



**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

CARRERA DE INGENIERÍA DE SISTEMAS

**DISEÑO DE UNA APLICACIÓN PROTOTIPO UTILIZANDO
TECNOLOGÍA BLOCKCHAIN PARA EL MANEJO DE
ASIGNATURAS, PROFESORES, ESTUDIANTES Y EL
REGISTRO DE CALIFICACIONES**

Trabajo de titulación previo a la obtención del
Título de Ingeniero de Sistemas

AUTOR: DIEGO MAURICIO YÁNEZ PASQUEL

TUTOR: GUSTAVO ERNESTO NAVAS RUILOVA

Quito - Ecuador
2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, DIEGO MAURICIO YÁNEZ PASQUEL, con documento de identificación N° 1723672232, manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 18 de agosto de 2023

Atentamente,



Diego Mauricio Yáñez Pasquel
1723672232

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Diego Mauricio Yánez Pasquel, con documento de identificación N° 1723672232, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del artículo académico: "Diseño de una aplicación prototipo utilizando tecnología blockchain para el manejo de asignaturas, profesores, estudiantes y el registro de calificaciones", el cuál ha sido desarrollado para optar por el título de: INGENIERO DE SISTEMAS, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 18 de agosto de 2023

Atentamente,



Diego Mauricio Yánez Pasquel
1723672232

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Gustavo Ernesto Navas Ruilova con documento de identificación N° 1705675625, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: DISEÑO DE UNA APLICACIÓN PROTOTIPO UTILIZANDO TECNOLOGÍA BLOCKCHAIN PARA EL MANEJO DE ASIGNATURAS, PROFESORES, ESTUDIANTES Y EL REGISTRO DE CALIFICACIONES, realizado por Diego Mauricio Yáñez Pasquel con documento de identificación N° 1723672232, obteniendo como resultado el trabajo de titulación bajo la opción de Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 18 de agosto de 2023

Atentamente,



Ing. Gustavo Ernesto Navas Ruilova, MSc
1705675625

Diseño de una aplicación prototipo utilizando tecnología Blockchain para el manejo de asignaturas, profesores, estudiantes y el registro de calificaciones.

Design of a prototype application using Blockchain technology for the management of subjects, teachers, students and the recording of grades.

Diego Mauricio Yáñez Pasquel, Ing. Gustavo Ernesto Navas Ruilova

Resumen

La tecnología Blockchain ha despertado un enorme interés en el ámbito educativo debido a sus características únicas que ofrecen seguridad y transparencia en la gestión de información y las distintas transacciones que pueden favorecer en la creación del prototipo con la capacidad de realizar el registro académico. El objetivo del prototipo que se ha desarrollado es proporcionar una plataforma que permita a los distintos usuarios: crear, manipular y registrar la información de forma confidencial e íntegra, mediante el uso de la tecnología Blockchain.

El uso de tecnologías como Ethereum, Solidity, Truffle, Ganache e IPFS permite construir un prototipo basado en Blockchain que ofrece una plataforma segura y transparente. Este prototipo tiene como objetivo proporcionar crear registros "inmutables y descentralizados" en donde se pueda garantizar la integridad de la información, permitir la verificación y sus credenciales para poder acceder de acuerdo a su rol, y así facilitar el intercambio de información de los estudiantes, con las instituciones educativas.

Este trabajo está implementado fundamentalmente para el uso de la tecnología de blockchain en un sistema donde se realiza el manejo de asignaturas, profesores y calificaciones, donde se pretende que sea un prototipo sin una funcionalidad completa, sino más bien el destacar el uso del blockchain.

Palabras clave: Consenso, Blockchain, IPFS, Solid, Truffle y Ganache.

Abstract

Blockchain technology has aroused enormous interest in the educational field due to its unique features that offer security and transparency in the management of information and the various transactions that can be favored in the creation of the prototype with the ability to perform academic registration. The objective of the prototype that has been developed is to provide a platform that allows different users to that allows different users to: create, manipulate and record information in a confidential and integrated way, through the use of Blockchain technology.

The use of technologies such as Ethereum, Solidity, Truffle, Ganache and IPFS allows to build a Blockchain-based prototype that provides a secure and transparent platform. This prototype aims to provide create "immutable and decentralized" records where the integrity of the information can be guaranteed, allow verification and their credentials to be able to access according to their role, and thus facilitate the exchange of information of students, with educational institutions.

This work is implemented primarily for the use of blockchain technology in a system where the management of subjects, teachers and grades is performed, where it is intended to be a prototype without full functionality, but rather to highlight the use of blockchain.

Keywords: Consensus, Blockchain, IPFS, solid, truffle and ganache.

¹ Ingeniería de Sistemas, Universidad Politécnica Salesiana, Ecuador.

Autor para correspondencia: dyanezp@est.ups.edu.ec

² Artículo académico previo la obtención del título de Ingeniero en Sistemas.

1. Introducción

La tecnología Blockchain cada vez tiene más usos y es por eso que ha generado un enorme interés en estos años debido a la seguridad que proporciona y a sus distintas características donde ofrece un alto nivel de seguridad y transparencia en la gestión de la información. En este contexto, la aplicación en el ámbito educativo representa una oportunidad extraordinaria para desarrollar un prototipo capaz de compartir la información de forma segura y por ello se realizará un prototipo capaz de registrar asignaturas, estudiantes, profesores y el correcto registro de calificaciones.

Al aprovechar la capacidad de Blockchain para crear registros "inmutables y descentralizados", esta herramienta podría garantizar la integridad de los datos educativos, permitir la verificación, validación de certificados, credenciales, y por ende el intercambio de información de los estudiantes con las instituciones educativas. Además, al eliminar intermediarios y centralizaciones, se podrían agilizar los procesos administrativos y minimizar los riesgos de fraude [1].

Para construir el prototipo basado en Blockchain y lograr este objetivo, podrían utilizarse diversas tecnologías y métodos. En este caso, puede emplearse la plataforma Blockchain de Ethereum para establecer y llevar a cabo contratos inteligentes. La red Ethereum usa el lenguaje de programación Solidity para construir contratos inteligentes [2].

Las pruebas de trabajo se han realizado con el consenso más popular para Ethereum, donde los nodos, o mineros, resuelven criptográficos desafiantes para validar y producir bloques. Por minar un bloque y las tasas de transacción que incluye se compensa a los mineros. Dado que Ethereum emplea actualmente un mecanismo de medición basado en el gas, los usuarios se ven obligados a elegir un precio de gas óptimo para evitar pagar demasiado o demasiado poco. En la actualidad, los usuarios dependen de oráculos de precios de gas como Geth y EthGasStation, pero estos sistemas son poco fiables y se bloquean con frecuencia. Gas es un concepto que Ethereum usa para fijar los precios de las transacciones y detener el abuso o mal comportamiento de la red. Cada transacción tiene un límite y un precio de gas fijado por el emisor, y este gas se emplea para calcular el coste de la

potencia de cálculo programable necesaria para la transacción. En función del precio del gas ofrecido por el remitente, los mineros pueden decidir si aceptan o rechazan las transacciones. Si el remitente no suministra suficiente gas, la transacción se considera inválida y se devuelve el gas no empleado [3].

Además, se utilizarán herramientas para facilitar el desarrollo, la compilación y la prueba de los contratos inteligentes como "Truffle y Ganach", y para gestionar la información de forma distribuida, se almacenará la información de forma segura y descentralizada con IPFS [4, 5].

