Storage of Educational Certificates Based on Blockchain Technology

Igor Ivanov, Ph.D.[1], Jesennia Cárdenas Cobo, MSc[2], Svetlana Zhdanova, MSc[3] and Artem Teliatitskiy, MSc[4]
[1]Universidad Tecnológica Empresarial de Guayaquil, Ecuador, i.v.ivanov1960@gmail.com,
[2]Universidad Estatal de Milagro, Ecuador, jcardenasc@unemi.edu.ec,
[3]Universidad Estatal Tecnológica de Belgorod, Rusia, umcitoo@yandex.ru,
[4]SofTrust Ltd., Rusia, snegirevnews@gmail.com

Abstract– ***The study shows the importance of creating a reliable storage system for electronic documents in the field of education. To this end, the general characteristics of the key methods of protection against counterfeiting in the field of education were analysed. An example is given of a prototype of the EDBlock information system developed by an international group of researchers. The basis of the system is blockchain technology. EDBlock can be applied in a number of educational institutions to ensure the security and legality of documents. Using the IDEF methodology, the basic information flows in the system are studied. The functional blocks of the developed prototype are highlighted and described. An algorithm is proposed to validate a transaction in a socially oriented system by voting for participants who do not have equal rights.***

Key words: ***Long Life Learning concept, blockchain, educational ecosystem, reliable data storage, trust protocol, social trust motivation.***

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2020.1.1.483
ISBN: 978-958-52071-4-1 ISSN: 2414-6390

18th LACCEI International Multi-Conference for Engineering, Education, and Technology: "Engineering, Integration, and Alliances for a Sustainable Development" "Hemispheric Cooperation for Competitiveness and Prosperity on a Knowledge-Based Economy", July 27-31, 2020, Virtual Edition.

Almacenamiento de los Certificados Educativos Basado en la Tecnología Blockchain

Igor Ivanov, Ph.D.[1], Jesennia Cárdenas Cobo, MSc[2], Svetlana Zhdanova, MSc[3] and Artem Teliatitskiy, MSc[4]
[1]Universidad Tecnológica Empresarial de Guayaquil, Ecuador, i.v.ivanov1960@gmail.com,
[2]Universidad Estatal de Milagro, Ecuador, jcardenasc@unemi.edu.ec,
[3]Universidad Estatal Tecnológica de Belgorod, Rusia, umcitoo@yandex.ru,
[4]SofTrust Ltd., Rusia, snegirevnews@gmail.com

Resume – El estudio muestra la importancia de crear un sistema de almacenamiento confiable de documentos electrónicos en esfera de la educación, para lo cual se analizaron las características generales de los métodos clave de protección contra las falsificaciones en el campo de la educación. Se presenta el ejemplo de un prototipo del sistema de información EDUBlock, desarrollado por un grupo internacional de investigadores. La base del sistema es tecnología blockchain. EDUBlock se puede aplicar en un conjunto de instituciones educativas para garantizar la seguridad y legalidad de los documentos. Utilizando la metodología IDEF se estudian los flujos básicos de información en el sistema. Se describen y destacan los bloques funcionales del prototipo desarrollado. Además se propone un algoritmo para validar una transacción en un sistema con orientación social, mediante la votación de los participantes que no tienen los derechos iguales.

Palabras clave – almacén confiable de datos, concepto de Long Life Learning, ecosistema educativo de blockchain, motivación de confianza social, protocolo de confianza.

Abstract - The study shows the importance of creating a reliable storage system for electronic documents in the field of education, for which the general characteristics of the key methods of protection against counterfeiting in the field of education were analysed. The example of a prototype of the information system EDUBlock, developed by an international group of researchers, is presented. The basis of the system is blockchain technology. EDUBlock can be applied in a number of educational institutions to ensure the security and legality of documents. Using the IDEF methodology, the basic information flows in the system are studied. The functional blocks of the developed prototype are described and highlighted. In addition, an algorithm is proposed to validate a transaction in a socially oriented system by voting for participants who do not have equal rights.

Keywords - blockchain educational ecosystem, Long Life Learning concept, reliable data storage, social trust motivation, trust protocol.

I. Introducción

En nuestro mundo que cambia rápidamente, el aspecto de la educación y la formación de especialistas demandados en el mercado laboral se está convirtiendo en un problema muy grave. Debido al rápido salto en el desarrollo de las tecnologías de telecomunicaciones, una gran audiencia de estudiantes tiene nuevas oportunidades para mejorar su profesionalismo. El e-learning se ha convertido en una de las principales innovaciones que se difunden cada vez más en las instituciones de educación superior. El objetivo principal de la adopción del e-learning en las instituciones de educación superior es incrementar la accesibilidad al proceso educativo sin restricciones de lugar y tiempo, además mejorar sustancialmente la calidad y el contenido de la educación. E-learning se refiere al uso de medios electrónicos y tecnología educativa, también las TIC como Internet, correo electrónico y computadoras en el proceso educativo [1].

El sistema educativo moderno tiene como objetivo principal crear un entorno libre y cómodo para que las personas se desarrollen. Un entorno en el que el propio alumno pueda determinar el tiempo, el ritmo de la capacitación y la forma del conocimiento. La ubicación de la institución de capacitación deja de ser importante, lo principal es la disponibilidad de acceso a los recursos de Internet. Este concepto conduce a la formación humana de un nuevo tipo – "homo faber", es decir el hombre que hace y fabrica o, en un aspecto más amplio, una persona que actúa, que ocupa una posición de vida activa en el mundo moderno.

La siguiente tendencia de nuestro tiempo es Long Life Learning: el aprendizaje de toda la vida. Para el crecimiento profesional, se vuelve prestigioso y útil de tener varios documentos educativos de varios niveles y carreras. Los trabajadores recogen sus carteras, acumulando certificados de aprobación de pruebas profesionales, cursos, escuelas y otros tipos de capacitación. Todo esto influye en que la persona activa tiene muchos documentos de educación y capacitación. Para la creciente demanda de formación asequible, aparece una oferta correspondiente en forma de sitios educativos globales en línea como COURSERA, EdX y Udacity. Si bien crean un gran valor para los consumidores, un resultado es que los datos se están convirtiendo en una nueva clase de activos, una que puede superar a las clases de activos anteriores [2]. La cartera de e-learning es una colección a través de la cual el alumno, en el entorno de tecnología de la información, aplica medios de información para representar y mostrar objetivos de aprendizaje, actividades de aprendizaje, logros de aprendizaje, rendimiento de aprendizaje, esfuerzos para aprender, progreso de los estudios e introspección del proceso de aprendizaje y resultado, que incluye principalmente trabajos de aprendizaje, participación en el aprendizaje, selección de aprendizaje, estrategia de aprendizaje e introspección de aprendizaje, etc [3].

