*

La estructura técnica del sistema desempeña un papel fundamental en el desarrollo de un ecosistema sólido y eficiente para la emisión y verificación de microcredenciales universitarias. La estructura está dividida en dos componentes principales: el frontend y el backend.

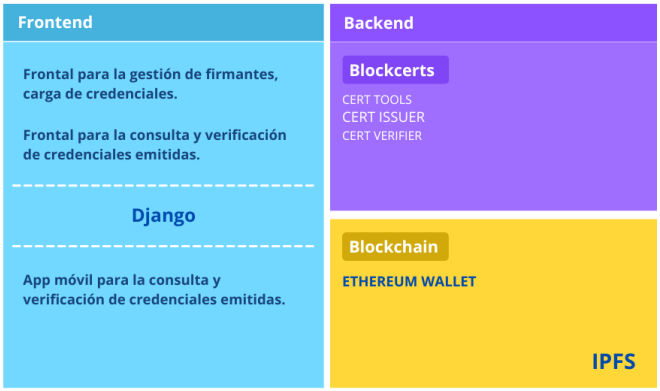

Fig. 6. Estructura técnica basada en Blockchain

1) ***Frontend:****:* En el frontend, los usuarios pueden interactuar con el sistema para llevar a cabo acciones clave como la creación de entidades y la configuración de preferencias del sistema. Estas funciones se implementan de manera intuitiva y eficiente, ofreciendo a los usuarios un control significativo sobre sus interacciones con el sistema.sss

El frontend propuesto está construido sobre Django, un marco de trabajo en Python de alto nivel, que promueve un desarrollo rápido, limpio y pragmático de las aplicaciones. Este enfoque, basado en el principio ”No se repita a sí mismo” (DRY), permite lograr una mayor eficiencia y un código más mantenible.

a) ***Portal de Verificación de Microcredenciales****:* En el frontend se ofrece un portal de verificación de microcredenciales. Este componente permite a los usuarios cargar y validar sus microcredenciales de forma independiente, proporcionando una plataforma transparente para el reconocimiento y verificación de las competencias adquiridas. Esta característica es fundamental para mantener la confianza en el sistema y garantizar que las microcredenciales siguen siendo una medida válida y confiable de habilidades y conocimientos.

Cabe destacar que, este componente facilitará a las empresas e instituciones empleadoras la validación de las habilidades adquiridas por sus candidatos, permitiéndoles tomar decisiones más informadas y efectivas durante sus procesos de selección de personal.

2) ***Backend****:* El backend del sistema es la pieza clave en la gestión, emisión y verificación de las microcredenciales. Para esto, se ha decidido hacer uso de los principales módulos de Blockcerts, que proporcionan una serie de herramientas para facilitar la emisión y verificación de certificados basados en la tecnología Blockchain. Esto asegura que las microcredenciales emitidas sean seguras, inalterables y fácilmente verificables por cualquier entidad.

a) ***Generación de microcredenciales en formato JSON-LD****:* El backend genera microcredenciales en el formato estandarizado JSON-LD (JavaScript Object Notation for Linked Data). Este formato se seleccionó debido a su capacidad para integrar y representar datos en un contexto específico, lo cual permite una gran interoperabilidad y estandarización. El uso de la ontología descrita previamente proporciona la estructura necesaria para generar las microcredenciales de forma consistente y significativa.

b) ***Rutas de aprendizaje personalizadas****:* Además, el backend se encarga de la lógica de definición de rutas de aprendizaje, lo que permite que se pueda configurar un camino educativo personalizado para cada estudiante. Esta funcionalidad asegura que cada usuario pueda seguir un camino alineado con sus objetivos y necesidades de aprendizaje.

c) ***URLs Descentralizadas mediante IPFS****:* Para garantizar la integridad y accesibilidad a largo plazo de las microcredenciales emitidas, el sistema genera URLs descentralizadas utilizando el Sistema de Archivos Interplanetarios (IPFS) como mecanismo de almacenamiento. IPFS es un protocolo y red diseñados para crear un método de almacenamiento y compartición de archivos descentralizado, lo que asegura la durabilidad y resistencia a la censura de las microcredenciales.