El objetivo de la aplicación es proporcionar una plataforma, capaz de permitir a los usuarios crear y administrar las asignaturas, profesores y registrar las calificaciones en cada asignatura de los estudiantes, de manera que los desarrolladores puedan escribir contratos inteligentes con reglas personalizadas, la tecnología Blockchain permite que cualquier persona pueda participar en la red de Ethereum ejecutando un nodo en su máquina [6].

En resumen, el desarrollo de una aplicación basada en tecnología Blockchain para la gestión de asignaturas, profesores, estudiantes y el registro de calificaciones, una herramienta muy valiosa para mejorar la manipulación de la información y la transparencia en el ámbito educativo.

La utilización de tecnologías como Ethereum, Solidity, Truffle, Ganache e IPFS nos permitirán desarrollar una aplicación "segura, descentralizada y transparente", con una solución innovadora y de calidad para la gestión en el ámbito educativo [7].

2. Trabajos Relacionados

Este artículo se fundamenta en una serie de elementos y conceptos clave que requieren un análisis detallado para poder desarrollar el presente prototipo. Se han dedicado esfuerzos exhaustivos para comprender el uso de Blockchain en diversos contextos, lo cual ha sido fundamental para informar y respaldar el desarrollo actual del prototipo.

En el artículo [5] la criptomoneda Bitcoin ha generado un alto grado de interés hacia las distintas áreas de trabajo en donde ha aumentado el incremento de tecnologías que usan Blockchain, en donde el Internet de las cosas (IoT), realiza tareas que generen un sistema que permita almacenar datos en una red descentralizada, capaz de generar un contrato inteligente, con la plataforma

Blockchain Ethereum, como lenguaje de desarrollo Solidity, para codificar la simulación del prototipo NodeJS y para poder guardar la información IPFS, con esto se ha generado una gran ventaja a la hora de almacenar la cadena de bloques de Ethereum. Blockchain almacena nuestra información de forma segura, ya que se almacena en todos los nodos, lo que ayuda a descentralizar el sistema, generando un registro de cada transacción y agregando bloques por cada transacción mediante validaciones y el consenso adecuado, ofreciendo así un sistema libre de ataques impidiendo que se alcance el consenso. Para ello, las billeteras Blockchain cuenta con una clave privada y pública, capaz de permitir transacciones uniendo las dos claves [5].

En el artículo [6] se define la tecnología Blockchain, como un libro mayor, distribuido e inmutable que ha ganado popularidad en todo el mundo. Fue destacada después de la publicación del libro blanco de Satoshi Nakamoto en 2008, donde se presentó una solución para el problema del doble gasto en una red descentralizada. Ethereum es la plataforma blockchain más utilizada y permite a los desarrolladores escribir contratos inteligentes con reglas personalizadas.

En los artículos [4, 8] podemos ver que, la información educativa se la maneja desde que se empieza la educación básica, hasta llegar a la educación superior y posteriormente a la vida profesional, pero para manipular de forma correcta la información tanto de los estudiantes como de los profesores en la actualidad existen varias opciones, pero una de las más seguras es las cadenas de bloques que genera Blockchain, aunque están relacionados con las criptomonedas existen técnicas que nos permiten utilizar la blockchain en diferentes áreas y una de ellas es la educación [9]. En donde la innovación de las nuevas tecnologías maximiza la forma correcta de manipular la información y garantiza [10] el uso de estos registros con una cadena de bloques, teniendo confianza y seguridad con una aplicación descentralizada capaz de compartir la información de los estudiantes de forma segura [11], usando la firma digital como una tecnología de encriptación asimétrica de forma que sea difícil de imitar, falsificar o manipular [12].

En los artículos [4, 12, 13] podemos ver qué blockchain ha generado un alto grado de popularidad, pero no existe una guía capaz de ampliar los conocimientos de esta nueva tecnología, para com-

prender la estructura se puede considerar aspectos teóricos y el empleo de aplicaciones web capaces de desarrollar y simular aplicaciones descentralizadas por parte de estudiantes con conocimientos en informática, una de las desventajas es la falta de habilidades para poder crear aplicaciones o realizar actividades donde se pueda experimentar con este tipo de aplicaciones descentralizadas.

El almacenar la información en la nube ha generado una facilidad el compartir y transferir información, sin embargo, los ataques a la información por parte de personas externas ha generado que se busque una mejor forma de proteger nuestra información y gracias a Ethereum se logró implementar los Smart Contracts complejos.

En el artículo [9] menciona que una de las ventajas de Blockchain es que nos permite llevar a cabo transacciones sin necesidad de algún tercero, con la confianza de que la información compartida se distribuye en todos los nodos que conforma la red, de forma íntegra y anónima. Cabe recalcar que la base del cifrado es la confianza que se le da a este mecanismo, pues debe ser capaz de cifrar y almacenar datos en el libro mayor como una cadena de bloque vinculado al anterior mediante un código hash incapaz de ser manipulado, blockchain necesita de un protocolo para proporcionar los acuerdos entre nodos para poder validar los datos que se almacenaran en el libro mayor a este proceso se lo llama consenso, para el desarrollo del presente prototipo se encontraron varias plataformas como Ethereum, Bitcoin, Nano, etc. Pero el que se utilizará para desarrollar es la plataforma de Ethereum, cuya criptomoneda es el Ether [1].

En el artículo [14] podemos ver que el uso de un sistema de transacciones Blockchain garantiza todo tipo de proceso legal, es decir, no será necesario de terceros como: abogados, contadores, entre otros intermediarios, porque el proceso será más rápido, seguro y sólido, gracias a la tecnología Peer-to-Peer. Los archivos que son demasiado grandes para almacenar son manipulados por IPFS mismo que usa algoritmos SHS-256 en donde devuelve hashes y se almacena en las cadenas de bloques usando contratos inteligentes cuando se accede a los registros.

En los artículos [15, 16] vemos que las cadenas con enormes registros no se guardan de forma

eficiente y desde la perspectiva de cadena de bloques, repetirá esta cadena en numerosos nodos y se necesitará de espacio adicional para almacenar dicha información, generando lentitud a la hora de almacenar, controlar o modificar la información, aumentando el costo a la hora de realizar cada ejecución, por ello IPFS innovo el intercambio de información con registros gigantescos de manera viable con las personas que sean específicas, actuando como una huella única donde mejora el intercambio de documentos Peer-to-Peer y ofreciendo mejor seguridad, ya que decide su ubicación y elimina cualquier registro repetitivo a la hora de almacenar la información.

y costoso, por ello Blockchain es seguro [19,20].

Una forma de mantener un registro compartido y descentralizado de transacciones, con un registro criptográfico que puede ser validado por múltiples nodos. Los contratos inteligentes son programas de computadora que establecen reglas para la evolución de los hechos en la cadena de bloques. Ya que, al combinar contratos inteligentes, se pueden automatizar transacciones y garantizar que cumplan con los acuerdos legales subyacentes [21].

3. Metodología y Materiales

3.2. Diagrama de bloques

3.1. Materiales

Para la obtención acerca de la tecnología Blockchain y los procesos que intervienen en el prototipo se hará uso de fuentes bibliográficas y de páginas oficiales de investigación de manera digital, esto implica la codificación del código fuente y la configuración de la arquitectura, se utiliza Solidity como lenguaje de desarrollo del prototipo, MetaMask como la aplicación de billetera para realizar la transacción, además se usará el gas que nos ofrece ethereum y por ende para poder utilizar el protocolo de desarrollo Blockchain [4]. Además, es una plataforma que permite ejecutar aplicaciones descentralizadas [1] y una opción segura con los servicios que dan las empresas públicas y privadas cuando se interactúa con el usuario final [17].