Sin embargo, con las ventajas obvias del aprendizaje electrónico, deben destacarse las siguientes dificultades en su implementación. En primer lugar, la institución educativa debe tener confirmación de que el participante del curso a distancia y la persona que solicita un certificado educativo son la misma

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2020.1.1.483
ISBN: 978-958-52071-4-1 ISSN: 2414-6390

persona. En segundo lugar, cada año aumenta el número de documentos educativos ilegales. El verano de 2018 The Guardian publicó un artículo en el que un servicio oficial de verificación de títulos en el Reino Unido (HDD) instó a los nuevos graduados que se toman selfies con sus nuevos diplomas a no compartir imágenes en las redes sociales para evitar alimentar el comercio multimillonario de documentos educativos falsos [4]. Cuando los solicitantes chinos ingresan a las universidades estadounidenses, se estima que el 90% de las cartas de recomendación son falsas, el 70% de los ensayos no son trabajos de estudiantes y el 50% de las transcripciones son falsificadas [5]. Tercero, cuando se mudan a otro estado o en busca de trabajo en el extranjero, un diploma de formación debe ser reconocido como un diploma en general, y también comparable con los estándares de capacitación del país anfitrión. Para legalizar diplomas extranjeros, hay una serie de organizaciones intermediarias que realizan una evaluación. La empresa intermediaria se ocupa de la cuestión de la autenticidad del certificado educativo y emite un certificado que indica el equivalente.

Eliminar y combatir estas deficiencias es un problema mundial. Se han realizado esfuerzos significativos en toda Europa para identificar documentos falsos. Recientemente, el proyecto FRAUDOC ha emitido directrices sobre falsificación de documentos educativos y fraude de documentos para evaluadores de credenciales. Las guías proporcionan una visión general de este fenómeno, así como herramientas y recomendaciones para detectar falsificaciones. En la Federación de Rusia, para combatir los documentos educativos fraudulentos, se aprobó un decreto del Gobierno de Rusia de agosto de 2013, "Sobre el Sistema Federal de Información, Registro Federal de Información de Documentos Educativos y (o) Documentos de Capacitación y Calificación" [6]. Este documento implica la implantación del sistema de información "Contingente", que acumularía diplomas y certificados electrónicos de un ciudadano. La República del Ecuador cuenta con la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT), cuyas funciones son mantener un registro de documentos educativos, incluida su verificación y aprobación [7].

II. Desarrollo

A. Posibilidad de utilizar el registro distribuido, para el almacenamiento de documentos.

De lo anterior, se deduce que existe una urgente necesidad global de crear una tecnología para resolver el problema de la falta de confianza y que proporcione un almacenamiento confiable y seguro de datos electrónicos. En nuestra opinión, dicha tecnología puede ser una tecnología de información multifuncional y multinivel llamada registro distribuido.

La tecnología de los registros distribuidos es un enfoque para el intercambio y el almacenamiento de información, que tiene ventajas innegables como poseer una copia completa del registro, sincronización de datos en línea, acceso instantáneo al historial de transacciones [8].

La razón principal del mayor interés es la expectativa de que esta tecnología eliminará los problemas y limitaciones existentes, inherentes a los métodos modernos de almacenamiento, contabilidad y transmisión de información. La tecnología de los registros distribuidos incluye un concepto como blockchain.

Un blockchain es un mecanismo de almacenamiento diseñado para mantener un registro de las transacciones que ocurren entre dos partes de manera permanente y verificable. Blockchain también es un mecanismo “peer-to-peer” abierto y distribuido de almacenamiento de datos [9]. Cada bloque apunta al bloque inmediatamente anterior a través de una referencia que es esencialmente un valor hash del bloque anterior (bloque padre) y se calcula mediante la función de hash. Función de hashes o funciones resumen - una función que convierte un conjunto de datos de entrada en una cadena de bits de salida de una longitud determinada, realizada por un algoritmo específico. El resultado de la conversión (cadena de salida) se denomina "hash". Vale la pena señalar que los hashes de tío blocks (hijos de los antepasados del bloque) también se almacenarían en ethereum blockchain. El primer bloque de una cadena de bloques se llama bloque de génesis que no tiene bloque primario [10]. Cada bloque, excepto el primario, tiene un enlace a información del bloque anterior. Los bloques en sí, así como los datos dentro de ellos, están protegidos por encadenamiento. Cada entrada contiene un enlace a una entrada fuente anterior, así como una condición de bloqueo y una regla de desbloqueo. Para describir las reglas y condiciones, se utiliza un lenguaje de programación que le permite establecer una lógica compleja y reglas para la interacción de los participantes. Puede ser varias fuentes y resultados en cada registro, es decir, un registro puede convertir varios registros de fuente a varios registros de resultados. Por lo tanto, la cadena de bloques nos lleva a contratos "inteligentes" que nos permiten formalizar las relaciones no solo entre las personas, sino también entre una persona y los programas. Como tal, blockchain tiene el potencial de crear confianza entre actores independientes y no familiares que tienen derecho a colaborar sin requerir ningún tipo de autoridad central [11].

La construcción de una cadena común se basa en el “árbol hash de Merkle”. El árbol de Merkle es una estructura de datos. Su estructura no es muy diferente de la estructura de datos usual en forma de árbol. La base es el cálculo del hash de datos basado en los hashes de todos los nodos secundarios. La raíz de árbol se escribe en el encabezado del bloque, lo que hace que sea imposible eliminar o reemplazar bloques de transacción. Siempre que los encabezados de los bloques estén protegidos adecuadamente de los cambios, para reemplazar un bloque, el atacante deberá reemplazar todos los bloques posteriores en la cadena de bloques. De este modo, un sistema adecuado para proteger los encabezados de bloque hace que sea imposible eliminar las transacciones de la cadena de bloques las registradas en él hace relativamente tiempo; por lo

tanto, la cadena de bloques satisface la condición de finitud de las transacciones [12].

La estructura de cada bloque de transacción es la misma y consta de las siguientes partes [13]:

1) versión del bloque;

2) hash del bloque anterior (bloque padre);

3) hash de todas las transacciones en el bloque;

4) fecha y hora en que se creó el bloque;

5) target, es decir enlace al objetivo de hash actual en la lista;

6) un campo de 4 bytes que aumenta su valor después de cada transacción o cálculo consecutivo.

