Universidad Nacional Autónoma de México. Facultad de Derecho

Jersain Llamas "Transparencia y protección de datos personales en la cadena de bloques (Blockchain)"

Estudiante: Martínez Gómez Angel Sahid
Número de cuenta: 315293917
Materia: Transparencia, Derecho de acceso a la información y Protección de datos personales
Grupo:2252

El presente trabajo se realizó en el **Seminario Constructivista** y el Aula jurídica virtual bajo estructura, fuentes y supervisión de la catedrática **Graciela Staines Vega**

Universidad Nacional Autónoma de México. Facultad de Derecho

Jersain Llamas "Transparencia y protección de datos personales en la cadena de bloques (Blockchain)"

Estudiante: Martínez Gómez Angel Sahid
Materia: Transparencia, derecho de acceso a la información y protección de datos personales
Grupo: 2252
Fecha: 8 de Diciembre de 2023

El presente trabajo se realizó en el **Seminario Constructivista** y el Aula jurídica virtual bajo estructura, fuentes y supervisión de la catedrática
Graciela Staines Vega

1. Epígrafes

1. Epígrafes

2. Marco Epistémico

1. ¿Qué **derechos puede proteger** la tecnología blockchain?
2. Definir **que es Blockchain**
3. ¿**Dónde surge** esta tecnología?
4. ¿**Cómo funciona** blockchain?
5. ¿Por qué se dice que la **información** que contiene es **inmutable**?
6. ¿Qué **ventajas** nos ofrece respecto a otras tecnologías?
7. Mencionar los **problemas** que aún tiene esta tecnología
8. Explicar los **tipos** de Blockchain que existen
9. Mencionar las **normas jurídicas que lo regulan** nacional e internacionalmente
10. Definir **que es la nube**
11. Definir que es la **anonimización y seudonimización**
12. ¿Qué **posibles soluciones** le podemos dar a los problemas que presenta?

3. Genealogía

Centro Canadiense de Investigación (*International Development Research Centre*)

Es una **empresa pública canadiense** encargada de ayudar a encontrar **soluciones** a los principales problemas que aquejan **a países en desarrollo**, mediante financiamiento y promoción de la **investigación e innovación**.

Fue creado en **1970** derivado de una **ley emitida por el Parlamento de Canadá** con la encomienda de **iniciar, alentar, apoyar y llevar a cabo investigaciones** sobre los problemas que acontecían en regiones estratégicas del mundo, impulsando la aplicación de conocimientos científicos y técnicos con la finalidad de generar **progresos económicos y sociales**.

Imagen tomada de (https://idrc-crdi.ca/es/acerca-del-idrc)

3. Genealogía

Red Iberoamericana “El Derecho Informático”

Fundada en **2009** por el abogado **Guillermo M. Zamora**, es una **comunidad** de profesionales del derecho y las nuevas tecnologías, creada a partir del **interés y con el objetivo de lograr generar un aporte significativo para el progreso del derecho informático**, así como las demás ciencias afines. Es en la actualidad la **comunidad más grande** en Latinoamérica de **derecho informátic**o, además de contar con el mayor acervo de noticias, doctrina y jurisprudencia en la materia.

Imagen tomada de https://elderechoinformatico.com/?page_id=6#:~:text=La%20Red%20Iberoamericana%20«El%20Derecho,de%20las%20demás%20ciencias%20afines.)

3. Genealogía

Agencia Española de Protección de Datos

Es una autoridad estatal de control, encargada **de velar por el cumplimiento de la normatividad sobre protección de datos**. Fue creada en **1992** y comenzó a funcionar en **1994**, cuenta con **independencia presupuestal**, así como con **autonomía funcional** y nace como c**onsecuencia** de obligación contraída por España al firmar del **Convenio 108 del Consejo de Europa**, en el que se establece la necesidad de contar con una autoridad independiente que vele por el derecho a la protección de datos. Funciona como una autoridad **administrativa independiente** con personalidad jurídica propia, **plena capacidad** pública y privada y su finalidad es **proteger los derechos y libertades fundamentales** de las personas físicas en lo que respecta al tratamiento de sus datos personales.

(Imagen tomada de (https://www.aepd.es/)

3. Genealogía

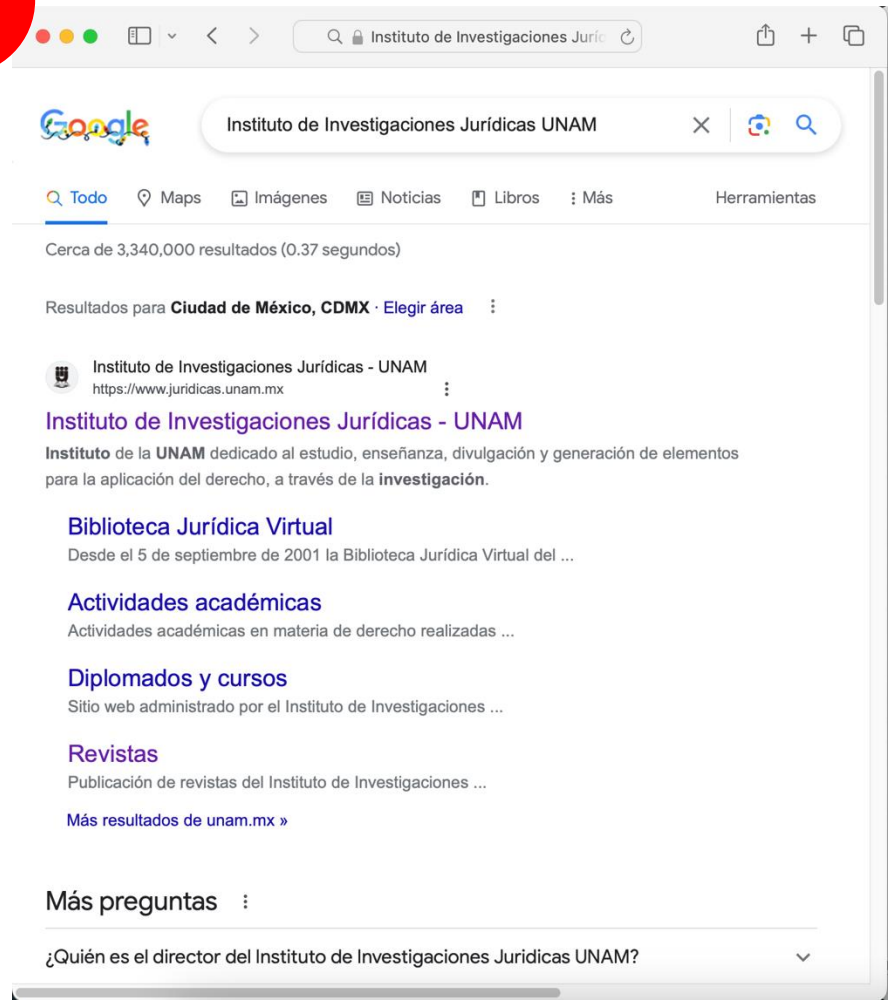
(Imagen tomada de: https://bogadosdisruptivos.mx/edicion-2021/jersain-zadamig-llamas-covarrubias/)

Autor

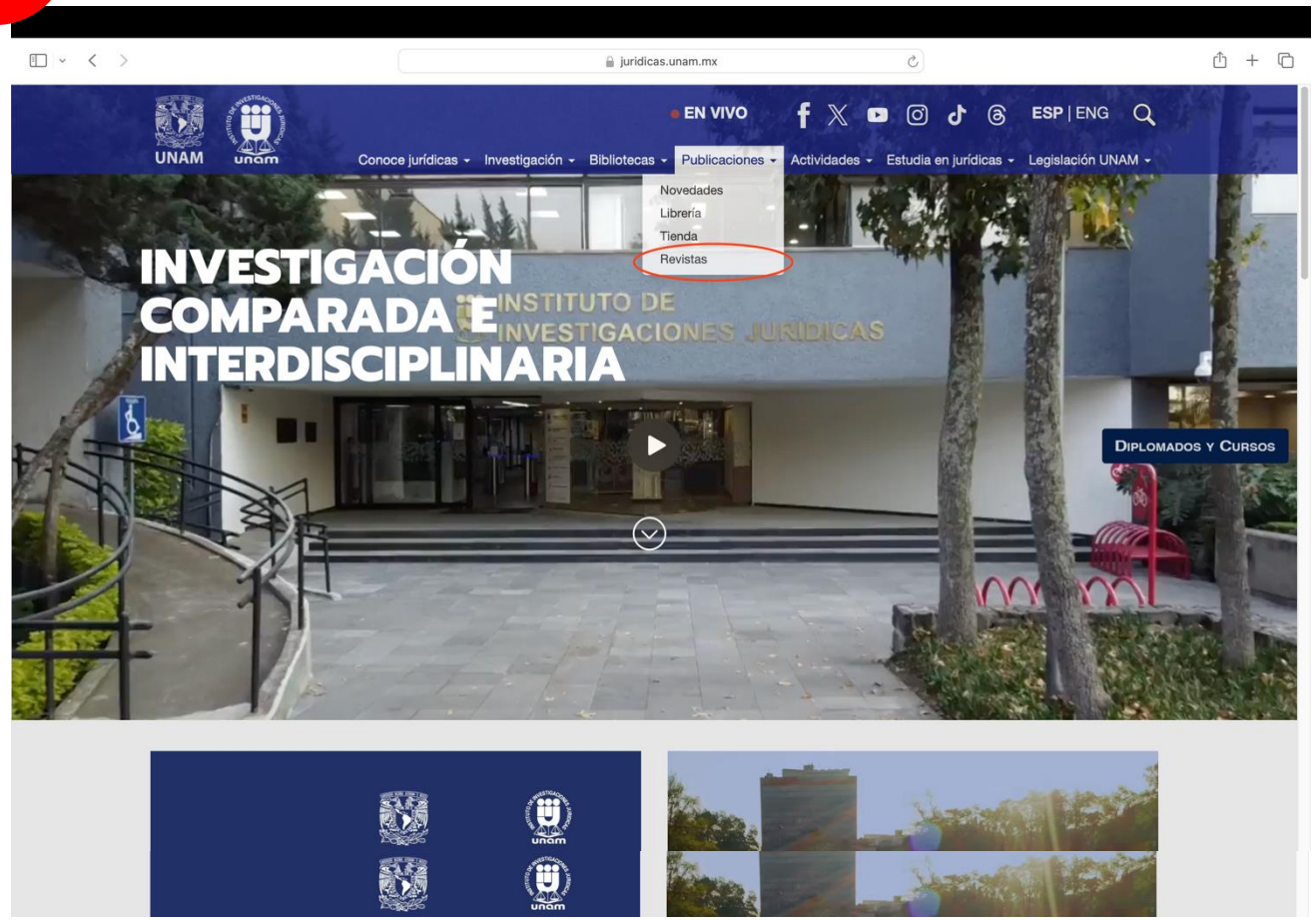
Jersain Zadaming Llamas Covarrubias es **abogado** por la **Universidad de Guadalajara**, **maestro** en derecho **constitucional y administrativo** por la misma institución. Doctorando en **ciencias de datos en el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación**. Miembro de la **Red Iberoamericana "El Derecho Informático"** Actualmente se desempeña como consultor y abogado especializado en derecho y las nuevas tecnologías de la información y comunicación