Solid, se centra en el intercambio de información y la privacidad que tiene como objetivo construir un ecosistema descentralizado que cambie radicalmente la forma en que funcionan las aplicaciones web en la actualidad. Blockchain, equipada con múltiples propiedades de seguridad y funciones de autenticación, es una tecnología crucial [18].

La cadena de bloques que registra información pública y segura, donde cada bloque contiene información encriptada, una huella única y la huella del bloque anterior. La prueba de trabajo y el consenso entre nodos aseguran la integridad de la cadena. Además, el sistema no depende de un servidor centralizado, sino que utiliza las computadoras de todos los participantes para mantener la cadena sin que se pueda modificarla, ya que sería muy difícil

Administrador

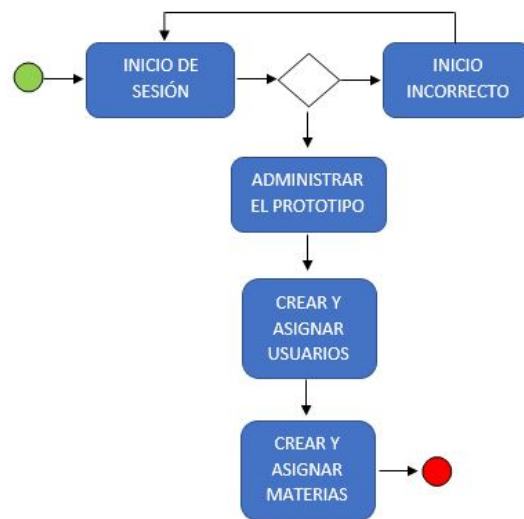


Figura 1. Bloque "Administrador".

Representa a un usuario con privilegios administrativos, encargado de la gestión global del prototipo. Puede realizar tareas como agregar o eliminar firmas, asignar profesores a firmas, etc.

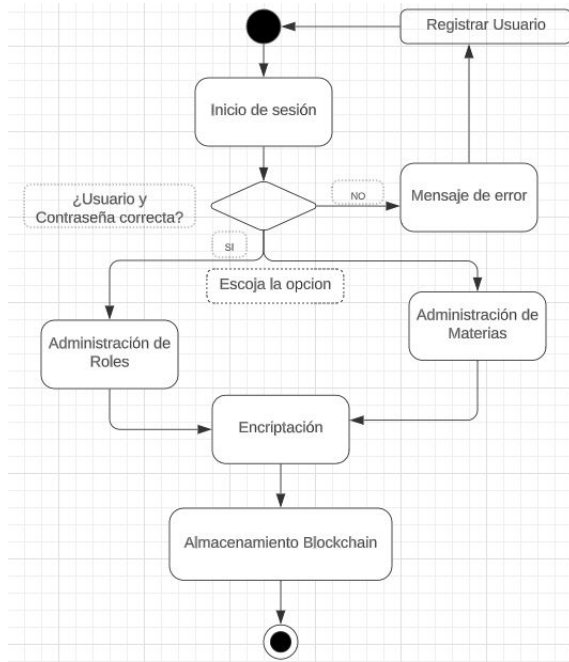


Figura 2. Diagrama de actividad "Administrador"

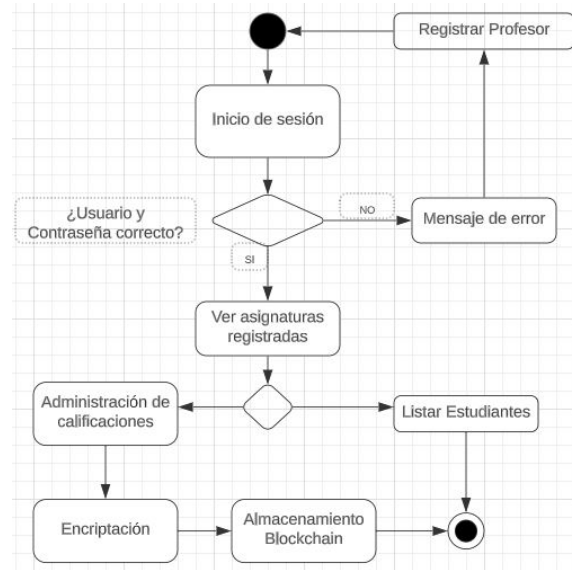


Figura 4. Diagrama de actividad "Profesores"



Figura 3. Bloque "Profesores"

Representa a los docentes que imparten las asignaturas. El administrador puede gestionar la información de los profesores, asignarlos a las asignaturas correspondientes, etc.

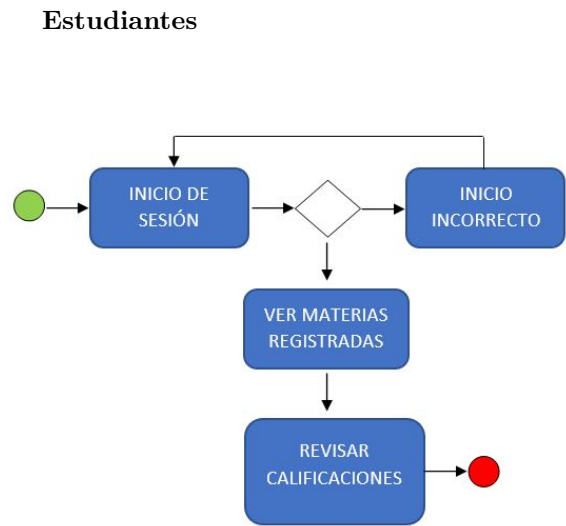


Figura 5. Bloque "Estudiantes"

Representa a los alumnos matriculados en las asignaturas. El administrador puede gestionar la información de los estudiantes, matricularlos en las asignaturas, etc.

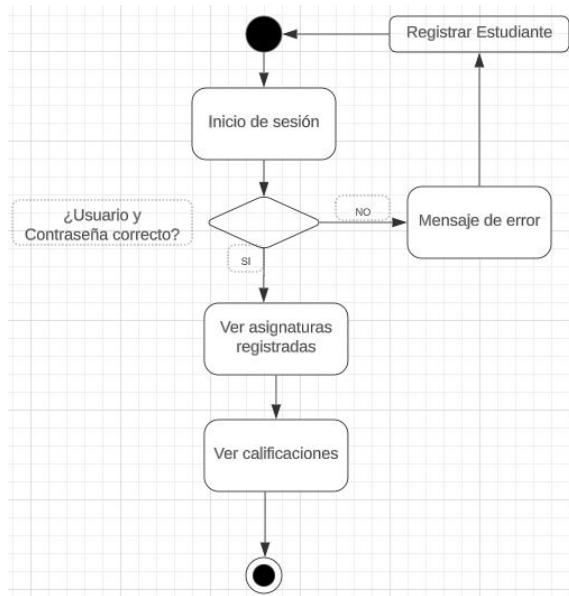


Figura 6. Diagrama de actividad "Estudiantes"

3.3. Metodología

Para la metodología de desarrollo ágil se usa SCRUM, ya que se puede trabajar de forma personalizada el prototipo que se llevara a cabo gracias a la amplia posibilidad de escalabilidad frente a la investigación de este artículo a realizar [22, 23].

3.3.1. Flujo de trabajo SCRUM

El presente artículo académico va dirigido a los estudiantes de las carreras de Computación, Ingeniería de Sistemas y personas profesionales que estén interesadas en conocer la tecnología Blockchain que requieran información con respecto a la seguridad, su forma de emplear y los distintos tipos de usos en el ámbito profesional con lo cual podrán hacer uso del conjunto de datos generados.