La estructura del bloque, no es necesario almacenar el documento en sí. Resulta que los datos permanecen en posesión del usuario, y solo el valor hash del documento específico ingresa al sistema distribuido. Manteniendo su clave privada en secreto, el usuario siempre puede recrear el valor hash del documento que se está comprobando. La coincidencia del valor obtenido con el hash especificado en la transacción válida, determina la autenticidad del documento unívocamente.

La seguridad de las bases de datos tradicionales como MySQL y MongoDB, está garantizada por un control de datos centralizado, que es responsabilidad del operador del sistema. El hecho de que las funciones de gestión se asignen a humanos hace que las bases de datos convencionales sean vulnerables. Un ejemplo es el hecho de comprometer la base de datos biométricos de la agencia India UIDAI [14].

Los errores y las acciones maliciosas de los empleados están costando cada vez más a las empresas que procesan grandes cantidades de datos y a la sociedad. El mercado para analizar grandes datos de usuarios está creciendo y con esto está creciendo el número de mensajes sobre el compromiso de cientos de millones de registros de usuarios. En junio de 2018, el investigador de seguridad Vinny Troia descubrió que Exactis, un corredor de datos con sede en Palm Coast, Florida, había expuesto una base de datos que contenía cerca de 340 millones de registros individuales en un servidor de acceso público. "Parece que esta es una base de datos con casi todos los ciudadanos estadounidenses", dice Troia [9].

El protocolo blockchain y su estructura, que se basan en el almacenamiento seguro de datos, crean un sistema de registro automatizado que forma un sistema interconectado y combate las amenazas emergentes. Los contratos inteligentes son métodos sin precedentes para garantizar el cumplimiento contractual, incluidos los contratos sociales. "Si tienes una gran transacción con una estructura de control específica, puedes predecir el resultado en cualquier momento", dicen Tapscotts [2]. "Si tengo una transacción firmada totalmente verificada con un número de firmas en una cuenta de firmas múltiples, puedo predecir si esa transacción será verificable por la red. Y si es verificable por la red, entonces esa transacción puede ser redimida y de manera irrevocable.
Ninguna autoridad central o tercero puede revocarla, nadie puede anular el consenso de la red. Es un concepto nuevo tanto en el derecho como en las finanzas. El sistema bitcoin proporciona un grado muy alto de certeza en cuanto al resultado de un contrato" [2].

La combinación de contratos inteligentes, así como la idea de la tecnología blockchain le permitirán organizar un sistema para almacenar información sobre todos los certificados y diplomas recibidos por una persona. Las ventajas proporcionadas por la combinación de estos métodos resolverán los problemas de un repositorio de documentos electrónicos asequible, confiable y al mismo tiempo abierto.

La tecnología Blockchain ofrece los siguientes cinco beneficios [9]:

1. Eficiencia: Blockchain se puede administrar fácilmente y puede rastrear registros de datos complejos.

2. Seguridad: la seguridad proporcionada por una cadena de bloques es mejor que la de una administración de datos centralizada. En último caso hay el riesgo de sufrir daños debido a la intrusión de hackers. En blockchain, falsificar datos es casi imposible debido al control simultáneo de los dispositivos donde se almacenan los datos, como los dispositivos móviles. Además, el hacker necesita cambiar todos los datos almacenados en los dispositivos para falsificarlos.

3. Resiliencia: toda la información en blockchain no se almacena en un lugar en comparación con una gestión de datos centralizada, sino la información se distribuye por igual entre los dispositivos móviles que interactúan. No existe un único punto de fallo. Incluso si varios dispositivos encuentran errores o degradación del rendimiento, la posibilidad de que una infraestructura encuentre amenazas maliciosas de blockchain es escasa. Incluso si es atacado, puede recuperarse fácilmente.

4. Transparencia: todos los datos de uso y el estado de los recursos están abiertos de forma predeterminada porque los metadatos de los recursos se comparten entre todos los dispositivos participantes.

5. Seguridad: Blockchain está asegurado mediante la distribución de datos entre muchas computadoras entrelazadas. Más del 50% de los sistemas dentro de la red vulnerables a cualquier piratería fracasan. Mediante el uso de una función hash, se crea una cadena de datos en bloque para construir el libro mayor que contiene todos los historiales de transacciones.

Por lo tanto, el uso de la tecnología blockchain conduce a la aparición de activos inteligentes. Al regular el trabajo de este concepto a través de la tecnología blockchain de acuerdo con la ley aplicable, es posible implementar una alcancía electrónica global de documentos educativos, donde la autenticidad se basa en la existencia del sistema descentralizado en sí. La nueva Estrategia Europa 2020, una estrategia para un crecimiento inteligente, sostenible e integrador, mantiene como objetivo claro salir de la crisis y preparar a la economía de la UE para los retos de la próxima década. La Agenda Digital para Europa, enmarcada dentro de la Estrategia, pretende obtener los beneficios económicos y

sociales sostenibles que pueden derivar de un mercado único digital en una Internet rápida y ultrarrápida y más aplicaciones interoperables [15].

Actualmente, algunas universidades e institutos usan la tecnología blockchain en la educación, y la mayoría de ellos usan esta tecnología para administrar su título académico y la evaluación general de los resultados del aprendizaje. La Universidad de Nicosia es la primera escuela en utilizar la tecnología blockchain para administrar los certificados de estudiantes recibidos de las plataformas MOOC [16]. Sony Global Education también ha utilizado la tecnología blockchain para crear una plataforma de evaluación global para proporcionar servicios de almacenamiento y administrar la información del título. El Instituto Tecnológico de Massachusetts (MIT) también emite títulos académicos electrónicos. Los estudiantes que participaron en proyectos de MIT Media Lab y que aprobaron la evaluación recibirán un certificado que se almacenará en la red blockchain [17]. Otro proyecto interesante en este campo es el desarrollo de compaña BlockTac. El sistema basado en blockchain está orientado y funciona con universidades, escuelas de negocios, asociaciones profesionales en España, así como con instituciones educativas internacionales en Europa y América Latina. [18]. Las instituciones educativas y los estudiantes concuerdan sus certificados en el sistema. Después, el estudiante puede estudiar en cualquier otra institución educativa y compartir su certificado, cuya legalidad se puede verificar directamente en el sistema, sin contactar a la institución que lo emitió.