4. Fuente

1

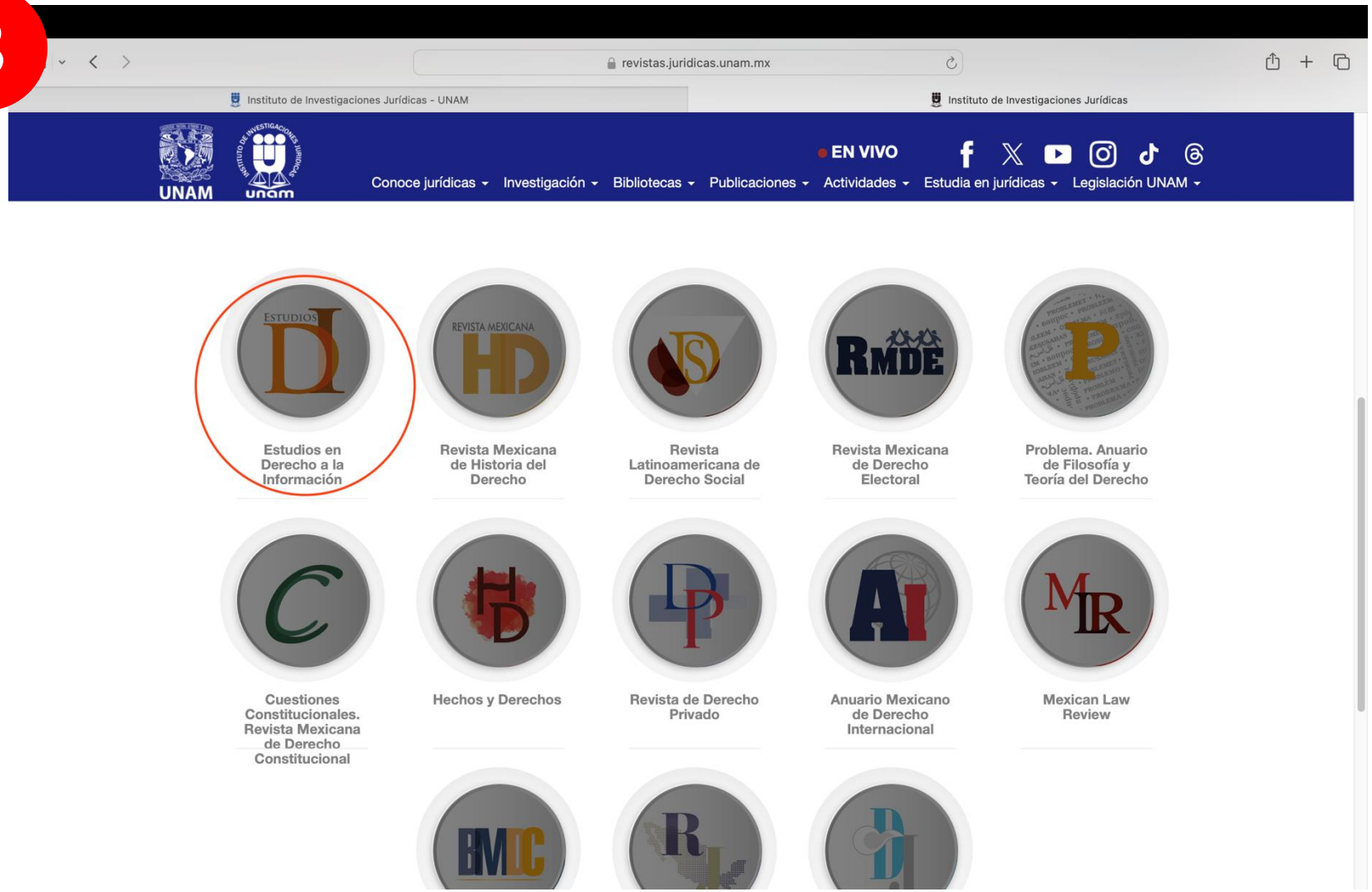

Instituto de Investigaciones Jurídicas UNAM
Todo
Maps
Imágenes
Noticias
Libros
Más
Herramientas
Cerca de 3,340,000 resultados (0.37 segundos)
Resultados para Ciudad de México, CDMX · Elegir área
Instituto de Investigaciones Jurídicas - UNAM
https://www.juridicas.unam.mx
Instituto de Investigaciones Jurídicas - UNAM
Instituto de la UNAM dedicado al estudio, enseñanza, divulgación y generación de elementos para la aplicación del derecho, a través de la investigación.
Biblioteca Jurídica Virtual
Desde el 5 de septiembre de 2001 la Biblioteca Jurídica Virtual del ...
Actividades académicas
Actividades académicas en materia de derecho realizadas ...
Diplomados y cursos
Sitio web administrado por el Instituto de Investigaciones ...
Revistas
Publicación de revistas del Instituto de Investigaciones ...
Más resultados de unam.mx »
Más preguntas
¿Quién es el director del Instituto de Investigaciones Juridicas UNAM?

2


juridicas.unam.mx
UNAM
EN VIVO
ESP | ENG
Conoce jurídicas
Investigación
Bibliotecas
Publicaciones
Actividades
Estudia en jurídicas
Legislación UNAM
Novedades
Librería
Tienda
Revistas
INVESTIGACIÓN COMPARADA E INTERDISCIPLINARIA
INSTITUTO DE INVESTIGACIONES JURÍDICAS
DIPLOMADOS Y CURSOS

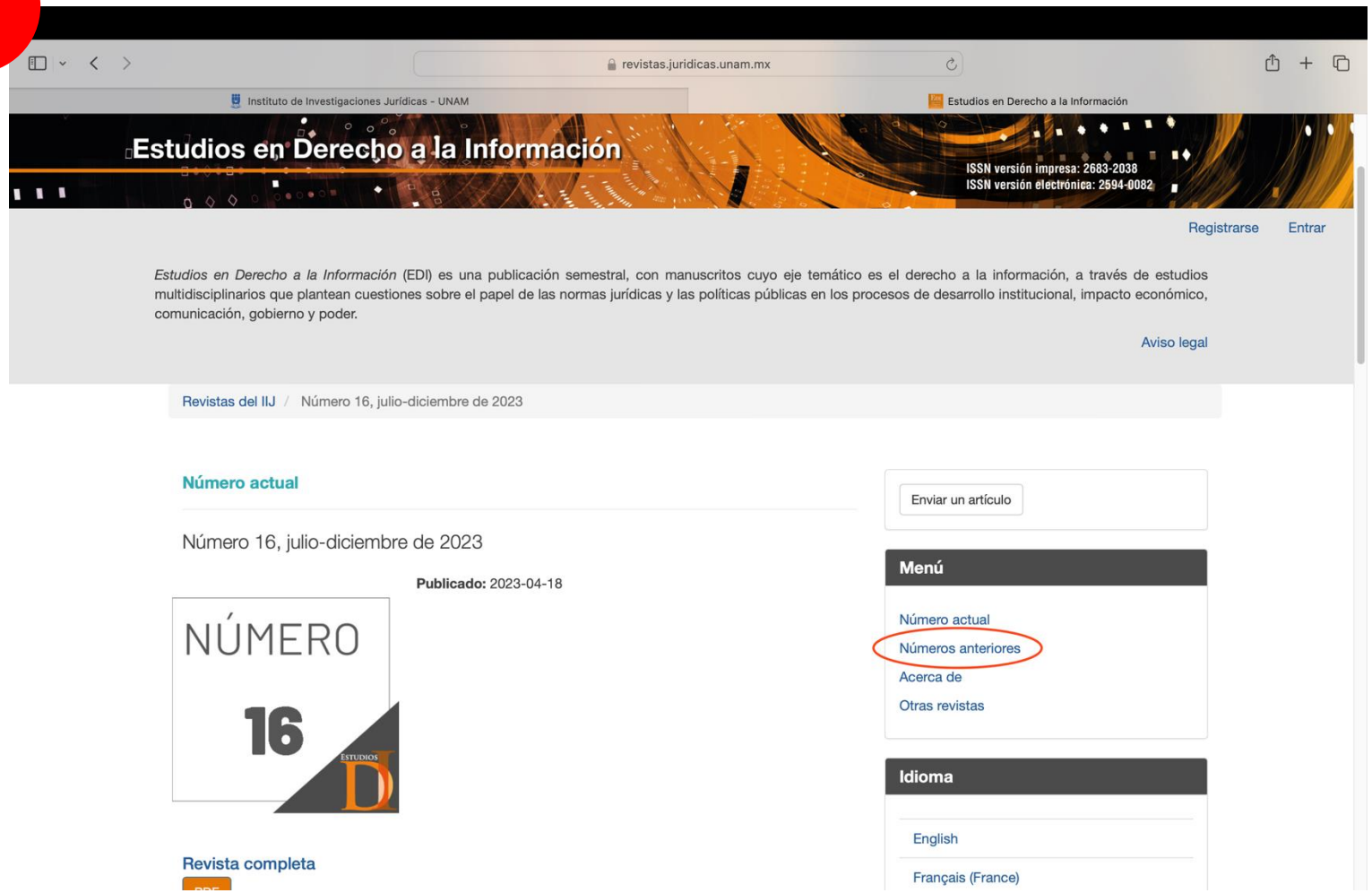
4. Fuente

3


revistas.juridicas.unam.mx
Instituto de Investigaciones Jurídicas - UNAM
Instituto de Investigaciones Jurídicas
UNAM
EN VIVO
Conoce jurídicas
Investigación
Bibliotecas
Publicaciones
Actividades
Estudia en jurídicas
Legislación UNAM
Estudios en Derecho a la Información
Revista Mexicana de Historia del Derecho
Revista Latinoamericana de Derecho Social
Revista Mexicana de Derecho Electoral
Problema. Anuario de Filosofía y Teoría del Derecho
Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional
Hechos y Derechos
Revista de Derecho Privado
Anuario Mexicano de Derecho Internacional
Mexican Law Review