Se diseño un prototipo utilizando tecnología Blockchain para el manejo de asignaturas, profesores, estudiantes y el registro de calificaciones, empleando los materiales explicados anteriormente.

3.3.2. Product Owner

El Product Owner ha definido y priorizado los requisitos entre los (stakeholders) interesados y las

partes involucradas para comprender sus necesidades y definir los requisitos clave del prototipo, además se ha generado las siguientes necesidades hacia él (development team) equipo de desarrollo para comunicar los requisitos y garantizar una comprensión clara del producto final.

Los requisitos del usuario son:

- Tener una opción para poder gestionar los usuarios, donde se pueda crear y gestionar usuarios con diferentes roles y permisos.
- Tener una opción para poder gestionar la información general del prototipo para almacenar y gestionar los datos de las asignaturas, profesores, estudiantes y calificaciones.
- Manipular la interfaz de usuario de forma intuitiva y fácil de utilizar.
- El prototipo tenga compatibilidad multi-plataforma con los diferentes navegadores, capaz de acceder al prototipo desde cualquier lugar.

Los requisitos del administrador son:

- Como administrador de seguridad, un prototipo con seguridades, para garantizar la privacidad y protección de la información.
- Como administrador tener un prototipo flexible y adaptable, con la posibilidad de añadir nuevas funcionalidades y características según las necesidades de los usuarios.
- Como administrador, un diseño escalable que permita agregar nuevas funcionalidades y características sin afectar el rendimiento y la eficiencia del prototipo.

3.3.3. Product BackLog

Las necesidades y funcionalidades relacionadas con el prototipo y que el cliente las detalla en la tabla1, esta tabla será útil para que los desarrolladores entiendan cuales son las funciones que tendrá disponible el prototipo.

Tabla 1. Product Backlog

| Sprints | Necesidades | Enunciado de historias de usuario |
|----------------|--------------------------------|---|
| Sprint 1 | Gestión de usuarios | Crear un nuevo usuario con diferentes roles y permisos. |
| | | Editar la información de un usuario existente. |
| | | Eliminar un usuario del prototipo. |
| | | Gestionar los permisos y roles de los usuarios. |
| Sprint 2 | Gestión de datos | Añadir una nueva asignatura al prototipo. |
| | | Añadir un nuevo profesor al prototipo. |
| | | Añadir un nuevo estudiante al prototipo. |
| Sprint 3 | Interfaz de usuario | Registrar las calificaciones de un estudiante en una asignatura. |
| | | Acceder a diferentes secciones del prototipo a través de un menú intuitivo. |
| Sprint 4 | Seguridad | Visualizar la información de las asignaturas, profesores, estudiantes y calificaciones de forma clara y ordenada. |
| | | Proteger los datos de los usuarios mediante la encriptación de la información. |
| Sprint 5 | Compatibilidad multiplataforma | Ofrecer un sistema de autenticación seguro para garantizar que solo los usuarios autorizados puedan acceder al prototipo. |
| | | Diseñar un prototipo compatible con los diferentes navegadores, como Firefox y Chrome. |
| Sprint 6 | Flexibilidad | Ofrecer una interfaz de usuario adaptable a diferentes tamaños de pantalla y dispositivos. |
| | | Permitir que los usuarios personalicen el prototipo según sus preferencias y necesidades mientras está en desarrollo. |
| Sprint 7 | Seguimiento del prototipo | Ofrecer soporte mientras está en desarrollo el prototipo. |
| | | Realizar mantenimiento del prototipo para asegurar su correcto funcionamiento mientras está en desarrollo. |
| Sprint 8 | Diseño escalable | Diseñar un prototipo para que pueda ser escalable, permitiendo la adición de nuevas funcionalidades y características sin afectar el rendimiento o la eficiencia. |

3.3.4. Sprint Planning Meeting

El objetivo general del Sprint es llevar adelante en el manejo de asignaturas, profesores, estudiantes y el registro de calificaciones mediante la implementación de funcionalidades que optimicen los procesos de gestión y faciliten la obtención del registro de calificaciones, para el uso de los usuarios involucrados.

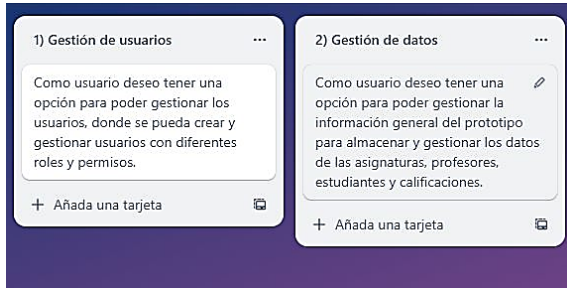


Figura 7. Product BackLog 1 y 2.

En la Figura 7, se puede ver la historia del usuario donde se crearán usuarios con distintos roles y permisos, además se puede ver la gestión de datos, quien será encargado de guardar la información general de los estudiantes, profesores, asignaturas y calificaciones.

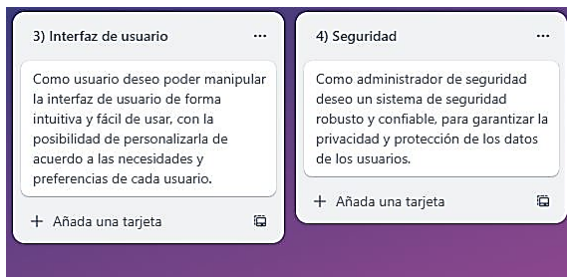


Figura 8. Product BackLog 3 y 4.

En la Figura 8, se tiene acceso a la interfaz de usuarios para poder manipular de forma intuitiva y fácil el prototipo, se ha generado las credenciales necesarias para el acceso de un rol de administrador.

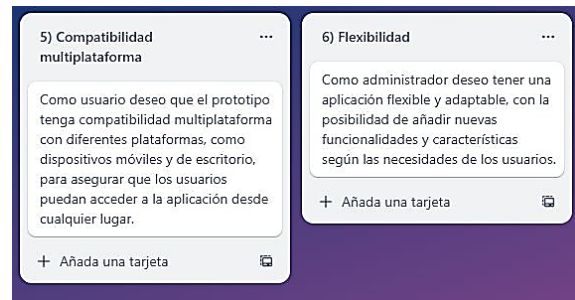


Figura 9. Product BackLog 5 y 6.

En la Figura 9, se puede ver la compatibilidad multiplataforma se ha limitado y probado con los navegadores Firefox y Chrome, quien será encargada de que el prototipo funcione.

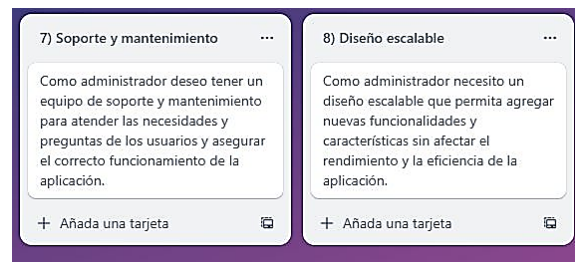


Figura 10. Product BackLog 7 y 8.

En la Figura 10, se ayudará con medidas para que sea escalable para que los usuarios o personal con conocimientos en esta tecnología puedan adaptarla.

