TÍTULO DO TFG/TÍTULO DEL TFG: Sistema de validación de títulos académicos basado en tecnologías Blockchain

Resumo / Resumen (máximo 350 palabra):

El presente TFG ofrece una solución a la falsificación de los títulos académicos universitarios aplicando de forma integral las tecnologías descentralizadas y de registro distribuido. Gracias a la seguridad y a la privacidad que proporcionan redes blockchain como Ethereum, los expedientes se vuelven resistentes a falsificaciones o a modificaciones fraudulentas, pues cualquier cambio se valida por todos los nodos de la red y se registra de forma permanente.

En este caso, la aplicación encripta y almacena los expedientes de los estudiantes en una blockchain. Estos expedientes constan de todas las asignaturas (e idealmente todas las actividades) que conforman un grado concreto, y son los profesores los que generan las transacciones que actualizan los expedientes. En cualquier momento, los estudiantes pueden descargar y enviar a cualquier entidad interesada su expediente para que pueda ser verificado en la aplicación.

El desarrollo realizado se origina en que, a pesar de los avances en materia de verificación de documentos, la falsificación de títulos académicos sigue siendo un problema extendido y recurrente que azota incluso a los países más desarrollados. Las soluciones tecnológicas tradicionales padecen de vulnerabilidades inherentes a su diseño como la presencia de elementos centralizados en su arquitectura (introduciendo puntos únicos de fallo) o carecer de un sistema que permita detectar cualquier modificación fraudulenta. Si bien existen multitud de soluciones que consiguen verificar los documentos *per se*, esto no evita que el fraude se produzca *durante* la consecución del título. Son muchos los casos en los que un estudiante puede haber superado unos exámenes o asignaturas mediante un trato de favor; un tipo de fraude cometido hasta por dirigentes políticos de primer nivel.

Además, existen pocas soluciones a este problema que descentralicen por completo su funcionamiento. Trabajar íntegramente sobre una arquitectura descentralizada garantiza que la persistencia del sistema (información de alumnos, profesores...) sea respaldada por todos los nodos de una red P2P, lo que evita modificaciones improcedentes sobre los archivos o depender de servidores centrales. Por ello, uno de los principales objetivos del trabajo fue apoyarse en una base de datos basada en el InterPlanetary File-System (IPFS), un protocolo puramente descentralizado.

Posibles aplicacións / Posibles aplicaciones (máximo 250 palabra):

Las redes blockchain popularizaron el uso de smart contracts (contratos inteligentes), unos programas que se ejecutan cuando se alcanzan ciertas condiciones. Su uso permite simplificar enormemente los trámites burocráticos. Por ejemplo, podrían automatizar las matriculaciones de los alumnos al cumplirse el pago de las asignaturas, o llevar a cabo la certificación de los títulos tras haberse alcanzado los créditos requeridos para un grado concreto.

Como cada actividad que se refleja en la aplicación queda protegida ante falsificaciones, el objetivo es registrar el mayor número de hitos que se dan durante el grado. Por ejemplo, se podría reflejar la realización de prácticas en empresas, o llevar un registro efectivo de las diferentes entregas de trabajos o prácticas que se generan a lo largo de un curso.

Por otro lado, si se adaptara la funcionalidad de las criptomonedas como créditos académicos (ECTS), la acreditación del expediente de un alumno se llevaría a cabo simplemente comprobando la cantidad de créditos acumulados en su cartera. Además, podría permitir la exportación de expedientes entre diferentes universidades del ámbito europeo.

Incluso, cabe la posibilidad de que otras entidades emisoras de títulos formasen parte de la aplicación, sin ser necesariamente del ámbito educativo. De esta manera, se podría llegar a proteger un Currículum Vitae completo, pues méritos extra-universitarios como cursos de idiomas u otras capacitaciones serían completamente compatibles y verificables en el sistema.

Etapas para o seu desenvolvemento futuro / Etapas para su desarrollo futuro (máximo 250 palabras):

Al hacer uso de tecnologías relativamente novedosas, se presentan retos que no se dan en los sistemas tradicionales. Así, para garantizar sus ventajas, se requerirá de un análisis exhaustivo y de un personal cualificado en la materia. Además, las decisiones de diseño marcarán la diferencia en cuanto a presupuesto y alcance.

Por un lado, de cara a su implantación en el sistema público educativo, sería necesario repensar qué tipo de blockchain es más adecuada dependiendo del tipo de aplicación y sus necesidades. Las redes públicas otorgan gran seguridad y transparencia por el número de nodos presente en la red, pero su consumo de energía es muy elevado y estaríamos sujetos a la volatilidad de la red en cuestiones de comisiones.

Igualmente, un despliegue masivo requeriría re-diseñar y re-implementar el sistema de almacenamiento descentralizado desde el principio para adecuarlo a las necesidades de persistencia a gran escala. Además, el protocolo IPFS no proporciona privacidad por defecto, lo cual es; un aspecto capital en sistemas de este tipo donde se maneja una gran cantidad información sensible. Por tanto, habría que implementar una capa que protegiera la privacidad de los datos de los usuarios.

Tampoco sería lo mismo plantear esta aplicación como un sistema de verificación universal que pudiera dar cabida a todas las universidades del entorno europeo, que limitar su uso a un ámbito nacional. Las exigencias técnicas según el alcance de la aplicación podrían ser muy distintas y sería necesario adaptar el sistema a ello.

Imaxes representativas / Imágenes representativas (máximo 2):