d) ***Identificación descentralizada con DIDs****:* Finalmente, el sistema utiliza Identificadores Descentralizados (DIDs) para garantizar la descentralización de las identidades. Los DIDs son una forma de identificador que permite que las entidades se autoidentifiquen de manera segura a través de sistemas digitales sin la necesidad de una autoridad central. Esta capacidad es esencial para garantizar la privacidad, la seguridad y la autenticidad de las interacciones dentro del sistema.

e) ***Ethereum****:* Se ha seleccionado a Ethereum como la plataforma Blockchain que soportará el modelo de emisión y verificación de microcredenciales. Ethereum es una de las plataformas de Blockchain más reconocidas y utilizadas en el mundo, conocida por su flexibilidad, seguridad y transparencia. Una característica importante de esta plataforma es la posibilidad de generar contratos inteligentes, los cuales permiten la automatización de tareas y posibilitan la gestión automática de revocaciones de credenciales.

f) ***Integración de Blockcerts en el sistema****:* Blockcerts es una tecnología basada en Blockchain que desempeña un papel fundamental en el modelo de gestión de confianza descentralizado para la emisión y verificación de microcredenciales universitarias. Blockcerts proporciona un marco robusto y seguro para garantizar la autenticidad, la integridad y la confiabilidad de las credenciales.

- *Cert-Tools*: Este módulo se utiliza para generar y emitir las microcredenciales de manera segura. Cert-tools ofrece herramientas y utilidades que permiten a las universidades y a otras instituciones académicas definir los atributos y las características de las credenciales, como el nombre del estudiante, el curso completado, el nivel de maestría, entre otros. Con cert-tools, se puede generar un archivo digital que contiene la información de la credencial y su

firma digital, asegurando su autenticidad y permitiendo su verificación en el futuro.

- *Cert-Issuer*: Este módulo se encarga de emitir las microcredenciales en la Blockchain, proporcionando un mecanismo seguro y transparente para su almacenamiento y registro. Cert-issuer utiliza tecnologías de Blockchain, como Bitcoin o Ethereum, para crear una transacción inmutable que contiene los datos de la credencial emitida. Al hacerlo, se asegura que la credencial sea resistente a la manipulación y que pueda ser verificada por cualquier persona o entidad interesada en el futuro.
- *Cert-Verifier*: Este componente permite la verificación de las microcredenciales emitidas. Cert-verifier proporciona herramientas y utilidades que permiten a los receptores de las credenciales verificar su autenticidad y validez. Al ingresar la credencial en cert-verifier, se realiza una verificación criptográfica y se comprueba su integridad utilizando la información almacenada en la Blockchain. Esto asegura que las microcredenciales sean fiables y confiables, brindando una capa adicional de seguridad y garantía tanto para los estudiantes como para las instituciones emisoras.

En conjunto, los módulos de Blockcerts, cert-tools, cert-issuer y cert-verifier, ofrecen un enfoque integral para la emisión y verificación de microcredenciales universitarias. Estos componentes trabajan en conjunto para garantizar la seguridad, la confiabilidad y la transparencia en todo el ciclo de vida de las credenciales, desde su generación y emisión hasta su verificación por parte de las partes interesadas.

IV. Caso de uso: Emisión y verificación de microcredenciales OPENCAMPUS

OpenCampus es un proyectado que se apoya de una plataforma para realizar la oferta de cursos en línea a través de Internet, de forma abierta y libre. Con OpenCampus, los educadores y formadores pueden diseñar sus cursos, probar nuevas formas de aprendizaje, establecer retos que permitan hacer analítica y ofertar formación a estudiantes de cualquier lugar del mundo. Además, los expertos en tecnología han implementado componentes de aprendizaje como nuevas características de la plataforma, de manera que apoyan a la creación de soluciones educativas innovadoras que benefician a profesores, estudiantes y autodidactas.