3.3.5. Sprint Review

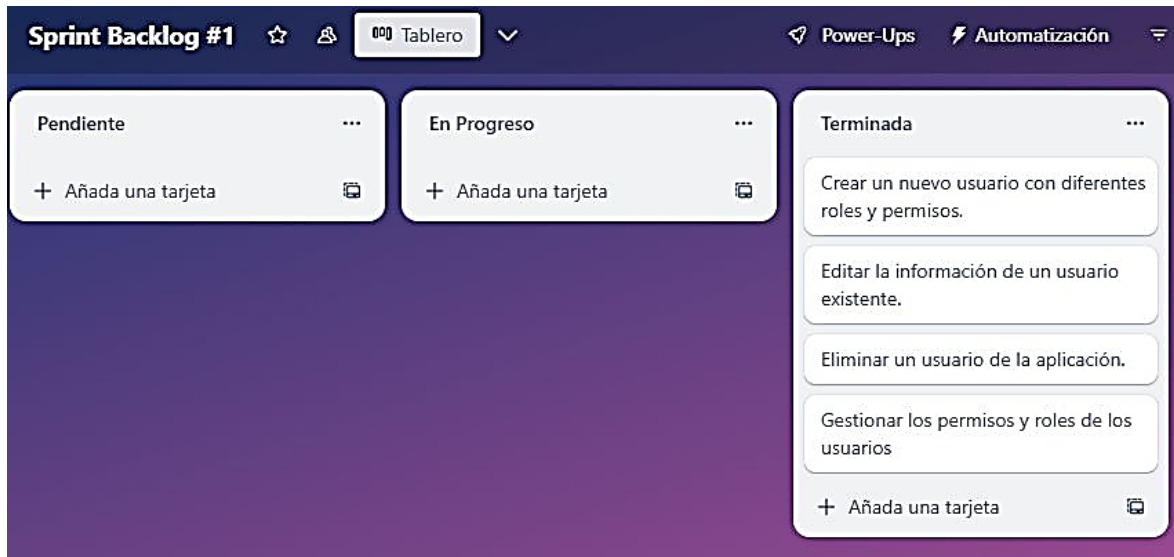


Figura 11. Gestión de usuarios - Sprint 1.

Desarrollo de la funcionalidad de usuarios, creación de los diferentes roles y permisos.

Tareas realizadas: Diseño de la interfaz de registro e inicio de sesión. Desarrollo de la funcionalidad de registro de nuevos usuarios. Implementación de la gestión de roles y permisos. Creación de las vistas y funcionalidades necesarias para la administración de usuarios.

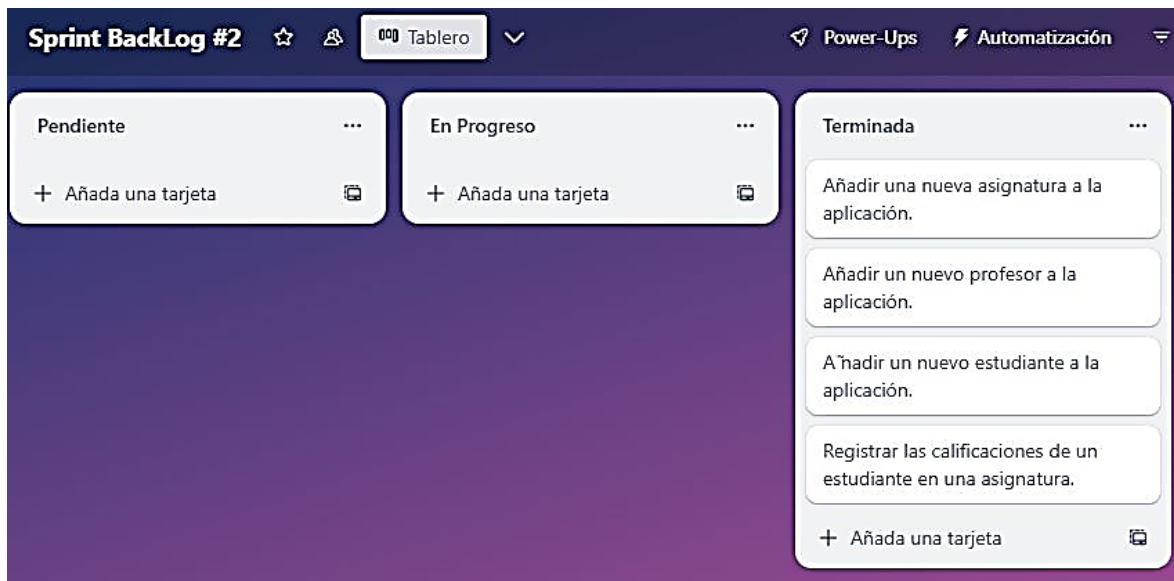


Figura 12. Gestión de datos - Sprint 2.

Almacenar y gestionar los datos de las asignaturas, profesores, estudiantes y calificaciones.

Tareas realizadas: Diseño de la estructura para guardar de forma segura la información de las asignaturas, profesores, estudiantes y calificaciones. Desarrollo de las funcionalidades de creación, lectura, actualización y eliminación (CRUD) para cada entidad. Implementación las vistas necesarias para gestionar la información de las asignaturas, profesores, estudiantes y calificaciones.

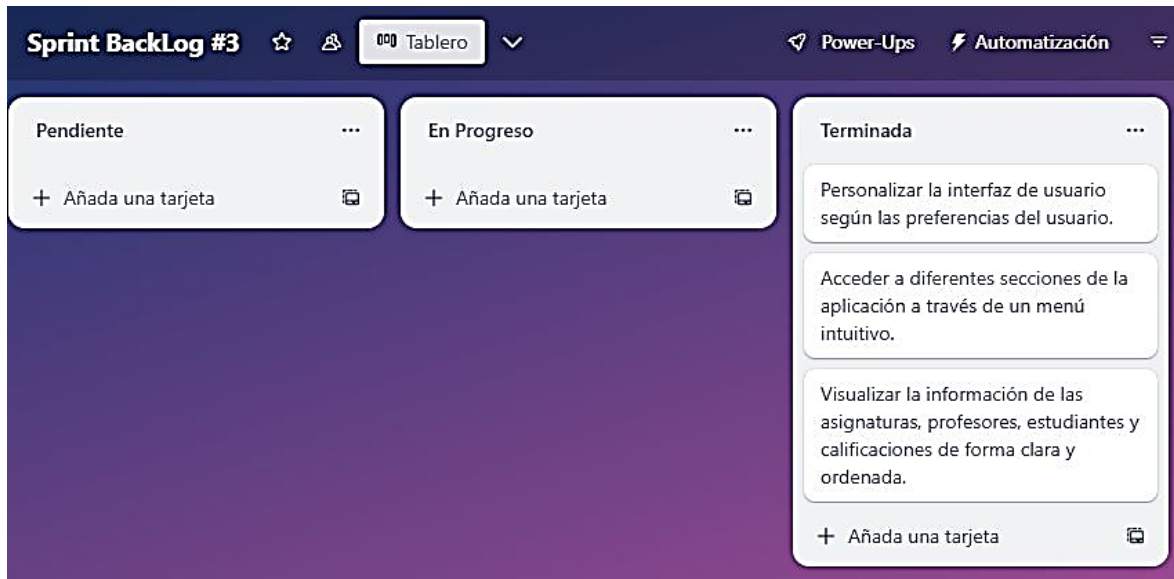


Figura 13. Interfaz de usuario - Sprint 3.

Proporcionar una interfaz intuitiva y fácil de usar, con opciones de personalización para adaptarse a las preferencias de cada usuario.

Tareas realizadas: Diseño de una interfaz de usuario con arquitectura flexible. Desarrollo de opciones de personalización, como la capacidad de cambiar los colores.