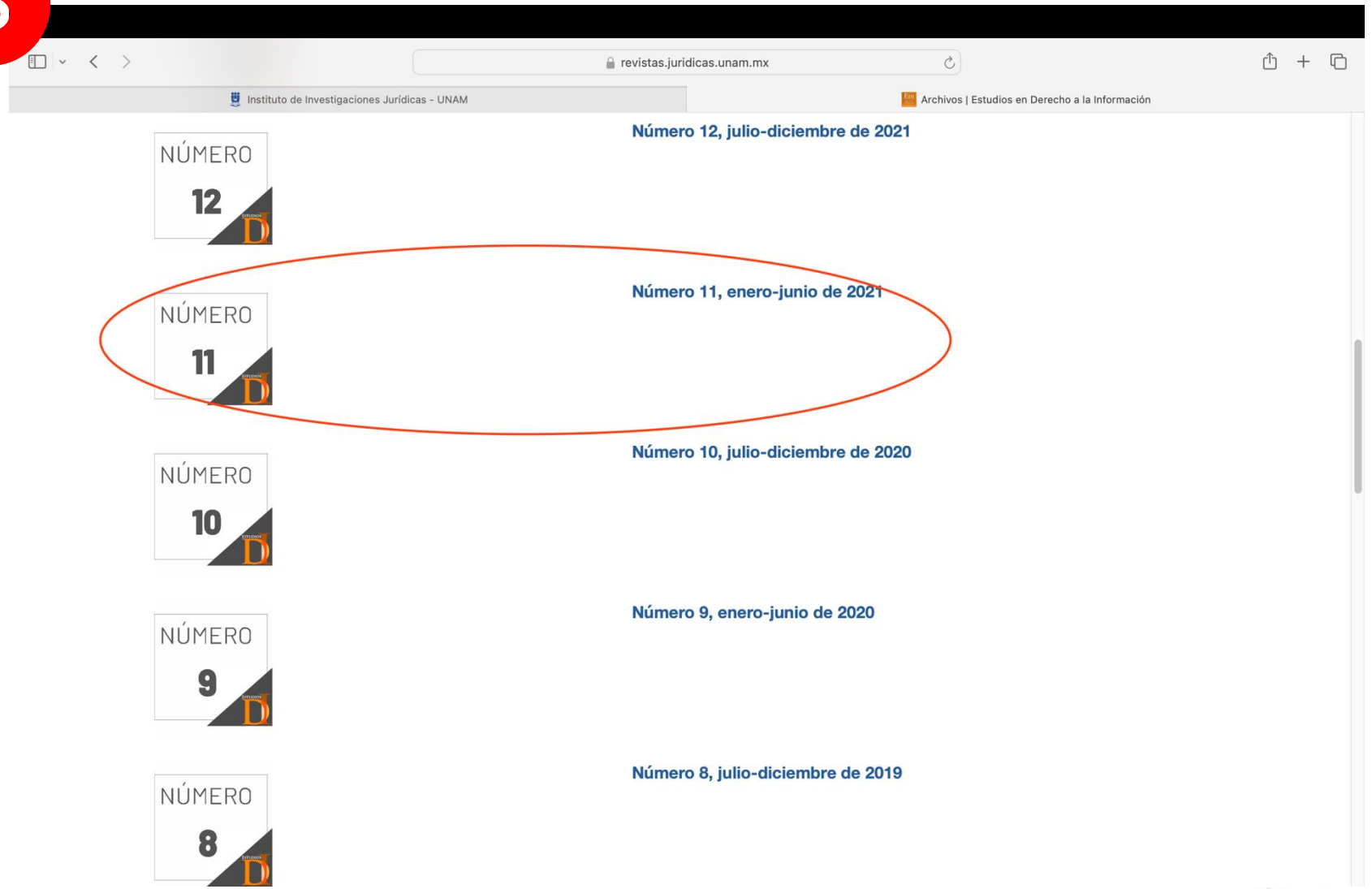
4. Fuente

4


revistas.juridicas.unam.mx
Instituto de Investigaciones Jurídicas - UNAM
Estudios en Derecho a la Información
Estudios en Derecho a la Información
ISSN versión impresa: 2683-2038
ISSN versión electrónica: 2594-0082
Registrarse
Entrar
Estudios en Derecho a la Información (EDI) es una publicación semestral, con manuscritos cuyo eje temático es el derecho a la información, a través de estudios multidisciplinarios que plantean cuestiones sobre el papel de las normas jurídicas y las políticas públicas en los procesos de desarrollo institucional, impacto económico, comunicación, gobierno y poder.
Aviso legal
Revistas del IIJ / Número 16, julio-diciembre de 2023
Número actual
Número 16, julio-diciembre de 2023
Publicado: 2023-04-18
NÚMERO
16
Revista completa
Enviar un artículo
Menú
Número actual
Números anteriores
Acerca de
Otras revistas
Idioma
English
Français (France)

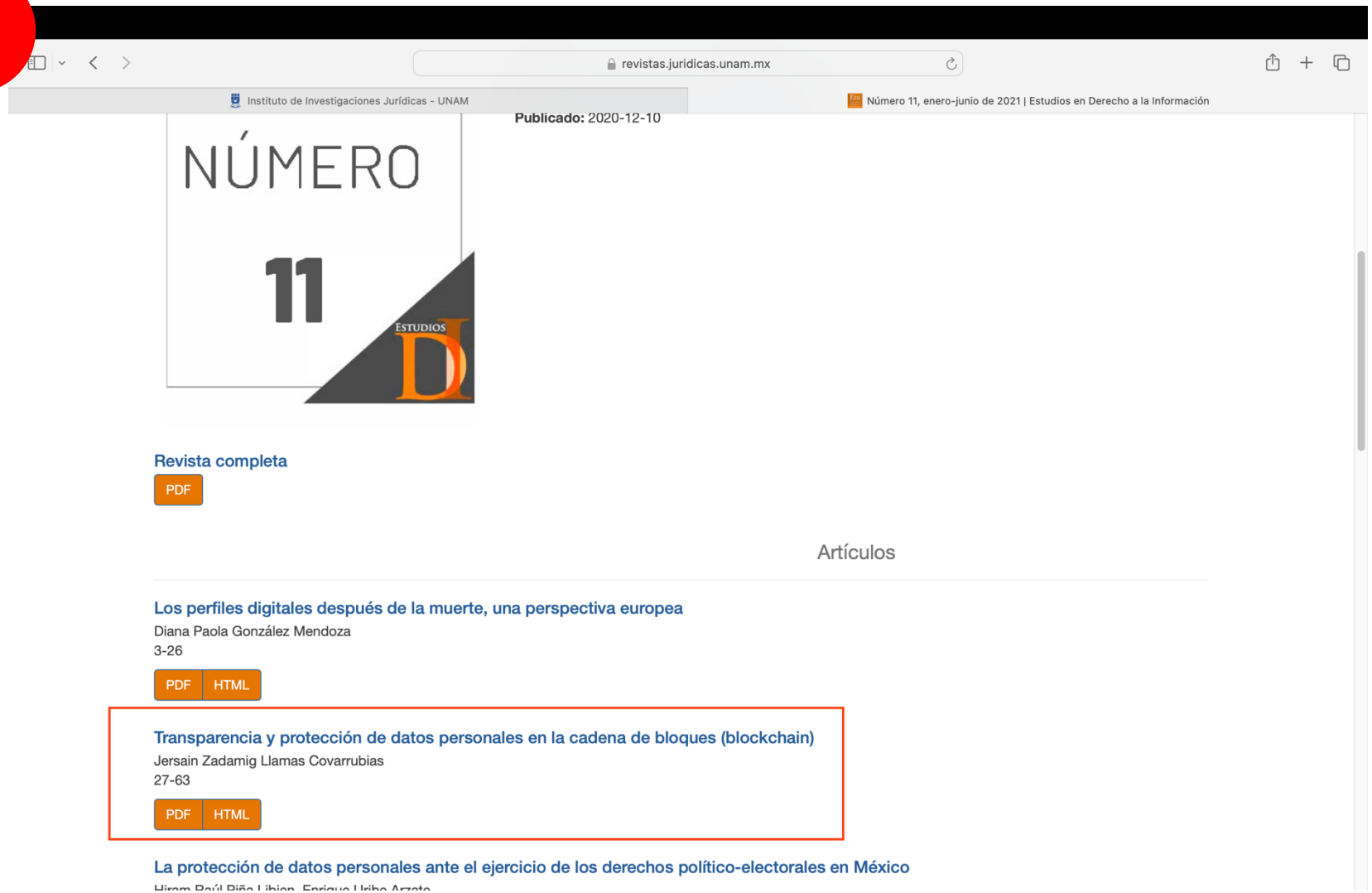
4. Fuente

5


revistas.juridicas.unam.mx
Instituto de Investigaciones Jurídicas - UNAM
Archivos | Estudios en Derecho a la Información
NÚMERO 12
Número 12, julio-diciembre de 2021
NÚMERO 11
Número 11, enero-junio de 2021
NÚMERO 10
Número 10, julio-diciembre de 2020
NÚMERO 9
Número 9, enero-junio de 2020
NÚMERO 8
Número 8, julio-diciembre de 2019

4. Fuente

6



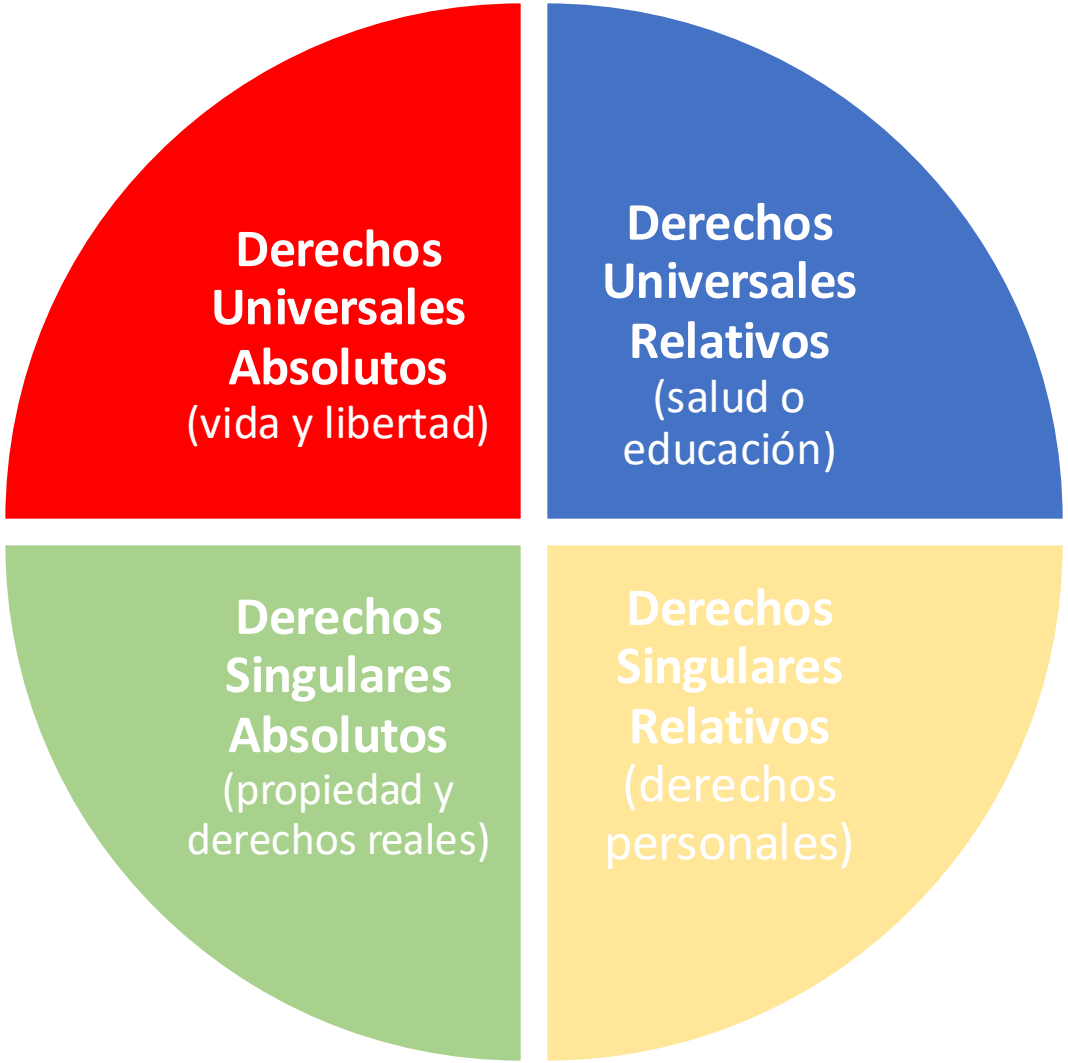
Aprendizaje significativo adquirido en el Seminario Contructivista de Derecho a la Información