B. Prototipo del sistema del almacenamiento seguro.

Por lo visto, el desarrollo e implementación de sistemas basados en tecnología de registro distribuido es una tarea urgente y solicitada en todo el mundo. Sin embargo, debe tenerse en cuenta que las implementaciones arquitectónicas y de software y sus descripciones detalladas son casi imposibles de encontrar. Además, vale la pena señalar el hecho de que los sistemas existentes no satisfacen completamente los requisitos de un usuario en particular. Requieren un refinamiento inmediato para las tareas de la organización. Para resolver estos problemas se requería el desarrollo del sistema de información EDUBlock, en cuyo proyecto trabajó un grupo internacional de investigadores e ingenieros.

B.1. La arquitectura del sistema de almacenamiento seguro.

Para diseñar el modelo de dominio, se utilizó un enfoque funcional basado en la metodología IDEF0. El diagrama de contexto IDEF0 refleja una descripción general de las actividades del sistema de información EDUBlock.

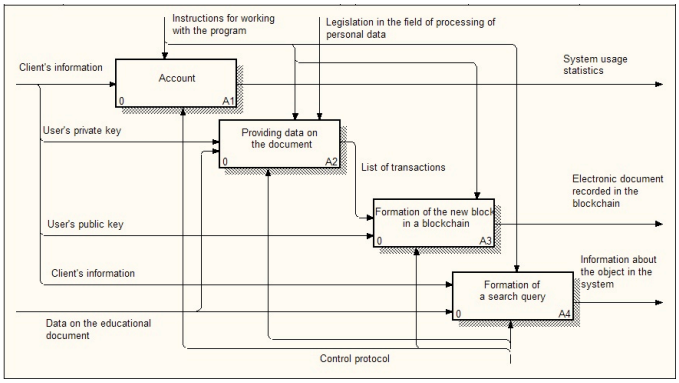

Fig. 1 El diagrama del contexto del sistema EDUBlock.

Los datos de entrada son datos sobre clientes, datos sobre documentos que se refieren a educación. La salida está representada por una entrada en la cadena de blockchain, que es una versión electrónica del documento, estadísticas sobre el uso del sistema, los resultados de una consulta de búsqueda. Una siguiente descomposición nos permite determinar los principales tipos de trabajo que ocurren en el sistema.

Según el diagrama en Fig. 1, todo el sistema está compuesto por cuatro bloques.

Los datos de todos los usuarios del sistema se envían a la entrada del primer bloque. En la salida, recibimos una solicitud para proporcionar datos en un documento sobre educación o estadísticas sobre el uso del sistema.

En el segundo bloque, se crea una nueva transacción que contiene información sobre el documento transmitido, así como los datos del usuario que forma esta transacción.

En el tercer bloque, se forma un nuevo elemento de bloque de la cadena blockchain, que contiene todas las transacciones creadas en el paso anterior.

En el cuarto bloque, en función de la información enviada sobre el documento, se genera una solicitud de búsqueda. Como resultado de la solicitud de búsqueda, el usuario recibe información sobre el documento en el sistema, si existera.

Con base a los flujos de información anteriores, se identificaron los siguientes subsistemas (módulos) como parte del sistema de información: módulo criptográfico, módulo de interacción entre redes, módulo blockchain y aplicación que proporciona una forma conveniente de interacción con el sistema.

El módulo criptográfico debería poder generar claves criptográficas basadas en el estándar RSA-2048. Las claves públicas y privadas están interconectadas por comunicación unidireccional. Un resumen de los datos personales obtenidos por el algoritmo SHA-512 y la clave privada del usuario genera una firma de transacción.

El módulo de interfuncionamiento se basa en la tecnología P2P. La tecnología punto a punto difiere de los enfoques estándares de escalado de infraestructura de red. Cuando se aplica el enfoque de "igual a igual", lo principal no es la comunicación entre el cliente-servidor, sino los métodos

de búsqueda de otros clientes en la red, por los cuales pueden intercambiar información entre ellos.

El módulo de control (Blockchain) se utiliza para crear transacciones, bloques transaccionales y de autorización. Además, este módulo describe algoritmos para verificar la información recibida, verificar la cadena de datos local, almacenar datos en la cadena local y un protocolo de confirmación.

B.2. La estructura de transacción.

Las siguientes estructuras de transacciones y bloques se han desarrollado e implementado para el sistema de información EDUBlock. Un bloque en una cadena de bloques consiste en un encabezado y un cuerpo. El cuerpo del bloque de documentos es una descripción del número de transacciones incluidas en él y las transacciones mismas. El encabezado del bloque contiene información específica que se requiere para mantener la ideología de esta tecnología.

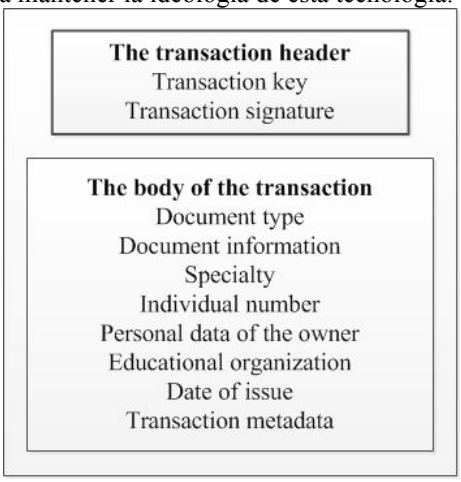

Fig. 2 La estructura de la transacción del sistema EDUBlock.

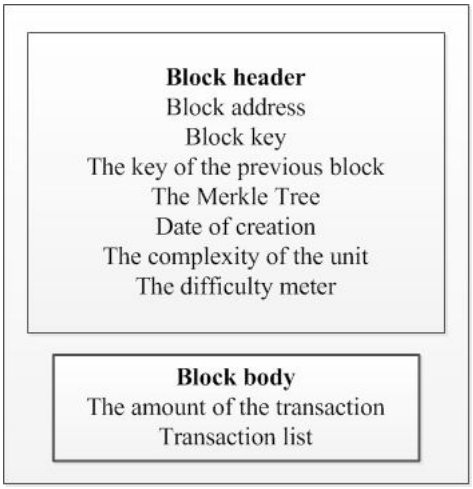

Fig. 3 La estructura del bloque del sistema EDUBlock.

La arquitectura del sistema se basa en la tecnología de registro distribuido. Un registro distribuido es una base de datos de información que se distribuye a través de una red de computadoras, servidores o sitios web. Esta tecnología no tiene una ubicación geográfica o administrativa. Todos los usuarios de la red, sin excepción, mantienen una copia idéntica y completa de todos los registros. La modificación del registro dará como resultado cambios de copia para todos los participantes de la red en un corto período de tiempo. Cualquier activo puede ser una entrada en un registro distribuido. La supervisión sobre la veracidad y la seguridad de las entradas del registro se mantiene a través de firmas y claves basadas en algoritmos criptográficos que permiten controlar el acceso al registro.