Para el sistema de emisión de microcredenciales de OPENCAMPUS, se han identificado los siguientes actores:

- Entidad emisora
- Estudiante o profesional
- Administrador del sistema
- Blockchain
- Entidad verificadora

De forma general, se describen a continuación a los principales casos de uso del sistema de emisión y verificación de microcredenciales:

A. Crear entidades

En este caso de uso, se realizan las siguientes acciones:

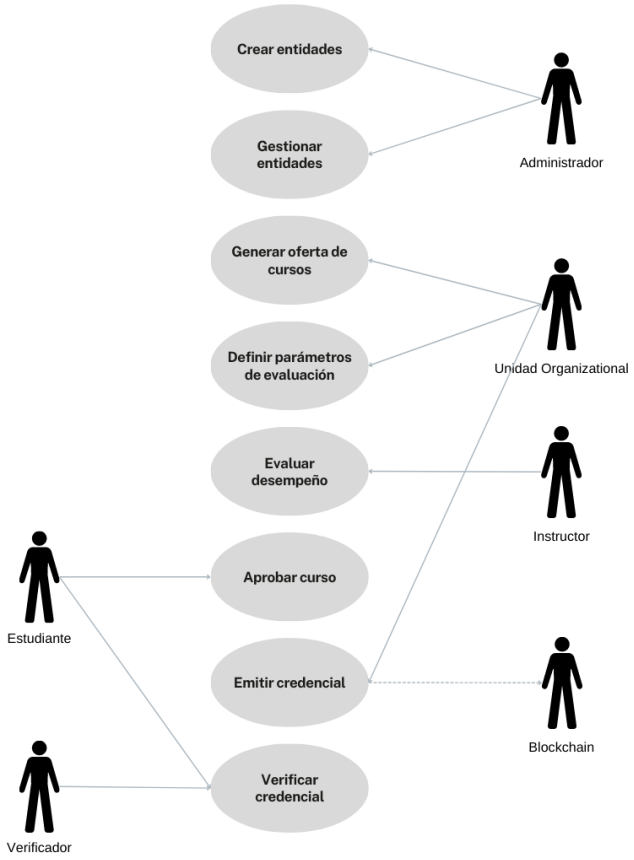

Fig. 7. Casos de uso del sistema de emisión de microcredenciales

- El administrador, que es responsable de la gestión de las entidades en el sistema, identifica la necesidad de crear una nueva entidad.
- El administrador ingresa los datos necesarios para crear la entidad en el sistema.
- El sistema crea la entidad y confirma su creación al administrador.

B. Gestionar entidades

En este caso de uso, se realizan las siguientes acciones:

- El administrador identifica la necesidad de modificar, actualizar o eliminar una entidad existente.
- El administrador realiza las acciones necesarias para gestionar la entidad en el sistema.
- El sistema realiza los cambios y confirma su realización al actor.

C. Generar oferta de cursos

En este caso de uso, se realizan las siguientes acciones:

- La unidad organizacional identifica la necesidad de crear un nuevo curso.
- La unidad organizacional define los parámetros del curso, como el contenido, los resultados de aprendizaje esperados, los requisitos previos, entre otros.