5. Introducción

Imagen obtenida de: (https://fcconsultingroup.com/seguridad-de-la-informacion/seguridad-y-privacidad-la-formula-perfecta-para-la-proteccion-de-la-informacion/)

Uno de los principales **retos de la tecnología y comunicación es la privacidad y seguridad de la información**, esto debido la constante puesta en peligro de nuestros **datos personales**. Blockchain, es una tecnología que, por sus características de **inmutabilidad, confianza, transparencia, descentralización y distribución de los registros**, representa una alternativa para mantener la privacidad y protección de nuestros datos personales. Ningún derecho es absoluto, ya que existen otros derechos que deben ser igualmente protegidos, por ello el **derecho de acceso a la información y protección de datos personales pueden ser limitados de forma excepcional** (pag 27-28)

5. Introducción



Esta clasificación **no contempla** el derecho a la información y protección de datos personales como derechos universales absolutos, sin embargo, esto no acarrea su desatención

(pag 28)

(Diagrama realizado por el ponente con el aprendizaje significativo adquirido en el seminario . Información de la página 28)

5.1. Derechos protegidos

Derechos potencialmente protegidos	
Derechos ARCO (acceso, rectificación, cancelación y oposición)	Derecho al Anonimato
Habeas Data	Derecho a la verdad
Derecho al Olvido,	Derecho a encriptar
Derecho a la Intimidad,	Derecho a la auditoría
Derecho a la privacidad	Derecho a la gobernanza electrónica

(Elaboración propia con base en el texto página 29.
Aprendizaje significativo adquirido durante el seminario)

6. Blockchain.

Imagen obtenida de (https://www.tradingdesdecero.com/satoshi-nakamoto/)

Imagen obtenida de (https://news.microsoft.com/es-xl/objetivo-2018-aprender-mas-acerca-blockchain/)

6.1. Origen

Blockchain surge en **2008** con la publicación del artículo "**Bitcoin: A Peer-to-Peer Electronic Cash System"** por **Satoshi Nakamoto**, siendo que un año después este desarrollaría la red que integraría bitcoin formando parte de esta la tecnología blockchain

6.2. Concepto

Blockchain es un **sistema descentralizado, distribuido y un mecanismo de consenso con sistemas criptográficos**. Este representa una herramienta innovadora pues funciona como un **medio de acoplamiento entre unidades independientes** y consiste en un **sistema de marcadores digitales** a prueba de manipulaciones. (pag 29-30)

6. Blockchain.

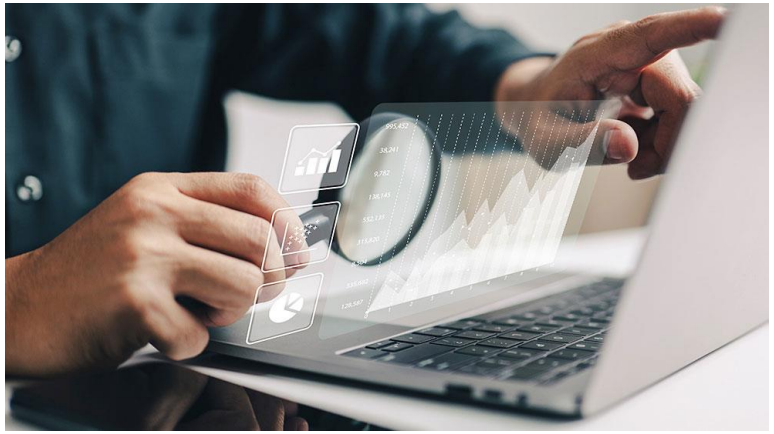


Imagen obtenida de: (https://www.gaceta.unam.mx/realizan-semanas-universitarias-por-la-transparencia-en-10-entidades-del-pais/)

Imangen obtenida de: (https://entrenadoresdepensamiento.com/revista/espiritu-de-consenso)

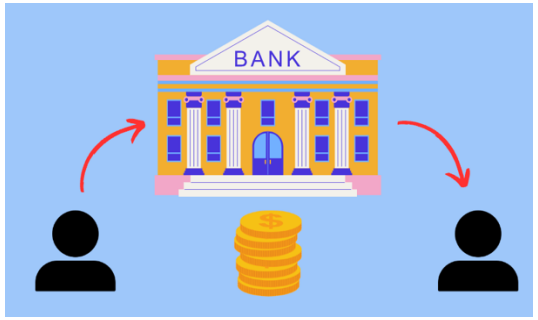
- Permite que los usuarios **registren transacciones** en un **libro mayor**, el cual es **compartido en una comunidad**.
- Este sistema permite crear una red entre personas, usando sus propios dispositivos **sin necesidad del control de una unidad central** y es gracias a esta característica que los dispositivos que integran la red **validan las transacciones mediante un mecanismo de consenso**.
- Esto se realiza mediante un software que una vez **instalado en un dispositivo** descarga la información que integra la cadena de bloques y replica todo el registro de la red garantizando la inmutabilidad de la información.
- Una de las **cualidades** principales que permite este sistema y su funcionamiento es la **transparencia** en la información que aloja, ya que los registros de información pueden ser **consultados y leídos por cualquier persona que pertenezca al sistema**

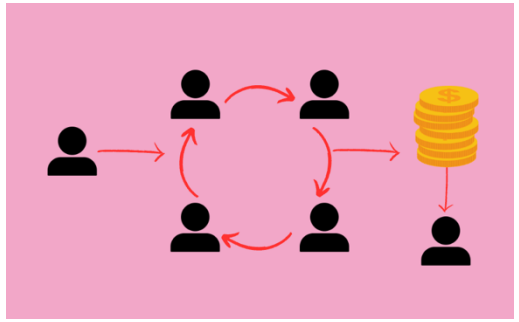
(pag 30)

6.3. Conceptos relevantes

6.3.1. Sistemas centralizados y descentralizados

Aquellos que **dependen de un ente central** son centralizados.. Aquellos descentralizados dependen de **una colectividad**. En un sistema como este, todos **sus componentes se conectan entre ellos** y si uno de ellos cae no afecta a los demás.





6.3.2. Cifrado

Transformar información para protegerla. Desde el punto de vista informático es ejecutar un algoritmo aplicado a una o varias contraseñas que **transforman la información en un conjunto de números, símbolos o letras con o sin sentido**. Normalmente solo **protegen el acceso** y no la información. **SHA-256** uno de los programas de cifrado más completos en la actualidad.

Transparencia = Usbñtqbsfñdjb

Imágenes hechas por el ponente con: (https://www.canva.com/es_419/)
Información: Edteam ¿Qué es blockchain y como funciona? 27 may 2022. 2.00-11.29. Video en https://www.youtube.com/watch?v=mKCcki6azHo

6.4. Funcionamiento general

6.4.1. Definición.

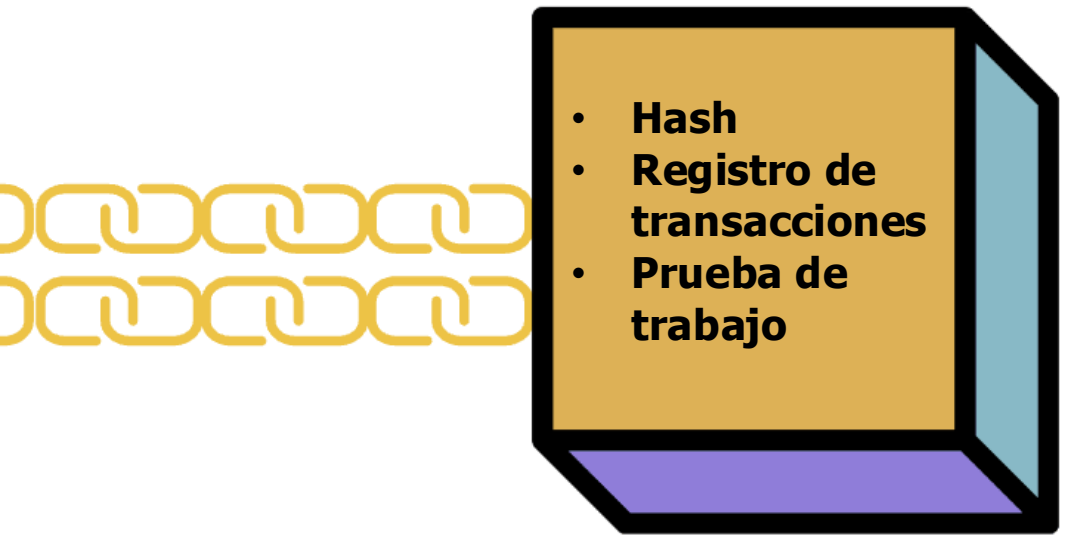
Imagen obtenida de: (https://es.dreamstime.com/tablero-del-registro-control-hombre-con-el-acuerdo-disponible-de-la-lista-diseño-plano-image118426183)

"**Registro compartido** de manera distribuida y **descentralizada** entre múltiples dispositivos, donde las transacciones se registran y validan mediante un mecanismo de consenso, las cuáles son agregadas en bloques unidos con una cadena criptográfica, con el fin de crear marcadores digitales a prueba de manipulaciones y resistentes a la misma" (1)

Respecto a su funcionamiento general, primero debemos visualizar que tenemos un **registro contable único y universal** en que escribimos todos los movimientos que realizamos. Este registro no se encuentra en una unidad central, sino que está **distribuido de manera descentralizada** en distintos dispositivos sin jerarquizar ninguno de ellos. (pag 31-32)

(1)Quirós, Fernando, 2019, "Advierten que en México debe realizarse un estudio exhaustivo antes de implementar tecnología blockchain para votaciones", CoinTelegraph en Español, disponible en https://es.cointelegraph.com/news/they-warn-that-in-mexico-an-exhaustive-study-must-be-carried-out-before-implementing-blockchain-technology-for-voting.