Como usuarios del sistema, ambas organizaciones realizan actividades educativas, así como usuarios comunes y corrientes. Cualquiera de los tipos de usuarios enumerados puede conectarse al sistema y proporcionar una lista de documentos educativos emitidos.

El hash raíz es la suma de todos los hashes emitidos para la sesión actual. Los hashes de un número ilimitado de usuarios se colocan en un bloque. La restricción es solo el tamaño del bloque, que en este sistema es de 500 kb, con la capacidad de acomodar hasta 130 transacciones.

El usuario del sistema, al completar una solicitud de confirmación de la autenticidad del documento emitido, crea una solicitud de búsqueda. La búsqueda se implementa de acuerdo con el algoritmo de árbol de búsqueda binario aleatorio, ya que al crear el árbol Merkle, el hash del valor viene en orden aleatorio.

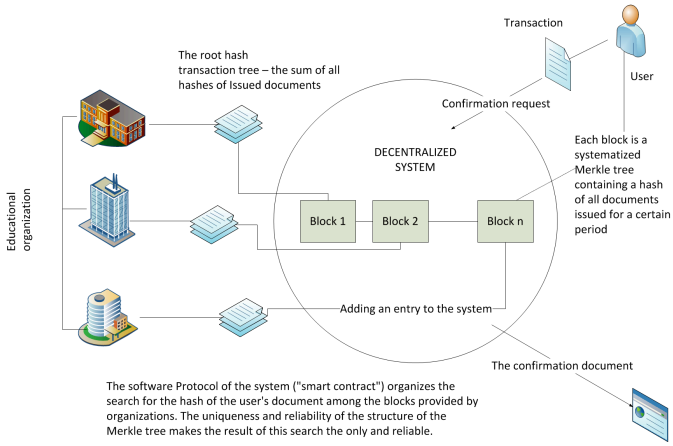

Fig. 4 El esquema de Contracto inteligente del sistema EDUBlock.

Al registrarse en el sistema, el usuario recibe un par de claves: públicas y privadas. La clave pública junto con otra información de registro se registra en la cadena de bloques, pero en una "rama de arbol" separada que no sea aquella en la que se escriben los bloques con datos del documento. En la próxima autorización, el programa le pedirá al usuario que descargue un archivo que contenga un par de claves. Según el algoritmo del protocolo de software, así como los datos

almacenados en la cadena de bloques, se decide la cuestión de otorgar o denegar el acceso a su cuenta personal.
La clave pública también se usa como la dirección del bloque, lo que nos permite unívocamente identificar al usuario que lo ha creado.

El proceso de entrada de datos, que combina transacciones confirmadas en bloques, la búsqueda de datos se realiza mediante la lógica del protocolo de software.

B.3. La interfaz del sistema.

La barra de navegación contiene el logotipo de la aplicación, así como elementos de menú.

El espacio principal contiene varias formas de entrada de información, tablas y áreas de salida de información. El espacio de trabajo se puede dividir en secciones, depende de qué elemento del menú esté seleccionado actualmente.

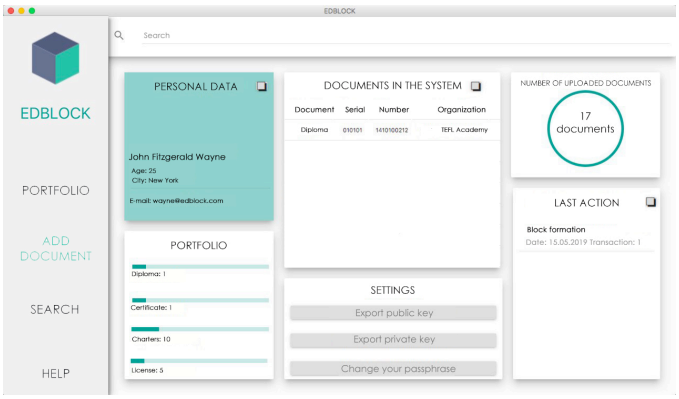

Fig. 5 El proceso de agregar un documento.

Consideremos en detalle la operación "Agregar un nuevo documento" (Fig. 5).

Esta operación se realiza en dos etapas: 1) agregar un documento; 2) la formación de un bloque con datos.

En la primera etapa, el usuario completa un formulario de envío de documentos.

El usuario puede colocar los datos sobre el documento manualmente utilizando el formulario de envío del documento y arrastrar un archivo que representa una versión electrónica del documento al respaldo pdf, y los datos pasarán automáticamente, si es posible, del documento al formulario.

Después de completar el formulario y de tener en cuenta todos los campos obligatorios, el usuario, al hacer clic en el botón "Add document", acumula los datos ingresados en el búfer intermedio. En la tabla "Current transactions" aparece un nuevo registro del documento archivado.

Para cambiar los datos sobre un documento ya enviado, el usuario solo necesita hacer clic en la línea correspondiente en la tabla " Current transactions"

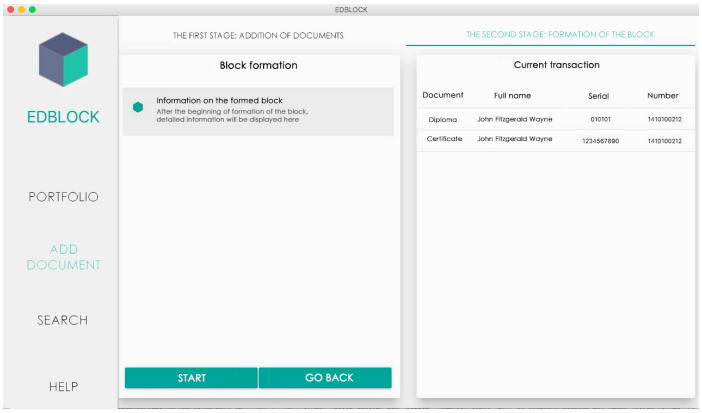

Fig. 6 El proceso de validación del documento.

Después de ingresar los datos de todos los documentos, puede pasar a la segunda etapa de archivo de documentos.

En esta etapa, el usuario puede comenzar a formar un bloque o volver a la primera etapa para realizar cambios adicionales en los documentos descargados.