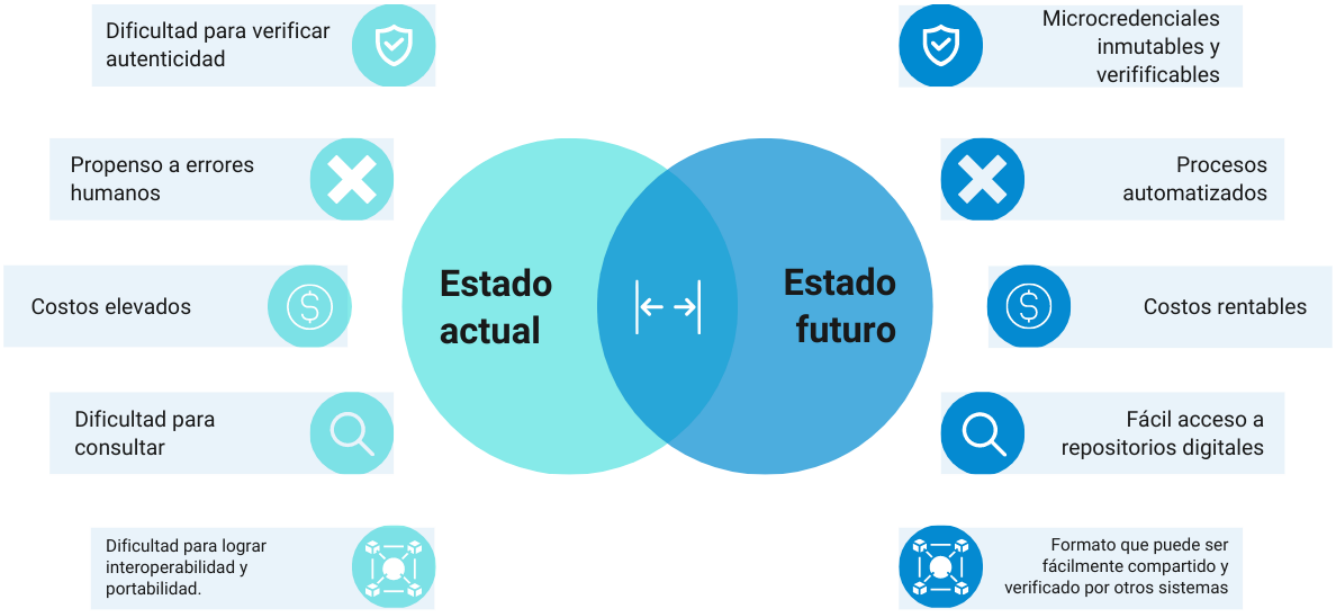

Fig. 8. Estado actual vs estado futuro

- El sistema crea el curso y confirma su creación a la unidad organizacional.

D. Definir parámetros de evaluación de los cursos

En este caso de uso, se realizan las siguientes acciones:

- La unidad organizacional en conjunto con el instructor identifican la necesidad de definir los parámetros de evaluación para un curso.
- Los actores definen los criterios y métodos de evaluación para el curso.
- El sistema registra los parámetros de evaluación y confirma su registro al instructor.

E. Evaluar desempeño de los estudiantes en el curso

En este caso de uso, se realizan las siguientes acciones:

- El instructor evalúa el desempeño de los estudiantes en un curso, basándose en los parámetros de evaluación definidos.
- El instructor asigna calificaciones a los estudiantes en función de su desempeño.
- El sistema registra las calificaciones y confirma su registro al instructor.

F. Aprobar cursos

En este caso de uso, se realizan las siguientes acciones:

- El estudiante completa los requisitos de un curso y solicita su aprobación.
- El instructor o la unidad organizacional verifica que el estudiante ha cumplido con los requisitos y ha alcanzado los resultados de aprendizaje esperados.
- El sistema registra la aprobación del curso y confirma su registro al estudiante y al instructor o unidad organizacional.

G. Emitir microcredenciales

En este caso de uso, se realizan las siguientes acciones:

- El estudiante completa un curso ofertado.
- El sistema de emisión de credenciales verifica la finalización del curso y las habilidades adquiridas por el estudiante/profesional.
- Se emite una credencial asociada a la identidad digital única y verificable del estudiante/profesional.
- La credencial se almacena en un registro inmutable en la cadena de bloques (Blockchain).

H. Verificar microcredenciales

En este caso de uso, se realizan las siguientes acciones:

- El verificador, que puede ser un empleador o una universidad educativa, solicita validad las habilidades y conocimientos de una persona.
- El estudiante proporciona acceso a su credencial.
- El verificador constata la autenticidad de la credencial a través del sistema de emisión de credenciales basado en Blockchain.

Como se puede apreciar en la Figura 8, se espera que la implementación del modelo de gestión descentralizada tenga un impacto significativo en el proceso de emisión y verificación de microcredenciales educativas en la plataforma Opencampus. En la actualidad, existen ciertos desafíos asociados a las credenciales educativas generadas, ya que su autenticidad resulta difícil de verificar, dificultando su consulta por parte

de las empresas empleadoras. Además, el proceso actual de generación de estas credenciales es costoso y susceptible a errores humanos.

La integración de un modelo de gestión descentralizado basado en Blockchain permitirá la generación de credenciales educativas más confiables y fáciles de verificar, así como en un proceso más eficiente, menos costoso y menos propenso a errores.

V. Conclusiones y trabajos futuros

La tecnología Blockchain muestra un gran potencial para dar solución a problemas de transparencia, seguridad y autenticidad en la emisión y verificación de microcredenciales. Gracias a la revisión de la literatura existente, se identificó que Blockchain proporciona una plataforma segura y descentralizada para el proceso de emisión, almacenamiento y verificación de este tipo credenciales.