6.4.2. Partes que lo integran



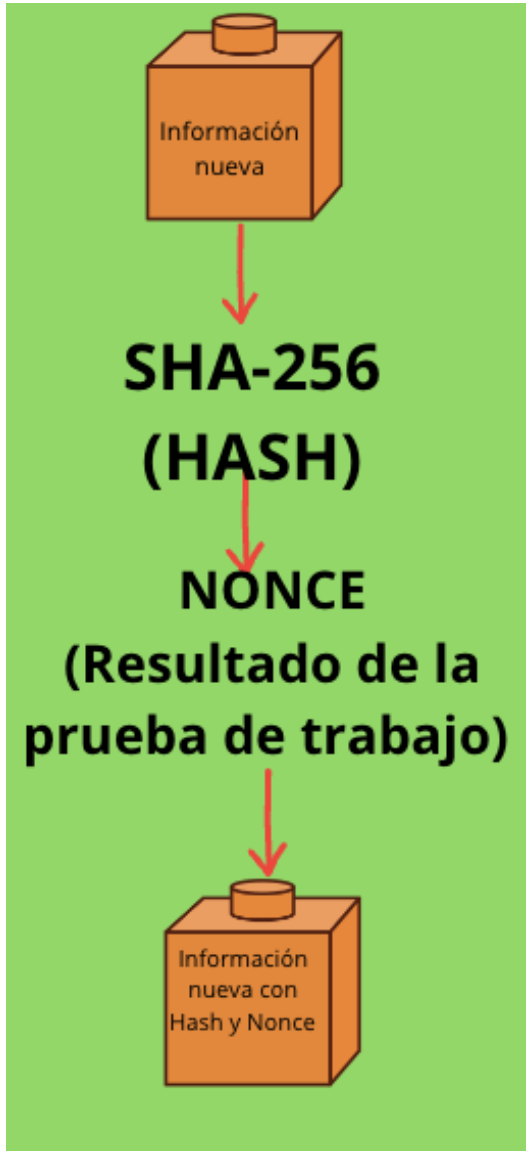
Imágenes hechas por el ponente con: (https://www.canva.com/es_419/)

1. Un **hash.** Que es el **resultado de la codificación** generada por SHA-256 (programa de cifrado) Este hash se genera respecto a la información que contiene el bloque anterior, es decir que ante la entrada de nueva información se crea un hash nuevo. Cualquier modificación a la información anterior cambiaría el hash, esto haría que se **rompiera la cadena de información**.
2. **Registro de transacciones**. Libro contable de los movimientos hechos en la información
3. **Prueba de trabajo**. Problema algorítmico de difícil resolución . La única forma de resolverlo es mediante **prueba y error**. (esta prueba y error se le llama minería) Se dan 10 minutos para la resolución del problema.

ED team. ¿Qué es blockchain y como funciona? 27 may 2022. 7.30-10.00. Video en https://www.youtube.com/watch?v=mKCcki6azHo

6.4.3. Actualización y sincronización.

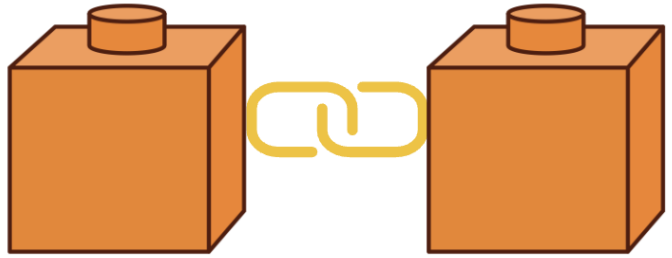
Imágenes hechas por el ponente con: (https://www.canva.com/es_419/)



Las transacciones son registradas mediante un mecanismo de concenso, el propuesto por Nakamoto es el "**Proof of work**" o prueba de trabajo, este es un mecanismo por el cual, mediante prueba y error y recursos computacionales se llega a un **factor que es aceptado de forma conjunta** por toda la red a esto de le llama **protocolo de concenso**. Cada uno de los bloques de la cadena es generado cada 10 minutos aproximandamente, tiempo en que los mineros tienen que cambiar el **NONCE** (resultado de las pruebas de trabajo) produciendo los hash de salida en el cifrado **SHA-256**, esto solo si el nuevo hash cumple los requisitos necesarios. Una vez generado el hash es enviado los demás mineros para su aceptación y validación.

(pag 33-34)

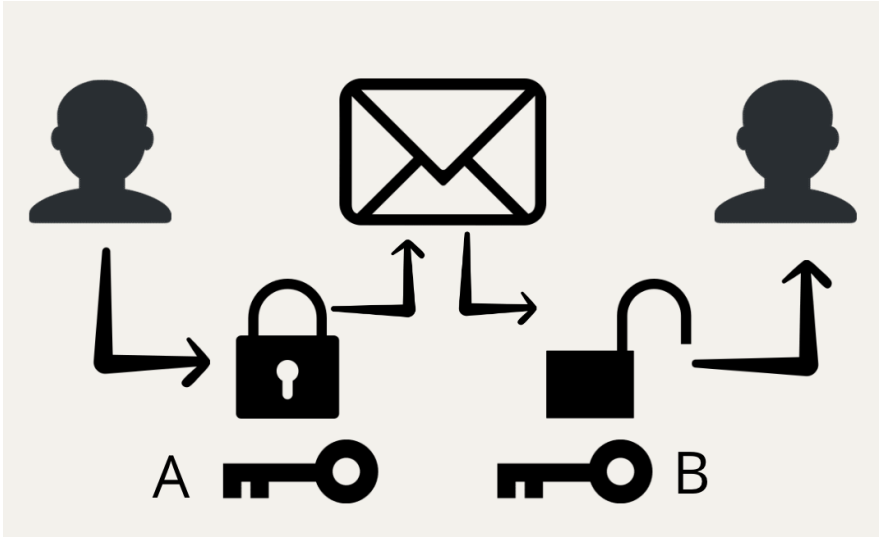
6.4.4. Adición de bloques.



- Hash actual
- Hash anterior
- Marca de tiempo
- Información

Estos son agregados en bloques unidos con una **cadena criptográfica**, lo cual brinda **inmutabilidad** a la información. Cada uno de los bloques de la cadena cuentan con un **historial del bloque anterior**, esto mediante la producción de un hash antes de que los bloques sean publicados,. Esta marca hará que los bloques anteriores sean **innmutlables**.

6.4.5. Sistema asimétrico de cifrado.



Imágenes hechas por el ponente con: (https://www.canva.com/es_419/)

Cuenta con dos llaves para acceder a la información, si se quiere compartir información con otra persona se debe **cifrar utilizando una clave pública**. Una vez cifrada la información se **descifrará** mediante una clave privada. Cada uno de los usuarios de blockchain cuentan con una clave privada unica e irrepetible que puede **encriptar y desecriptar la información**.

(pag 35-36)

6.4.6. Inmutabilidad de blockchain.	6.4.8. Transparencia.	6.4.7. Permanencia en la red.
Al estar conectados todos los bloques existen **marcadores** específicos para la información que impiden su manipulación y siendo un sistema descentralizado los **usuarios en concenso expulsarían la información inválida o apócrifa**.	Se dice que blockchain es un sistema transparente al poderse examinar todas las transacciones existentes en la información, esto gracias a la unidad de los **bloques protegidos con marcadores que ofrecen inmutablidad**	Es un sistema **autopioético** en el cual se generan bloques de manera constante al existir una recompensa a los usuarios al resolver las pruebas de trabajo. En su funcionamiento primigeneo la recompensa obtenida eran **bitcoins**

Diagrama realizado con el aprendiaje significativo adquirido durante el seminario de Derecho a la información

(pag 37-39)

7. Transparencia y blockchain

7.1. Ventajas y desventaja.

VENTAJAS	DESVENTAJA
1. Cierra el camino a cualquier intento de cambios no autorizados de la información y registra todos los movimientos y modificaciones que se llevan a cabo, funcionando como un **vehiculo de vigilancia y control** 2. Los **registros son almacenados de forma sequencial con marcas de tiempo y autenticación en cada modificación**	1. Desde un punto de vista técnico existe falibilidad de este sistema descentralizado, esto debido a la **credibilidad de los nodos que verifican la infomación**, ya que una cadena solo puede considerarse garantizada cuando el 51% de los nodos sean considerados honestos (pag 38)

Diagrama realizado con el aprendiaje significativo adquirido durante el seminario de Derecho a la información

7.2. Problemas de blockchain.

7.2.1. Problema 1.

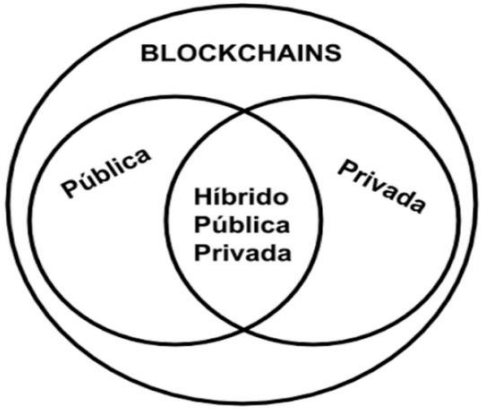
7.2.1.1. Tipos de Blockchain

TIPOS DE CADENA

A. **Publicas**, son aquellas que **no son propiedad de nadie**, **abiertas** al público y **todos pueden participar** en el proceso de toma de decisiones, la participación de los usuarios es incentivada con recompensas en la prueba de trabajo y el libro de resgistros es público.

B. **Privadas**, son en las que consorcios o grupos de individuos deciden contar con **un libro solo distribuido** entre ellos.

C. **Hibridas** son aquellas en las que se tiene una autorización **parcialmente provada** y es usada en grupos de compañías por un consorcio, es decir los datos desean mantenerse privados, pero se quiere aprovechar las herramientas de certeza de la información.



FUENTE: gráfico hecho con base en Zambrano, 2017: 29.