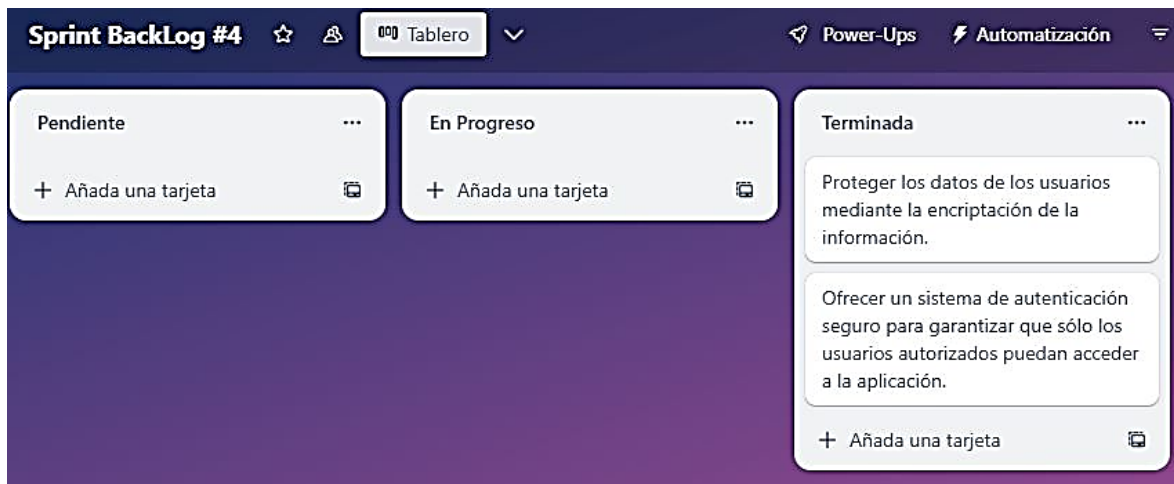


Figura 14. Seguridad - Sprint 4.

Implementación de un prototipo seguro y capaz de garantizar la privacidad y protección de la

información.

Tareas realizadas: Creación de medidas de seguridad internas como el cifrado de contraseñas.

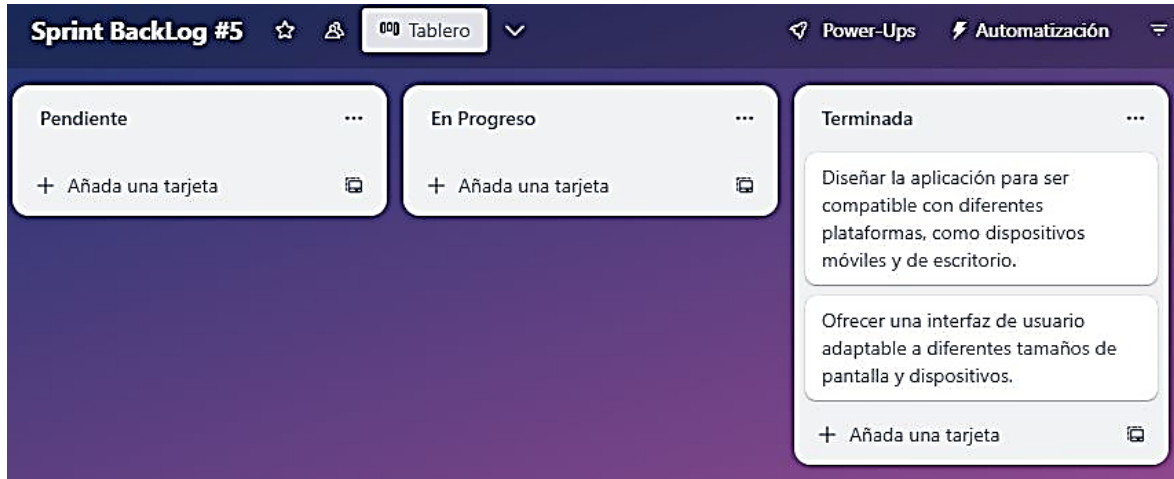


Figura 15. Compatibilidad multiplataforma - Sprint 5.

Asegurar que el prototipo sea compatible con diferentes plataformas, como dispositivos móviles y de escritorio.

Tareas realizadas: Desarrollo de una interfaz que se adapte a los navegadores, Firefox y Chrome. Manipulación del prototipo en diferentes navegadores para garantizar su funcionalidad en diferentes plataformas.

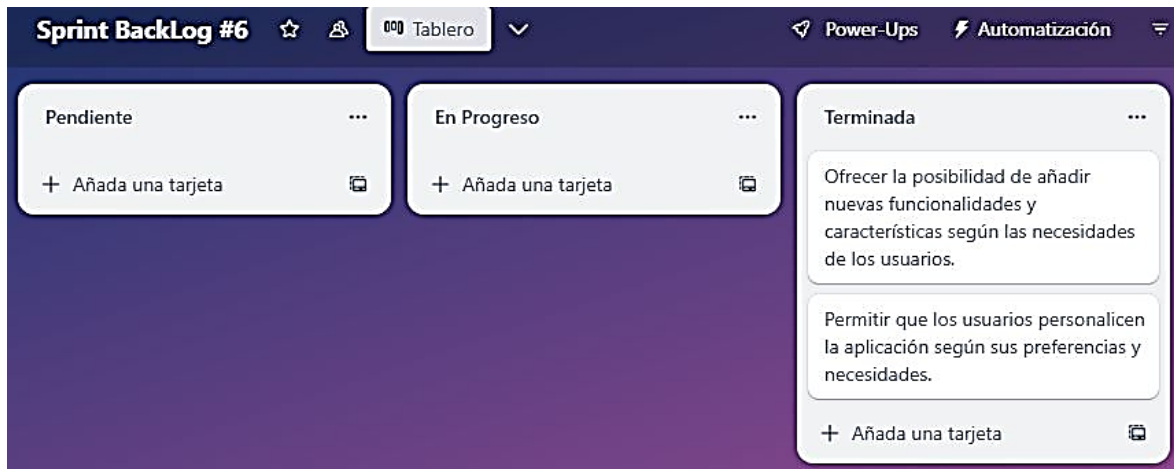


Figura 16. Flexibilidad - Sprint 6.

Permitir la adición de nuevas funcionalidades y características según las necesidades de los usuarios.

Tareas realizadas: Implementación de un prototipo con complementos o extensiones que permita añadir nuevas características sin afectar el núcleo del prototipo. Documentación de las herramientas utilizadas para que los desarrolladores puedan contribuir con nuevas funcionalidades de manera sencilla.

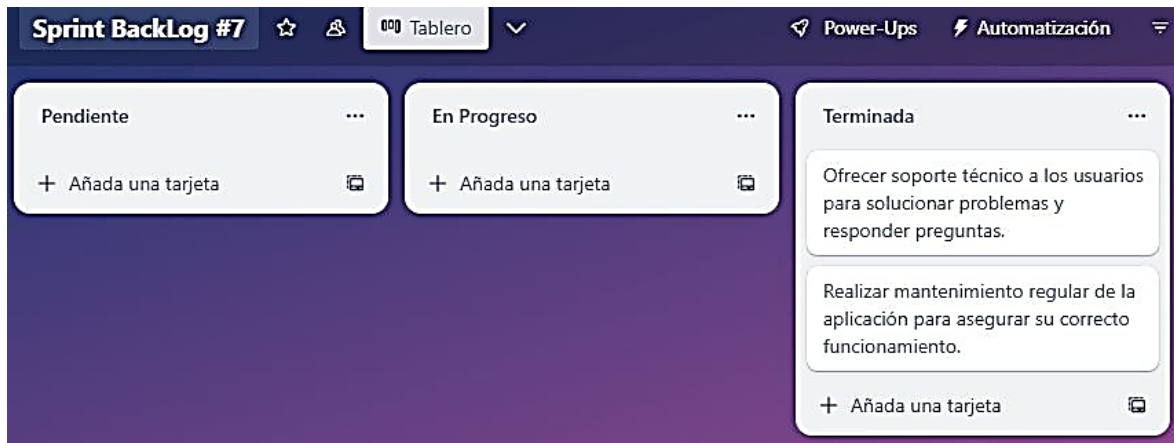


Figura 17. Seguimiento del prototipo - Sprint 7.