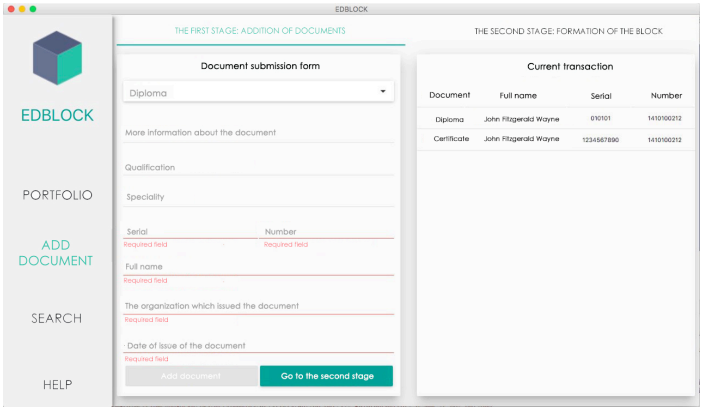

Fig. 7 El proceso de formar del bloque.

Al comienzo de la formación del bloque, el usuario acepta que los datos ingresados son correctos y no serán cambiados posteriormente.

A continuación, se producen los siguientes pasos:

Formación de transacciones: los registros del búfer temporal se transfieren a la matriz transaccional. Cada transacción está firmada por la clave privada del usuario, que es responsable de la precisión de la información ingresada y la ausencia de difamación en ella.

Formación de bloque: todas las transacciones creadas se ingresan en el cuerpo del bloque, se registra la clave pública de la persona que crea este bloque, se ingresa el hash del bloque anterior y se ingresa otra información especial en el encabezado del bloque. Se está implementando el algoritmo de árbol de Merkle.

Durante la formación, toda la información sobre el progreso del trabajo se muestra al usuario.

Después de que se forma el bloque, el programa notificará al usuario sobre esto, al mismo tiempo, el bloque se enviará a la red para confirmar su validez.

El perfil del usuario proporciona un acceso conveniente a la información personal y estadística, un panel para exportar claves, una descripción de las últimas acciones realizadas, así como una descripción general de los documentos que están en el sistema y fueron enviados por este usuario.

El perfil de usuario puede ser en tres colores: verde, amarillo, rojo. El color se establece en función del nivel de la confianza del usuario y de forma predeterminada, todos los usuarios tienen un "perfil verde", es decir un perfil en el que ninguno de los documentos presentados era de carácter dudosa.

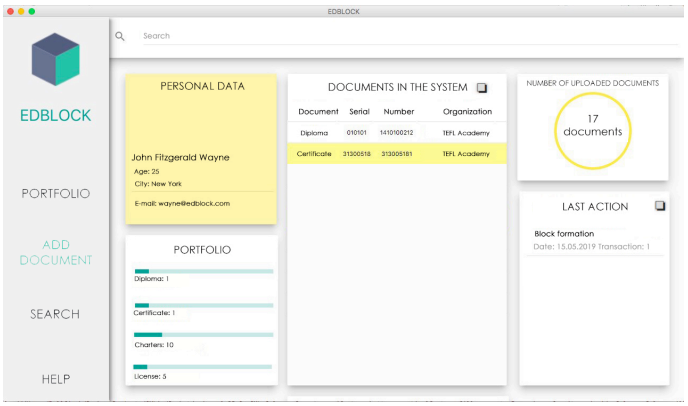

Fig. 8 El ejemplo del perfil de usuario.

El perfil de color amarillo (Fig.8) significa que algunos documentos enviados a los usuarios plantearon dudas entre otros miembros de la red. Debido a la imposibilidad de verificar el documento con la organización que lo emitió, por cuanto no está registrado en el sistema, tanto el documento, como el perfil, están marcados con un color diferente.

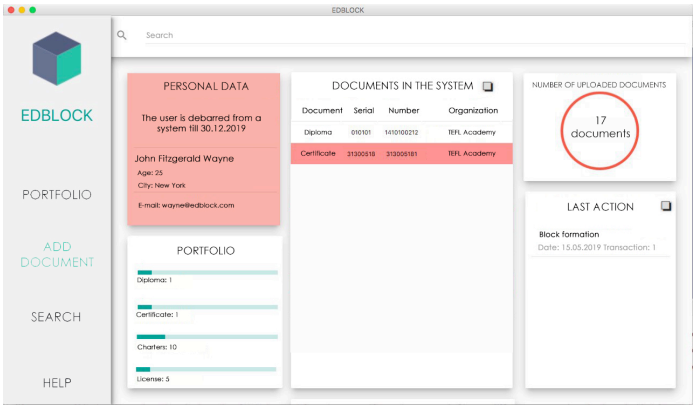

Fig. 9 El ejemplo del perfil de usuario no confiable.

Si el perfil de usuario es rojo (Fig.9), esto significa que fue visto en el envío de documentos falsos. Su tarjeta con datos personales, así como los documentos están marcados en el color correspondiente. Los usuarios identificados en el fraude quedan suspendidos de la participación en el sistema, es decir, sin la capacidad de presentar documentos por un período. Además, el indicador de reputación cae.

Si el perfil es amarillo o rojo, la tarjeta del perfil también indica el número de ciertos documentos "no confiables" en el color correspondiente.

C. Algoritmo del consenso del registro distribuido orientado a esferas sociales.

La validez del bloque es confirmada por el algoritmo de consenso. La dificultad de obtener una solución común en la cadena de bloques está asociada con las siguientes características:

1. Los participantes son desconocidos y pueden conectarse o desconectarse libremente.
2. Resistencia a las influencias externas. No es posible desconectar un nodo incluso si se sabe de antemano que el nodo no es confiable.
3. No se requiere un centro autorizado para confirmar las transacciones. El principio mismo de organizar una red blockchain es la raíz de la confianza.

El problema se resuelve utilizando algoritmos especiales, entre los cuales hay dos categorías: algoritmos basados en la evidencia de trabajo "Proof-of-Work" y algoritmos basados en la confirmación de la parte "Proof-of-Stake". El estudio de las características de los algoritmos de trabajo anteriores ha llevado a comprender la inaplicabilidad de la familia de algoritmos PoW para resolver la clase de problemas sociales. Mantener el rendimiento del sistema a través de los esfuerzos del usuario, es una motivación clave para los algoritmos de clase PoS. El sistema de información "EDUBlock" no implica un componente monetario.

Motivación: el deseo de crear un registro único de documentos educativos legales que confirme las competencias y el conocimiento de los estudiantes. El algoritmo de consenso de dicho sistema necesita una forma diferente de remuneración por el trabajo. Como alternativa, se propone utilizar conceptos tales como "actividad" y "derecho de voto". Uno de los tipos de algoritmo PoS se utiliza como base: Prueba de participación delegada o DPoS.