(pag 41-42)

7.2.1.2. Falibilidad.

Imagen tomada de (https://www.freepik.es/vector-gratis/gente-trabajo-equipo-piezas-rompecabezas_5686193.htm)

En los sistemas públicos la **colectividad** puede verificar la resolución de la **prueba de trabajo**, sin embargo, en los sistemas privados llamados también ***Distributed Ledger Technology*** (DLT) en español, **Tecnología de libro mayor distribuido**, solo los **miembros** de estos grupos forman el equipo que aprobará en concenso las pruebas de trabajo, con ello pueden **ponerse de acuerdo para formar un grupo mayoritario** que apruebe **modificaciones indebidas** a la información que se contiene. Para su implementación en el sector público debe existir una sinergia entre el sector público, privado y sociedad civil, con la finalidad de que la información en el contenida no sea manipulada. En las **redes privadas** la caracteristica de descentralización del sistema genera que existan **riesgos a la inmutabilidad de la información**, ya que el mecanismo de concenso funciona dentro de un grupo cerrado que puede o no aprobar decisiones correctas. (pag 42)

7.2.2. Problema 2.

Imagen obtenida de (https://www.freepik.es/vector-premium/privacidad-datos-usuario-internet-proteger-aplicacion-rastrear-o-seguir-concepto-comportamiento-usuario-hombre-sosteniendo-tecla-despues-bloquear-ojo-espia-telefono-inteligente-dejar-ver-informacion-privada_16243140.htm)

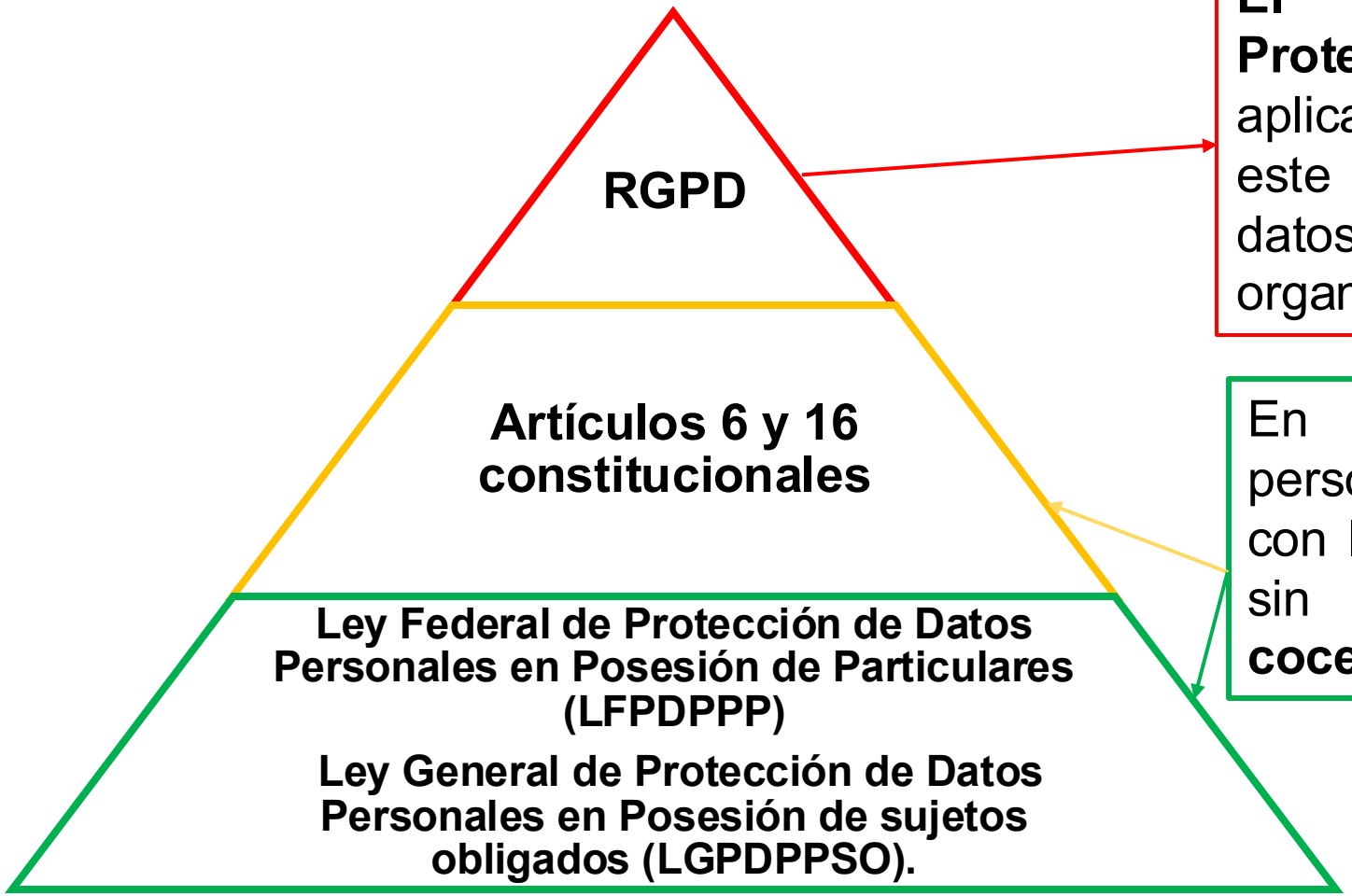
Otro problema que surge con esta tecnología es su **transparencia *per se***, que aunque es una de las ventajas más representativas, también representa un **riesgo** para los **intereses jurídicos de confidencialidad y reserva de información** en los casos en los que los usuarios **no deseen que la información que en ellas se introduce sea divulgada**. De acuerdo a un informe publicado por el **Centro Internacional de Investigaciones para el Desarrollo de Canadá** (*International Development Reserch Center*) existen distintos tipos de clasificaciones de blockchain y derivado de la situación en que se quiera ocupar, debe seleccionarse entre público, privado e hibrida.

(pag 42)

8. Protección de datos personales y blockchain

8.1. Marco jurídico internacional

8.2 Marco jurídico Nacional.



El RGPD (Reglamento General de Protección de datos) fue aprobado en 2016 y aplicado en **2018** por el Parlamento Europeo, este regula el tratamiento que se da a los datos personales de las personas, empresas y organizaciones en la Unión Europea.

En materia de Protección de Datos personales. Ambas leyes son incompatibles con la aplicación de la tecnología blockchain, sin embargo, **reconocen y aceptan el cocepto de nube infomática**

(pag 43)

Diagrama realizado con el aprendiaje significativo adquirido durante el seminario de Derecho a la información

8.2.1 Concepto de Nube

El artículo 3° fracción VI de la **Ley General de Protección de Datos Personales en Posesión de sujetos obligados** en donde se define el concepto de cómputo en la nube como:
"Modelo de **provisión externa** de servicios de cómputo bajo demanda, que implica el **suministro de infraestructura, plataforma o programa informático**, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente".

8.2.2. Tipos de servicio de nube.

Software as a Service (SaaS)	Platform as a Service (PaaS)	Infrastructure as a Service (IaaS)
Servicio que puede ser usado **sin la necesidad de descargar un software**, ejemplo de este es Google Drive (modelo de entrada de blockchain que permite nuestra legislación	Plataforma en la que se **permite desarrolar aplicaciones y ofrecer servicios sin necesidad de instalar un software**, ejemplo de este es Google App Engine.	Servicio online que permite **pagar por recursos de hardware**, ejemplo de este es Amazon Web Services, el cual ofrece servicios de procesamiento.

(pag 43)

Diagrama realizado con el aprendiaje significativo adquirido durante el seminario de Derecho a la información

8.3. Asuntos por considerar en la cadena de bloques.

Imagen obtenida de (https://esemanal.mx/2020/08/que-tan-segura-es-su-red/)

Imagen obtenida de (https://www.cinconoticias.com/anonimo-autores-literatura/)

A. **La inmutabilidad de la información y su oposición al derecho de rectificación, cencelación, oposición o el derecho al olvido,** así como la transmición de datos personales en una red dsitribuida.

B. Si los datos que serán proporcionados a Blockchain deben ser cosiderados datos personales o al estar cifrados bajo una función Hash pueden ser **seudonomizados o anonimizados.** Siendo que de esta forma no podría aplicarsele el reglamento General de Protección de datos pues no se consideran en nuestro país como información personal por no ser concerniente a una **persona identificada o identificable,** esto es no poder poderse conocer su identidad de manera directa (pag 43-44)

8.3.1. Tratamiento en Europa.

Imagen obtenida de (https://luismariolemus.com/2018/05/15/el-impacto-del-reglamento-generl-de-proteccion-de-datos-gdpr-en-mexico/)

Imagen obtenida de (https://abdc.es/blog/agencia-espanola-proteccion-datos/)

En europa datos personales se considera a toda información sobre una persona física identificada o identificable.

Persona física identificable se define como a "toda persona cuya identidad pueda determinarse de forma directa o indirecta vía un identificador como el nombre, número de identificación, datos de localización o uno o varios elementos de la identidad física, fisiológica, genética, económica cultural o social de una persona".Por ello el RGPD deja fuera los datos anónimos al considerar que no guardan relación con una persona que sea identificada o identificable. Por su parte, la **agencia Española de Protección de Datos** se manifiesta sobre el tema mencionando que el proceso de anonimización es "eliminar o reducir los riesgos de reidentificación de los datos anonimizados" es decir evitar la identificación de las personas (pag 44-45)

8.3.2 Anonimización.

Anonimización	Seudonimización
Podemos definir la anonimización como las **técnicas** que se emplean en datos personales con el fin de ser **disociados**, eliminando la posibilidad de identificación a las personas de forma **irreversible**. Por ello la información anonimizada en ningun caso pueden tener **vínculo** con un dato que pueda provocar la identificación de las personas.	Hace que los datos personales no se puedan identificar a una persona, sin utilizar información adicional, por ello se considera **reversible**. Mientras que en este procedimiento se reemplazan campos de información personal a través de distintos medios, se mantienen datos adicionales que en conjunto pueden permitir la **identificación de las personas**.

Diagrama realizado con el aprendiaje significativo adquirido durante el seminario de Derecho a la información

(pag 46)

8.3.3. Riesgos.

El **Grupo de Trabajo del artículo 29** (Ahora Comité Europeo de Protección de Datos, **organo consultivo** encargado de velar por que los paises de la unión europea **apliquen sistematicamente** las normas en **materia de protección de datos**) ha comentado que para anonimizar los datos es necesario **eliminar de forma irreversible los elementos suficientes para que no pueda identificarse al interesado**. Este organo identifca tres **riesgos clave** a tener en cuenta en la anonimización:

1. **Singularización**. La posibilidad de extraer un **conjunto de datos o registros que permitan identificar** a una persona

2. **Vinculabilidad.** La capacidad de vinculación de información de un interesado con un grupo mediante **analisis de correlación**

3. **Inferencia**. La posibilidad de **deducir una probabilidad** mediante el valor de un atributo a partir de los valores de un conjunto de datos.

(pag 45)

8.3.4. Datos seudonomizados

Imagen obtenida de (https://quelibroleo.com/noticias/autores/50-escritores-con-seudonimo/)

RGPD MAY/2017 Correciones 23/MAY/2018
LGPDPPSO D.O.F.26/ENE/2017 Sin reforma

El **Reglamento General de Protección de datos** los define como:

"el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (Artículo 4)"

En la legislación mexicana este concepto, así como el de anonimización son inexistentes, sin embargo, la palabra disociación si tiene una definición , que es:

"el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo" (artículo 3, fracción XIII, Ley General de Protección de Datos Personales en Posesión de sujetos obligados LGPDPPSO).

De su interpretación prodemos concluir que el proceso de **disociación** es un proceso realmente de seudonimización.

(pag 46)

8.4. Codificación, cifrado y hash.

CODIFICACIÓN	CIFRADO	HASH
Su finalidad es mantener la **usabilidad de los datos** y puede **revertirse** usando el mismo algoritmo sin necesidad del uso de una clave	Su finalidad es mantener la **confidencialidad de los datos** y requiere una clave para descifrar la información. Su acción es **irreversible,** sin embargo, al ser identificable el titular de la clave se vuelve un método seudonimizado ya que los datos no se convierten irreversiblemente a anonimos**.**	Sirve para **validar la integridad del contenido y detectar sus modificaciones.** Además de ello sus resultados si se convierten de forma casi irreversible en anónimos, pues solo mediante ataques ciberneticos y con computación cuántica se puede penetrar en la seguridad de los sistemas criptográficos (pag 47-49)

9. Soluciones.

9.1. Derechos ARCO y blockchain

Los **derechos ARCO son los derechos de acceso, rectificación, cancelación y oposición**. Con motivo del uso de esta tecnología se podrían llegar a ver vulnerados los derechos de rectificación, oposición y cencelación debido a la inmutabilidad de la red, así como su transparencia.