Atender las preguntas y asegurar el correcto funcionamiento del prototipo mientras está en desarrollo.
Tareas realizadas: Seguimiento y resolución de incidencias. Actualizaciones periódicas para corregir errores y mejorar el prototipo. Pruebas de rendimiento para garantizar la escalabilidad.

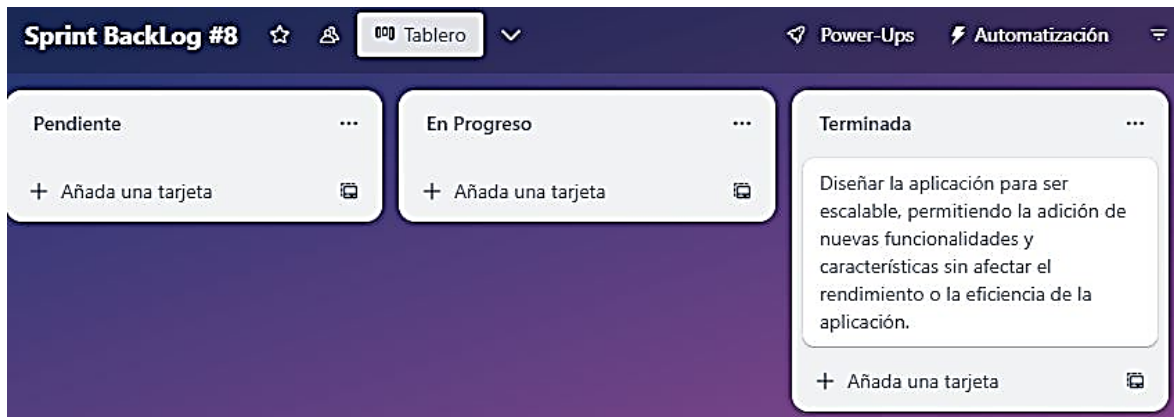


Figura 18. Diseño escalable - Sprint 8.

Diseñar un prototipo escalable que permita agregar nuevas funcionalidades y características sin afectar el rendimiento y la eficiencia.

Tareas realizadas: Es escalable por la propia naturaleza de la cadena de bloques de blockchain al incorporar un nuevo elemento en la cadena, las cadenas anteriores siguen funcionando con las nuevas funcionalidades y documentación para futuras expansiones o mejoras del mismo.

3.3.6. Sprint Retrospective

Después de llevar a cabo cada Sprint de manera minuciosa, se lograron obtener diversas mejoras en cada uno de ellos, lo que permitió fortalecer el proyecto de manera significativa:

Sprint 1: Gestión de usuarios

Lo que funcionó bien: Se logró implementar en el prototipo el registro de usuarios y la gestión de roles con sus respectivos permisos.

Lo que se puede mejorar: El proceso de inicio de sesión podría optimizarse para una experiencia más fluida.

Acciones a tomar: Investigar y aplicar técnicas de autenticación y autorización más eficientes para mejorar el proceso de inicio de sesión.

Sprint 2: Gestión de la información general del prototipo

Lo que funcionó bien: Se desarrolló un prototipo de gestión de entidades como asignaturas, profesores, estudiantes y calificaciones.

Lo que se puede mejorar: La interfaz de usuario puede ser más intuitiva y amigable para facilitar la navegación y la gestión de datos.

Acciones a tomar: Obtener feedback de los usuarios y realizar pruebas de usabilidad para identificar áreas de mejora en la interfaz de usuario y hacer ajustes según sea necesario.

Sprint 3: Personalización de la interfaz de usuario

Lo que funcionó bien: Se implementó la capacidad de personalización de la interfaz de usuario.

Lo que se puede mejorar: Las opciones de personalización pueden ampliarse para abarcar más aspectos visuales y de diseño.

Acciones a tomar: Identificar qué aspectos de la interfaz de usuario son más importantes para los usuarios y agregar más opciones de personalización en consecuencia.

Sprint 4: Seguridad

Lo que funcionó bien: Implementación de roles de usuario para poder ingresar al prototipo de acuerdo al rol del usuario.

Lo que se puede mejorar: Es necesario evaluar continuamente las vulnerabilidades y amenazas de seguridad emergentes para mantener el prototipo.

Acciones a tomar: Establecer un proceso de revisión de seguridad regular y estar al tanto de las últimas prácticas de seguridad.

Sprint 5: Compatibilidad multiplataforma

Lo que funcionó bien: El prototipo se probó y funcionó correctamente en los navegadores Firefox y Chrome.

Lo que se puede mejorar: Se deben implementar adaptaciones a los navegadores Firefox y Chrome. Acciones a tomar: Ejecutar pruebas adicionales para realizar mejoras específicas y garantizar una grata experiencia en los navegadores Firefox y Chrome.

Sprint 6: Flexibilidad

Lo que funcionó bien: Se desarrolló una arquitectura modular que permite agregar nuevas funcionalidades.

Lo que se puede mejorar: Es necesario establecer un proceso formal para evaluar y seleccionar las nuevas funcionalidades a agregar.

Acciones a tomar: Implementación para el seguimiento de funcionalidades y establecer criterios claros para su inclusión en el prototipo.

Sprint 7: Seguimiento del prototipo

Lo que funcionó bien: Se estableció un área de seguimiento del prototipo, capaz de atender las necesidades y preguntas para mejorar el prototipo.

Lo que se puede mejorar: Se pudo realizar interfaces intuitivas fáciles de utilizar.

Acciones a tomar: Implementar interfaces para garantizar una respuesta rápida y eficiente que sean amigables con el usuario final.

Sprint 8: Diseño escalable

Lo que funcionó bien: La arquitectura permite ser escalable gracias a su propia naturaleza.

Lo que se puede mejorar: Se deben establecer pautas y mejores prácticas para asegurar una fácil integración de nuevas funcionalidades.

Acciones a tomar: Documentación y mejoras para el desarrollo de nuevas funcionalidades. Además, se realizaron revisiones para agregar nuevas características.

4. Discusión y resultados

Se realizaron pruebas para validar el funcionamiento de la herramienta mediante pruebas de caja negra, para verificar el funcionamiento de la tecnología Blockchain, las interfaces de estudiantes, profesores, asignaturas y el ingreso de calificaciones, la integración entre componentes y

la seguridad del prototipo.

Gestión de usuarios

Se implementó en el prototipo, un registro de usuarios con sus respectivos roles y permisos.

La capacidad de definir diferentes roles y permisos ha brindado la flexibilidad para adaptar las necesidades del prototipo. Sin embargo, el proceso de inicio de sesión puede mejorarse para hacerlo más rápido y fluido, ya que solo es un prototipo que se basa en el funcionamiento de blockchain y no es un prototipo completo.