Blockcerts, al estar basado en un estándar abierto permite la interoperabilidad entre diferentes sistemas y plataformas, lo que garantiza la confiabilidad y transparencia de las credenciales emitidas. Además, su seguridad, escalabilidad y medidas de privacidad hacen de Blockcerts una opción ideal para instituciones educativas. Su amplia adopción a nivel mundial es una muestra de su confiabilidad y viabilidad.

En el presente manuscrito se propone la adopción de la tecnología Blockchain en el sector educativo, específicamente en la emisión y validación de microcredenciales universitarias. La implementación de un sistema basado en estándares abiertos, posibilita que plataformas educativas, como Opencampus, puedan mejorar la transparencia, la confiabilidad y la eficiencia en los procesos educativos.

El desarrollo de una ontología específica para microcredenciales universitarias es un paso importante para definir y estandarizar las relaciones entre las diversas entidades involucradas en el proceso de emisión y verificación de estas credenciales. Esta ontología puede servir como un marco de referencia para futuras implementaciones en otras instituciones educativas.

Uno de los desafíos clave que se puede abordar en trabajos futuros es la correcta gestión de las identidades descentralizadas en el modelo. Para superar este desafío, es fundamental establecer estándares y marcos de trabajo claros que permitan la interoperabilidad efectiva de los Identificadores Descentralizados (DIDs) entre diferentes plataformas y sistemas.

La ontología propuesta podría desempeñar un papel importante en la resolución de este desafío. Mediante la abstracción adecuada de esta problemática, se puede proporcionar una solución que permita la correcta gestión de las identidades descentralizadas en el modelo. La ontología podría definir los conceptos y las relaciones necesarias para representar y manipular los DIDs de manera correcta.

Referencias bibliográficas

[1] Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26

[2] Clements, K., West, R. E., Hunsaker, E. (2020). Getting started with open badges and open microcredentials. International Review of Research in Open and Distributed Learning, 21(1), 154-172.

[3] Ehrenreich, J., Mazar, I., Rampelt, F., Schünemann, I., Sood, I. (2020). Recognition and verification of credentials in open education. Report of intellectual output 3. Url: https://oepass.eu/wp-content/uploads/sites/22/2020/03/OEPass-IO3-report-1.pdf.

[4] Poveda, L. A. (2018). Alguns aspectes sobre Blockchains i smart contracts en educació superior. Revista d'Innovació Docent Universitària, 65-76.

[5] Mosquera, J., Piedra, N. (2020). Methodological Framework for the integration of Blockchain Technology in Coffee Industy. 2020 9th International Conference On Software Process Improvement (CIMPS), 35-43.

[6] Chukowry, V., Nanuck, G., Sungkur, R. K. (2021). The future of continuous learning–Digital badge and microcredential system using Blockchain. Global Transitions Proceedings, 2(2),355-361

[7] Vidal, F., Gouveia, F., Soares, C. (2019). Analysis of Blockchain technology for higher education. 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 28-33.

[8] Jaramillo, M. P. (2020). Use of Blockchain technology for Academic Certification in Higher Education Institutions. LACLO 2020.

[9] Pollard, V., Vincent, A. (2022). Micro-credentials: A Postdigital Counternarrative. Postdigital Science and Education, 1-17.

[10] Jirgensons, M., Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. Journal of teacher education for sustainability, 20(1), 145-156.

[11] Bartolomé, A., Lindín, C. (2018). EKS Posibilidades del Blockchain en Educación Blockchain possibilities in Education. https://doi.org/https://doi.org/10.14201/eks20181948193

[12] Turcu, C., Turcu, C., Chiuchisan, I. (2019). Blockchain and its Potential in Education. arXiv preprint arXiv:1903.09300.

[13] Alammary, A., Alhazmi, S., Almasri, M., Gillani, S. (2019). Blockchain-based applications in education: A systematic review. Applied Sciences, 9(12), 2400.

[14] sweli, N. T., Twinomurinzi, H., Ismail, M. (2022). The International Case for Micro-Credentials for Life-Wide And Life-Long Learning: A Systematic Literature Review. Interdisciplinary Journal of Information, Knowledge, and Management, 17, 151-190.