9.1.1. **Solución 1.** Cambiar datos y tener bifurcaciones

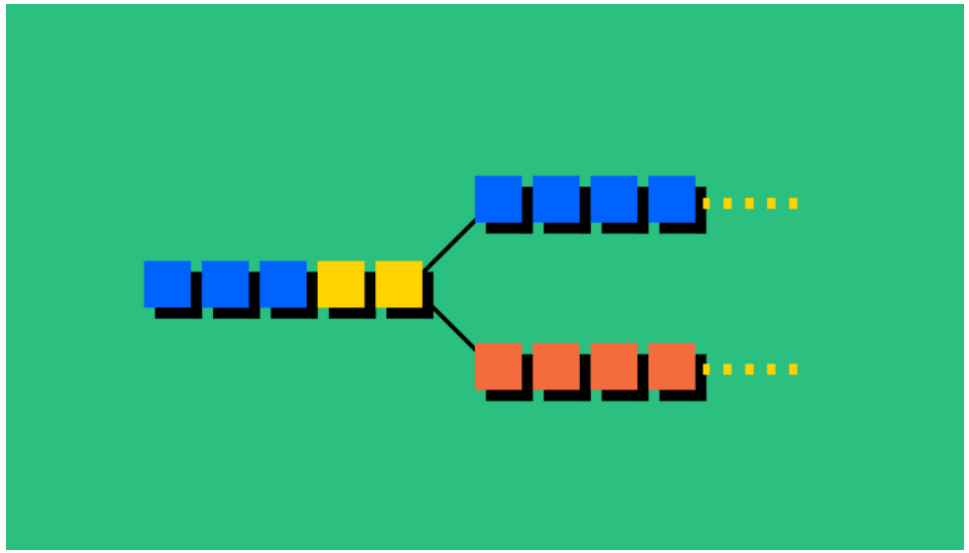


Imagen obtenida de (https://www.coinbase.com/es-LA/learn/crypto-basics/what-is-a-fork)

Los datos existentes en la cadena de bloques, si bien no son mutables por si mismos, si lo es cada uno de los nodos que lo integran, pudiendo mediante modificaciones **generar bifurcaciones en la red generando dos ramas distintas de información** durante un periodo de tiempo. Estas bifurcaciones son llamadas ***Fork*.**

(pag 51-52)

Tipos de fork

Gráfico 16. *Hard Fork*

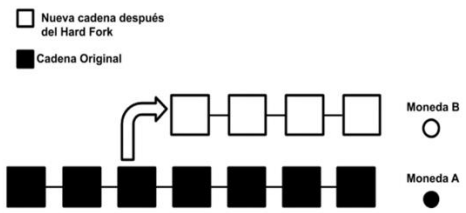
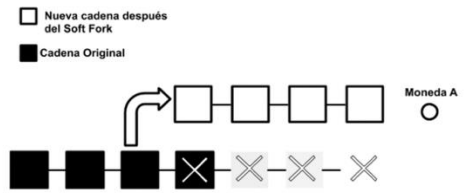
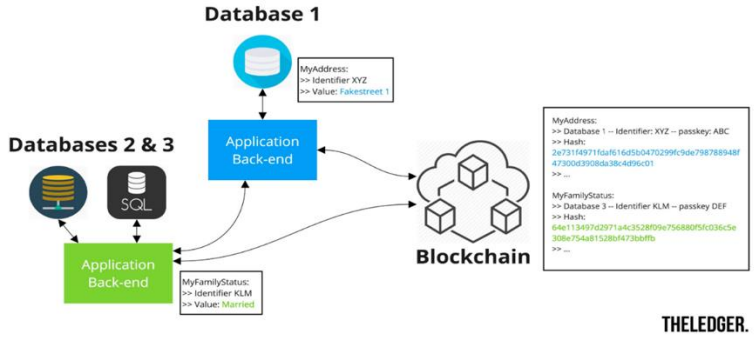


Gráfico 17. *Soft Fork*



1. **HARD FORK**. O bifurcación dura, se le llama de esta forma ya que desúés del cambio en la información ambas **cadenas siguen creciendo de forma independiente.** Estas ocurren cuando **una parte de la red opera con un conjunto de reglas distintas** al concenso general.
2. **SOFT FORK.** O bifurcación suave, esta consiste en un **cambio ligero a las reglas de concenso,** lo cual permite la operación de usuarios no actualizados con nuevas reglas. Esta bifurcaión **solo es temporal**, **mientras los mineros se actualizan**. (temporales mientras se actualizan las reglas)

9.2.2. Solución 2. Almacenar los datos personales fuera de la cadena y hash de la cadena.

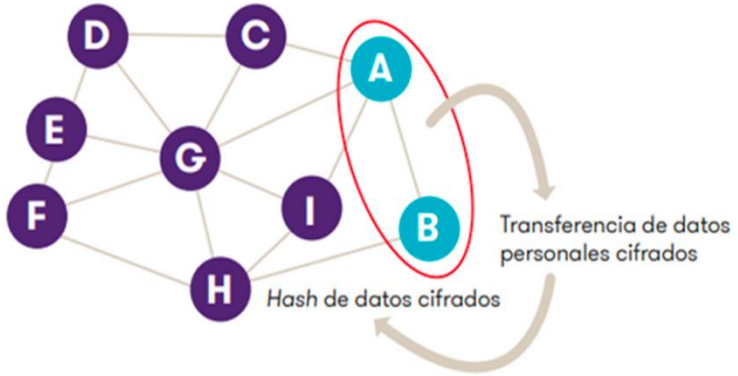


FUENTE: gráfico hecho por Van Humbeeck (2017).

En esta solución se crea una **nueva estructura fuera de la cadena** en la que se agregan referencias o identificadores convertidos a hash, para así no comprometer los datos personales. En este caso el blockchain, mediante un hash, es usado para verificar que la información personal no ha sido modificada. (pag 52-54)

Imágenes obtenidas de: Jersain Zadaming, Llamas Covarrubias, "Transparencia y protección de datos personales en la cadena de bloques (Blockchain)" en *Revista Estudios de derecho a la información* Vol. XI México Pág. 27-63, 2011.

9.2.3. **Solución 3.** Canal privado de comunicación y los hash



FUENTE: gráfico hecho por Grant Thornton (2018: 6).

Otra solución propuesta es la creación de **canales privados con datos cifrados**, en los cuales dos nodos tengan comunicación y mediante un canal privado se compartieran la información, almacenandla en un blockchain común al que solo ellos puedan acceder

9.3.4. **Solución 4.** Eliminar claves de cifrado

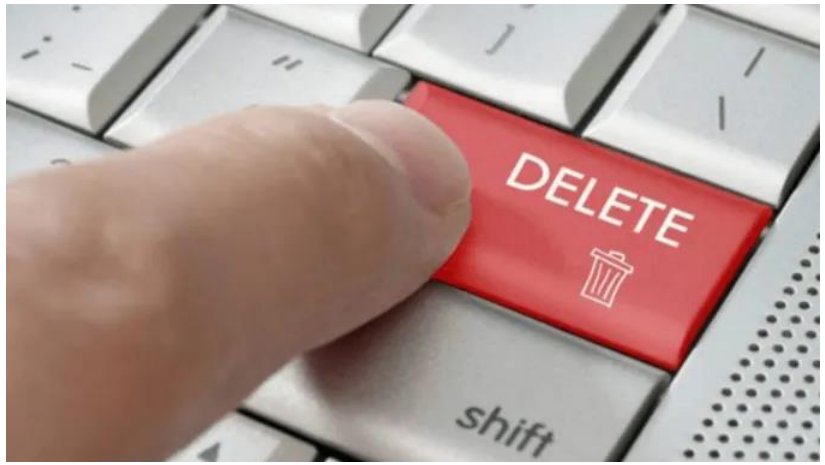


Imagen obtenida de (https://ecuadortoday.media/2019/11/08/aprende-a-borrar-tu-informacion-personal-que-aparece-en-internet/)

Eliminar las claves privadas para así no poder descifrar determinada información y con ello convertir la información en ilegible y anonimizada, así cumplir con los derechos de cancelación y oposición. De esta forma no se modificaría la base de datos, solo de cancelarían los datos protegidos (pag 54-56)

9.2. Transmisión de datos en redes de blockchain

9.2.1. Solución 1.

Imagen obtenida de (https://nacionmx.com/2018/04/01/recomendaciones-para-el-uso-adecuado-de-tecnologias-e-internet-en-ninos-y-jovenes/)

Usuarios responsables de su propia información personal, donde nadie controla o posee sus datos. Se plantea el caso de los blockchains privados en los que los **consorcios deben decidir con quien compartir los registros** distribuidos y así preservar la seguridad de la información. En caso de las blockchain públicas los participantes que ingresen información a la cadena deben estar correctamente informados de su funcionamiento, así como de la **libertad informática y el habeas data**, así como conciencia de la forma en la que se compartirá la información.