Gestión de la información general del prototipo

Se ha desarrollado un prototipo de gestión de asignaturas, profesores, estudiantes y calificaciones con las ventajas que ofrece blockchain. Ahora se puede almacenar y gestionar fácilmente la información utilizando las técnicas de blockchain.

Se realizaron pruebas de caja negra para obtener información de los usuarios y poder simplificar y reorganizar algunos elementos para facilitar la navegación dentro del prototipo.

Personalización de la interfaz de los usuarios

Se ha implementado una interfaz de usuario, donde cada usuario puede adaptar el prototipo según sus preferencias.

Sin embargo, las opciones de personalización podrían ser más amplias, ya que actualmente, solo se puede cambiar los colores del fondo y brindar una experiencia más personalizada a los usuarios.

Seguridad

Aquí se implementaron medidas de seguridad como la encriptación propia de la blockchain para proteger la información de los usuarios. Sin embargo, se debe ser conscientes de las amenazas de seguridad emergentes y mantener el prototipo actualizado.

Es útil establecer un proceso de revisión de seguridad regular para evaluar las vulnerabilidades y aplicar actualizaciones de seguridad según sea necesario.

Compatibilidad multiplataforma

El prototipo ha sido probado y funciona correctamente en los navegadores Firefox y Chrome.

5. Conclusiones

En conclusión, a lo largo de los diferentes sprints se lograron avances significativos en el desarrollo y mejora del prototipo. La gestión de usuarios, incluyendo el registro y una asignación de roles y permisos solo para pruebas capaces de brindar un mayor control sobre quién accede al prototipo y qué acciones se puede ejecutar.

La gestión de la información general del prototipo, incluyendo asignaturas, profesores, estudiantes y calificaciones, ha sido probado. Aunque la interfaz de usuario ha sido funcional, se ha podido identificar oportunidades para mejorar su intuitividad y facilitar la navegación. El recopilar feedback y ejecutar pruebas de usabilidad con los sprints realizados en sus distintas etapas nos ayudó a implementar cambios que mejoraron la experiencia de los usuarios.

La capacidad de personalizar la interfaz de usuario es un aspecto que no estaba dentro de nuestro proyecto. Sin embargo, se aplica esta opción de personalización para permitir un entorno amigable con el usuario.

En términos de seguridad, se ha implementado medidas como la propia encriptación por parte de Blockchain para proteger la información de los usuarios. No obstante, se debe estar atento a las amenazas emergentes.

La compatibilidad multiplataforma ha sido lograda con éxito, lo que ha permitido que los usuarios puedan acceder al prototipo desde los navegadores Firefox y Chrome capaz de obtener una experiencia óptima en dichos navegadores.

En conclusión, el desarrollo de un prototipo basado en tecnología Blockchain para la gestión educativa ofrece una solución innovadora con registros seguros sin que se pueda modificar por parte de terceros. La combinación de Ethereum, Solidity, Truffle, Ganache e IPFS permite crear una plataforma confidencial e íntegra.

6. Trabajos Futuros

Se puede investigar y aplicar técnicas de autenticación más eficientes, como la autenticación de dos factores o la integración con proveedores de identidad externos. Además, se puede implementar la opción de recordar el inicio de sesión para evitar tener que ingresar las credenciales cada vez.

Aunque el prototipo es compatible, todavía enfrenta algunos problemas específicos en dispositivos móviles como la adecuada adaptación del prototipo con cada dispositivo, que a futuro y con un poco más de investigación se podrá corregir.

Referencias

- [1] J. W. Abijaude, H. Serra, L. M. S. Santiago, P. de Lima Sobreira, K. El Guemhioui, O. A. Wahab, V. da Costa Wanderley, and F. Greve, "Introducing blockchain, smart contract and distributed application concepts and practices from an extra-curricular university training," in *2021 IEEE World Conference on Engineering Education (EDUNINE)*, 2021, pp. 1–6.
- [2] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.
- [3] R. Mars, A. Abid, S. Cheikhrouhou, and S. Kallel, "A machine learning approach for gas price prediction in ethereum blockchain," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2021, pp. 156–165.
- [4] F. Xue, H. Tian, and Y. Ge, "Teaching information management system based on blockchain technology," in *2022 International Conference on Education, Network and Information Technology (ICENIT)*, 2022, pp. 165–168.
- [5] J. P. de Brito Gonçalves, G. Spelta, R. da Silva Villaça, and R. L. Gomes, "Iot data storage on a blockchain using smart contracts and ipfs," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 508–511.
- [6] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur, and H.-N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.
- [7] —, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.
- [8] W. Q. Zheng, "Design and implementation of an intelligent education platform based on blockchain technology," in *CIBDA 2022; 3rd International Conference on Computer Information and Big Data Applications*, 2022, pp. 1–6.
- [9] V. Jurii, M. Radoevi, and E. Fuzul, "Creating students profile using blockchain technology," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2019, pp. 521–525.
- [10] J. Alanya Beltran, J. Padilla-Caballero, F. Ochoa Tataje, C. Poma Garcia, A. Perez Mendoza, and T. Sharma, "Implementation and execution of block chain technology in the field of education," in *2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART)*, 2022, pp. 748–753.
- [11] R. A. Mishra, A. Kalla, N. A. Singh, and M. Liyanage, "Implementation and analysis of blockchain based dapp for secure sharing of students' credentials," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, 2020, pp. 1–2.
- [12] R. R. Chandan, M. Lourens, K. K. Ramachandran, S. V. Akram, R. Bansal, and D. Kapila, "Implementation and execution of blockchain technology in the field of education," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 2022, pp. 1480–1485.
- [13] X. Chen, Z. Xing, B. Karki, Y. Li, and Z. Chen, "Blockchain simulation: A web application for it education," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 0486–0491.

- [14] P. Khandelwal, "Storing student records using blockchain and ipfs," in *2021 International Conference on Computational Performance Evaluation (ComPE)*, 2021, pp. 188–182.
- [15] T. N. Shankar, S. Padhy, S. Dash, M. B. Teja, and S. Yashwant, "Induction of secure data repository in blockchain over ipfs," in *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2022, pp. 738–743.
- [16] X.-d. Chen, J. Lu, M. Gong, B.-J. Guo, and Y.-p. Xu, "Design and implementation of decentralized online education platform," in *2020 5th International Conference on Mechanical, Control and Computer Engineering (ICM-CCE)*, 2020, pp. 970–974.
- [17] A. Rachmat and Albarda, "Design of distributed academic-record system based on blockchain," in *2019 International Conference on ICT for Smart Society (ICISS)*, vol. 7, 2019, pp. 1–6.
- [18] T. Cai, Z. Yang, W. Chen, Z. Zheng, and Y. Yu, "A blockchain-assisted trust access authentication system for solid," *IEEE Access*, vol. 8, pp. 71 605–71 616, 2020.
- [19] J. Zhang, R. Tian, Y. Cao, X. Yuan, Z. Yu, X. Yan, and X. Zhang, "A hybrid model for central bank digital currency based on blockchain," *IEEE Access*, vol. 9, pp. 53 589–53 601, 2021.
- [20] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li, and R. Chen, "Nutbaas: A blockchain-as-a-service platform," *IEEE Access*, vol. 7, pp. 134 422–134 433, 2019.
- [21] P. Treleaven, R. Gendal Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.
- [22] A. Srivastava, S. Bhardwaj, and S. Saraswat, "Scrum model for agile methodology," in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 864–869.
- [23] P. Rittitum, W. Vatanawood, and A. Thongtak, "Digital scrum board using leap motion," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, 2016, pp. 1–4.