Desde un punto de vista político, el principio de DPOS es similar a una democracia representativa de dos capas con el sufragio de los terratenientes, donde los delegados son aquellos fabricantes de bloques que son delegados por la comunidad para resolver problemas cotidianos; los derechos de voto o sufragio de los representantes se otorgan a quienes poseen una determinada forma de propiedad. Esta propiedad puede ser una unidad de ahorro, lo que representa un compromiso de la comunidad, así como una pérdida de liquidez; se parece al sufragio histórico de la propiedad de la tierra, popular antes de las formas más universales de democracia que la burguesía trajo a la sociedad [19].

El sistema desarrollado es en todos los sentidos humanista. Por sistema humanista nos referimos a un sistema

cuyo comportamiento está fuertemente influenciado por el juicio humano o la percepción. Los métodos tradicionales de análisis de sistemas y modelado por computadora basados en métodos numéricos exactos incapaces de comprender la gran complejidad de los procesos de pensamiento humano y la toma de decisiones. La aceptación de esta premisa sugiere que, para poder hacer afirmaciones significativas sobre el comportamiento de los sistemas humanistas, puede ser necesario abandonar los estándares de rigor y precisión [20]. Es por eso que la lógica del algoritmo se basa en el concepto de conjuntos difusos y la aplicación del aparato de lógica difusa.

Para determinar la acumulación en forma de votos para la elección de delegados, presentamos el conjunto *X* "Usuario del sistema". Este conjunto incluye a todos los usuarios del sistema. El derecho a votar en la elección de un delegado está determinado por el número de votos. Este indicador se calcula en función de los siguientes criterios: tiempo dedicado continuamente en el sistema; número total de documentos educativos recibidos; el número de documentos educativos con confirmación en la emisión de la organización educativa relevante; saldo de la cuenta, estimado en el monto de la moneda interna del sistema. Los usuarios que se expresan activamente en el sistema reciben una recompensa en forma de un cargo por voz y forman un conjunto *A* de "Votante activo".

La lógica del algoritmo se basa en el concepto de números difusos y el uso del aparato de la lógica difusa. El conjunto difuso *A* "Votante activo" está representado por un conjunto de pares $A = \{(f_A(x), x)\}$, donde *x* es el usuario del sistema, $f_A(x)$ es la función de pertenencia que determina la actividad del participante. En nuestra opinión, $f_A(x)$ es un criterio global difuso para el sistema, presentado en forma de composición de cuatro criterios difusos locales. De acuerdo a la teoría de conjuntos difusos, cada uno de los criterios asume un valor desde *0* hasta *1*. Estos son:

- *t(x)* es el tiempo que el usuario pasa continuamente en el sistema;
- *d(x)* es el número total de documentos educativos recibidos;
- *d*(x)* es el número de documentos educativos que tienen confirmación en la emisión de la organización educativa relevante;
- *m(x)* es el saldo monetario de la cuenta, estimado en el valor de la moneda interna del sistema.

El votante puede regular el nivel de su actividad aumentando cualquiera de los criterios difusos locales enumerados. La evaluación de los valores de estos criterios locales ha llevado a la comprensión de la imposibilidad de utilizar el aparato "duro" de las matemáticas de intervalo difuso. Para obtener un valor cuantitativo del criterio global $p_A(x)$, L.A.Zade y R. Bellman propusieron un sistema de "relaciones suaves". La esencia de la informática suave es que, a diferencia de la informática tradicional y dura, está dirigida a una adaptación con la imprecisión generalizada del mundo real. Por lo tanto, el principio rector de la informática suave es: "... explotar la tolerancia a la imprecisión, la incertidumbre y la verdad parcial para lograr la capacidad de seguimiento, la robustez, el bajo costo de la solución y una mejor relación con la realidad". En el análisis final, el modelo a seguir para la informática suave es la mente humana [21].

El valor cuantitativo final se determina de la siguiente manera:

$$f_A(x) = m(x) + d^*(x) + d(x) + t(x) - m(x)\cdot d^*(x) - m(x)\cdot d(x) - m(x)\cdot t(x) - d^*(x)\cdot d(x) - d^*(x)\cdot t(x) - d(x)\cdot t(x) + + m(x)\cdot d^*(x)\cdot d(x) + m(x)\cdot d^*(x)\cdot t(x) + m(x)\cdot d(x)\cdot t(x) + +d^*(x)\cdot d(x)\cdot t(x) - m(x)\cdot d^*(x)\cdot d(x)\cdot t(x) \quad (1)$$

Conjunto *Y* "Delegados" se forma por la elección de representantes. Dentro de *Y* se forman un conjunto difuso V "Delegados votantes". La tarea principal resuelta por los representantes de este conjunto es la regulación del sistema mediante la generación de bloques. Como criterio difuso $r_V(y)$, se eligió un concepto como "reputación del delegado *y*". La exactitud de los juicios seleccionados es confirmada por estudios de otros autores en esta área:

"La reputación es un fundamento de la nueva economía digital, con compañías como AirBnB y Uber construyendo la confianza a través de calificaciones y revisiones. Entre los académicos, la reputación ya es un producto comercial, y la promoción y la contratación se basan en parte en la reputación medida por el número de citas y la métrica del índice H de impacto de la publicación. Imaginen que el comercio de la reputación académica podría extenderse más allá del mundo académico y convertirse en la base de una economía educativa"[16].

El criterio de reputación $r_V(y)$ del delegado *y* como evidencia de la participación inicial de la propiedad se determina con base en los siguientes cinco criterios difusos locales:

l(y) es disponibilidad de una licencia para realizar actividades educativas;

d(y) es el número de documentos educativos emitidos por la organización;

v(y) es número total de votos recibidos de los usuarios del sistema;

p(y) es porción de metadatos firmados válidos en los inválidos;

s(y) es el número total de participación como delegado.