(pag 57-58)

10. Reflexiones finales.

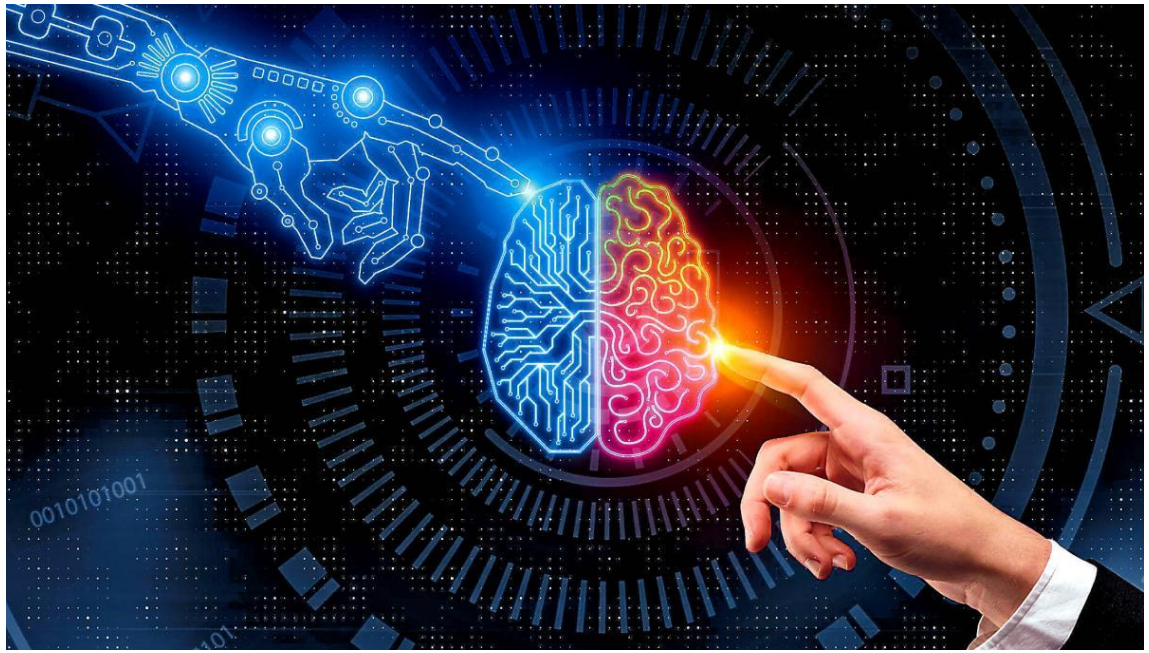


Imagen obtenida de: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/como-sera-la-evolucion-tecnologica-para-la-decada-2020-2030-444186)

Durante el transcurso de esta investigación pudimos **observar la forma en la que funciona blockchain, su surgimiento en una estructura monetaria y como su avance ha llegado a favorecer la transparencia**, así como la protección de datos personales. Es innegable que la tecnología **avanza** a pasos agigantados y con ella **nuevos riesgos respecto nuestra información personal**. Si bien blockchain representa una **herramienta orientada hacia la transparencia**, aún existen muchas áreas de oportunidad en las que esta tecnología puede mejorar. De igual forma debemos tener conciencia de lo necesario que se vuelve en nuestros días la **actualización de nuestra legislación** armonizando con legislación establecida en el ámbito internacional. El estudio de temas que convergen con el ámbito tecnológico se vuelve cada vez más **obligatorio y menos opcional.**

10.1. Claves teóricas

Keywords

Blockhchain, Consenso, Datos, Derechos, Información, Protección de datos ersonales, Sistema, Tecnología, Transparencia, Usuarios, Innovación,Normatividad, Transacciones

Ínice Analítico

10.2. Reflexiones prácticas

10.2.1 Marco Jurídico

Como se mencionó durante la exposición, en el marco jurídico internacional existe el **RGPD (Reglamento General de Protección de datos)** fue aprobado en 2016 y aplicado en 2018 por el Parlamento Europeo y el consejo, el cual regula el tratamiento que sealizan las personas, empresas y organizaciones de los datos personales relacionados con persona en la unión europea.Respecto al marco jurídico nacional tenemos los **artículos 6 y 16 constitucionales** en materia de protección dedatos personales, de ellos se desprende la **Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) de 2010 la cual no ha sido reformada y la Ley General de Protección de Datos Personales en Posesión de sujetos obligados (LGPDPPSO) de 2017 la cual tampoco ha sido reformada, razon por la cual ambas resultan insuficientes para atender a las necesidades de regulación de este tipo de tecnologías.**

10.2.2. Solicitud de información.

Huracán Otis, de categoría 5, causa daños históricos··· y no hay Fonden

El huracán "Otis" arrasó Acapulco con mayor fuerza que "Paulina" y afectó a otras regiones de Guerrero, como Tecpan de Galeana, de por sí golpeado recientemente por el fenómeno "Max". Todo ello, después de la extinción del fondo destinado a la mitigación de desastres.

Acapulco. Destrozos e incomunicación. Foto: AP Photo/Marco Ugarte

NACIONAL | Por Margena de la O | jueves, 26 de octubre de 2023 · 05:01

CHILPANCINGO, GRO. (Proceso).- El huracán que más se acercó al grado en el

MÁS LEÍDAS

NACIONAL
Frente frío 16 azotará con heladas y lluvias intensas de viernes a domingo a estas entidades

NACIONAL
Advierten al "mirrey" de Lomas de Angelópolis: Si no se presenta este viernes, será detenido

NACIONAL
FGR detiene a René Gavira por fraude de casi 20 mil mdp en Segalmex

DEPORTES
Otro revés a la Conade de Ana Guevara: Debe pagar 15 mdp a la esgrimista Paola Pliego

NACIONAL
Temblor sacude a la Ciudad de México antes de que se activara la alerta sísmica

Imagen obtenida de (https://www.proceso.com.mx/nacional/2023/10/26/huracan-otis-de-categoria-5-causa-danos-historicos-no-hay-fonden-317386.html)

En el marco del Seminario Le fue solicitada a la autoridad, **Secretaría de Hacienda y Crédito Público información respecto a la erogación de recusrsos que representaban el FONDEN**, esto mediante los siguentes cuestionamientos:

1. Siendo que este fideicomiso fue suprimido en julio de 2021 y transcurridos tres años de esto ¿Por qué temas específicos se han tenido que erogar los 17,984 millones de pesos que correspondían a este fondo?
2. ¿Qué desastres han ameritado que estos recursos sean erogados y a que dependencias han sido canalizados?
3. ¿Quién se ha encargado de operar la aplicación de estos recursos en cada caso?
4. ¿Qué acciones concretas de prevención se han financiado con estos recursos?
5. ¿En alguno de estos casos se han contratado seguros para la prevención de consecuencias derivadas de desastres naturales? Indíqueme en que parte de la Plataforma Nacional de Transparencia existen datos respecto estas erogaciones y en caso de no existir indíqueme algunas referencias respecto a este tema.

10.3. Postura epistémica.

Respecto a la fuente selecta consultada se presentaron algunos inconvenientes en la invetigación. Como primer punto podemos mencionar la **falta de estructura del artículo**, es entendible que al ser una fuente especializada existan algunos términos que se dan por entendidos. Sin embargo, **palabras esenciales somo hash, codificación y la clasificación de los sistemas me parece que merecen un apartado completo de desarrollo para entender su funcionamiento respecto al blockchain**. El segundo inconveniente que se presentó es que **muchos de los términos usados al principio de la lectura eran explicados casi al final de ella**, **dificultado** el recabar información, así como su **sintesis**. Fuera de estos dos inconvenientes es una fuente muy completa escita por un **especialista con propuestas innovadoras** a los problemas que hoy en dia presenta este sistema.

11. Fuente selecta.

Jersain Zadaming, Llamas Covarrubias, “Transparencia y protección de datos personales en la cadena de bloques (Blockchain)” en *Revista Estudios de derecho a la información* Vol. XI México Pág. 27-63, 2011.

12. Fuentes complementarias

A. Luhmann, Niklas, 1998, Sistemas sociales: lineamientos para una teoría general, 2a. ed., coord. de Javier Torres Nafarrate, trad. de Silvia Pappey Brunhilde Erker, Rubí, Barcelona-México-Santafé de Bogotá, Anthropos Editorial-Universidad Iberoamericana-Pontificia Universidad Javeriana, Centro Editorial Javeriano.

B. Quirós, Fernando, 2019, “Advierten que en México debe realizarse un estudio exhaustivo antes de implementar tecnología blockchain para votaciones”, CoinTelegraph en Español, disponible en https://es.cointelegraph.com/news/they-warn-that-in-mexico-an-exhaustive-study-must-be-carried out-before-implementing-blockchain-technology-for-voting.

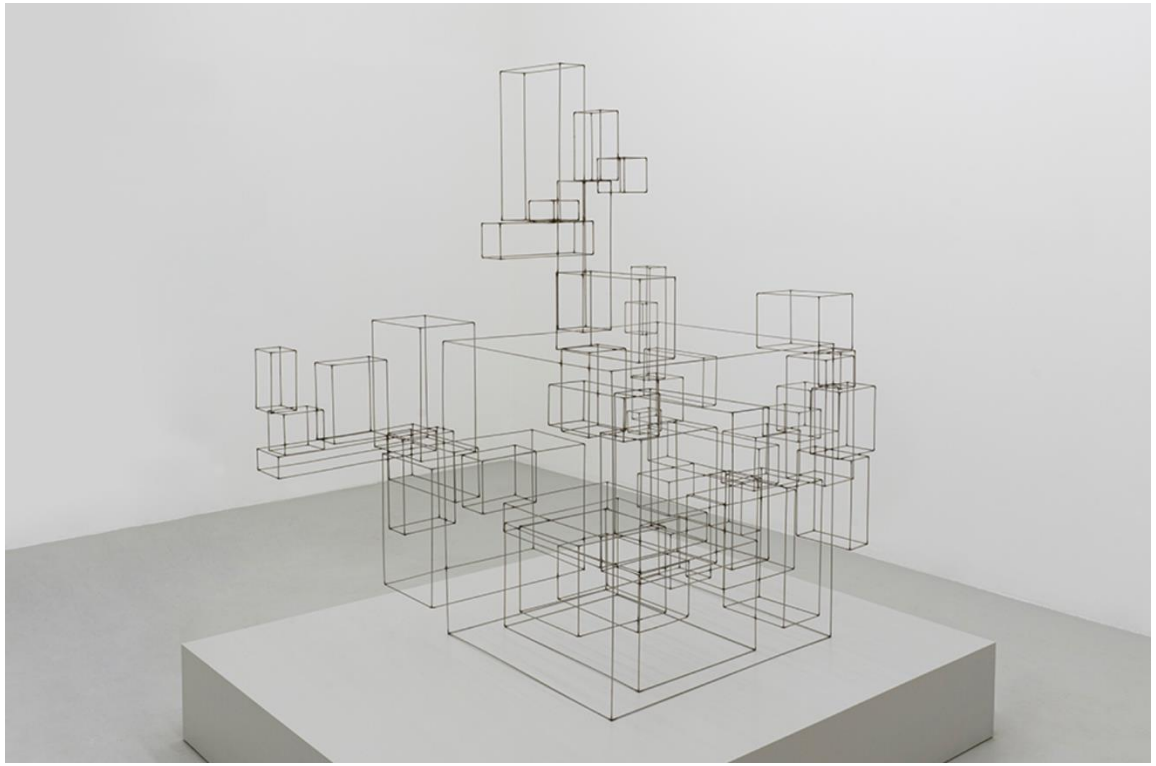
Lección de anatomía del Dr. Nicolaes Tulp, 1632

Rembrandt Harmenszoon van Rijn
168,5 centímetros de alto y 216,5 cm de ancho.
Se conserva en el Mauritshuis de La Haya
Perteneciente al siglo de oro Neerlandez

¡Gracias su atención, citar y difundir el presente material!

El presente trabajo se realizó en el **Seminario Constructivista** y el Aula jurídica virtual bajo estructura, fuentes y supervisión de la catedrática **Graciela Staines Vega**

SPALL II parte de la exposición Body Space Time 2018
Antony Gormley
Barra de acero inoxidable de sección cuadrada de 2 mm, 142 x 110 x 143 cm, 55,90 x 43,30 x 56,29 in. Galleria Continua, San Gimignano, Italy
Escultura contemporánea.



¡Gracias su atención, citar y difundir el presente material!

El presente trabajo se realizó en el **Seminario Constructivista** y el Aula jurídica virtual bajo estructura, fuentes y supervisión de la catedrática **Graciela Staines Vega**