El valor final del criterio reputación $r_V(y)$ se calcula de manera similar a la función de pertenencia del conjunto difuso "Votante activo" (1) y se puede representar en la fórmula de la siguiente manera:

$$r_A(y) = l(y) + d(y) + v(y) + p(y) - l(y)\cdot d(y) - l(y)\cdot v(y) - l(y)\cdot p(y) - d(y)\cdot v(y) - d(y)\cdot p(y) - v(y)\cdot p(y) + l(y)\cdot d(y)\cdot v(y) + l(y)\cdot d(y)\cdot p(y) + l(y)\cdot v(y)\cdot p(y) + d(y)\cdot v(y)\cdot p(y) - l(y)\cdot d(y)\cdot v(y)\cdot p(y)\cdot(1 - s(y)) + s(y) \quad (2)$$

Cada uno de los delegados seleccionados está involucrado en la formación de un bloque válido de las transacciones de

los usuarios. Cada delegado tiene un tiempo fijo para emitir bloques de cadena dentro de un solo ciclo de votación. Al celebrar una votación abierta sobre la validez del bloque formado, el bloque se considera válido, si más de la mitad de los delegados lo aceptan. Después de completar todo el círculo de votación, nuevamente se realiza una subasta para seleccionar nuevos delegados.

CONCLUSIÓN

Por lo tanto, la introducción de un sistema de acumulación de documentos educativos basado en las ideas de la tecnología blockchain resolverá los problemas de un repositorio de documentos electrónicos asequible, confiable y al mismo tiempo abierto. Debido a la creciente popularidad de los cursos masivos en línea abiertos (MOOC) y al rápido desarrollo de las tecnologías de aprendizaje electrónico, el monitoreo dinámico de las áreas populares de aprendizaje resolverá los problemas de responder rápidamente a todos los requisitos de los niveles educativos. La fiabilidad y la protección de los documentos educativos proporcionarán registros distribuidos. El sistema EDUBlock involucra la participación voluntaria y gratuita de universidades, instituciones educativas, agencias gubernamentales y especialistas calificados. Cada uno de ellos acepta las reglas del sistema y no entrega dinero, sino su propia reputación.

REFERENCIAS BIBLIOGRÁFICAS

[1] Asma Ali Mosa Al-araibi, Mohd Naz'ri bin Mahrin, Rasimah Che Mohd Yusoff, Suriayati Binti Chuprat. A model for technological aspect of e-learning readiness in higher education Received: 15 March 2018 /Accepted: 6 November 2018 /Published online: 26 November 2018 # Springer Science+Business Media, LLC, part of Springer Nature 2018

[2] Don Tapscott and Alex Tapscott Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin, 2016

[3] He Yongqiang and Yuan Jinwu. Study on the Evaluation System of E-Learning Based on E-Learning Portfolio. Computing and Intelligent Systems: International Conference, ICCIC 2011, held in Wuhan, China, September 17-18, 2011. Proceedings, Part 3. Springer Science & Business Media, 2011

[4] Linda J Børresen, Stig Arne Skjerven. Detecting fake university degrees in a digital world https://www.universityworldnews.com/post.php?story=20180911120249317

[5] André Hesselbäck. The modern counterfeit industry and higher education http://www.skvc.lt/uploads/documents/files/Naujienos/Andre_Hesselback_Vilnius_November_2016.pdf

[6] Decreto del Gobierno de la Federación de Rusia del 26 de agosto de 2013 N 729 "Sobre el Sistema de Información Federal" Registro Federal de Información sobre Documentos de Educación y (o) Calificaciones, Documentos de Capacitación " https://base.garant.ru/70441478/

[7] Secretaría de Educación Superior, Ciencia, Tecnología e Innovación https://www.educacionsuperior.gob.ec/

[8] Banco Central de la Federación Rusa. Informe para el desarrollo de consultas públicas de tecnologías de registros distribuidos. Diciembre de 2017. https://www.cbr.ru/content/document/file/36007/reestr_survey.pdf

[9] Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. Ali Hadi Mohsin, A. A. Zaidan, Bilal Bahaa, O.s. Albahri, A.s. Albahri, Mohammed Assim Alsalem. Computer Standards & Interfaces. Diciembre de 2018. DOI: 10.1016/j.csi.2018.12.002

[10] Zibin Zheng, Hong-Ning Dai, Shaoan Xie. Blockchain challenges and opportunities: a survey Article in International Journal of Web and Grid Services · October 2018

[11] Barbosa L.S. (2017) Digital Governance for Sustainable Development. In: Kar A. et al. (eds) Digital Nations – Smart Cities, Innovation, and Sustainability. I3E 2017. Lecture Notes in Computer Science, vol 10595. Springer, 2017.

[12] BitFury Group, Jeff Garzik. Open and closed blockchains. Part 1. http://forklog.com/wp-content/uploads/public-vs-private-pt1-1.0-ru.pdf.

[13] Hasil-E-Hayaat, Anu Priya, Aanchal Khatri, Prashant Dixit. Rise of Blockchain Technology: Beyond Cryptocurrency. Applications of Computing and Communication Technologies: First International Conference, ICACCT 2018, Delhi, India, March 9, 2018, Revised Selected Papers, pp. 286-300. Springer, 2018.

[14] Rs 500, 10 minutes, and you have access to billion Aadhaar details. Tribune Investigation — Security Breach. Posted at: Jan 4, 2018, 2:07 AM. https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html

[15] Esteban Vázquez Cano, Eloy López Meneses and José Luis Sarasola. La expansión del conocimiento en abierto: MOOC. Barcelona: Octaedro, 2013.

[16] Mike Sharples and John Domingue. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. Adaptive and Adaptable Learning: 11th European Conference on Technology Enhanced Learning, EC-TEL 2016, Lyon, France, September 13-16, 2016, Proceedings, pp. 490-497. Springer, 2016.

[17] Andreas Meier, Henrik Stormer. Blockchain = Distributed Ledger + Consensus. HMD Praxis der Wirtschaftsinformatik December 2018, Volume 55, Issue 6, pp 1139–1154. DOI: 10.1365/s40702-018-00457-7

[18] Acerca de BlockTac. https://www.blocktac.com/acerca-de/

[19] Ian Grigg. Seeking Consensus on Consensus - DPOS or Delegated Proof of Stake and the Two Generals' Problem https://steemit.com/eos/@iang/seeking-consensus-on-consensus-dpos-or-delegated-proof-of-stake-and-the-two-generals-problem

[20] Zadeh L.A. (1974) The Concept of a Linguistic Variable and its Application to Approximate Reasoning. In: Fu K.S., Tou J.T. (eds) Learning Systems and Intelligent Robots. Springer, Boston, MA

[21] Zadeh L.A. (1998) Roles of Soft Computing and Fuzzy Logic in the Conception, Design and Deployment of Information/Intelligent Systems. In: Kaynak O., Zadeh L.A., Türkşen B., Rudas I.J. (eds) Computational Intelligence: Soft Computing and Fuzzy-Neuro Integration with Applications. NATO ASI Series (Series F: Computer and Systems Sciences), vol 162. Springer, Berlin, Heidelberg.