Alliance for Daily Justice

Ciencia Jurídica y Sostenibilidad

Comunicación

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

Transparency and Personal Data Protection in Blockchain

Angel Sahid Martínez Gómez. Estudiante de la Facultad de Derecho de la UNAM, Seminario Constructivista para la Justicia Cotidiana.

Recibido: 1 de junio
Aceptado: 7 de junio
Publicado: 12 de junio de 2025

Resumen: Esta comunicación presenta una síntesis de «Transparencia y protección de datos personales en la cadena de bloques», donde se evalúa si blockchain, registro descentralizado e inmutable, puede equilibrar transparencia y privacidad. Se subraya su utilidad para auditorías públicas, pero se advierte que la inmutabilidad dificulta ejercer derechos ARCO y el derecho al olvido, además del riesgo de reidentificación. Se examinan cuatro soluciones: bifurcaciones para corregir registros, almacenamiento fuera de la cadena con hashes, canales cifrados y destrucción de claves privadas. Se concluye que, sin reformas a las leyes mexicanas de datos y lineamientos de gobernanza, la tecnología no garantiza por sí sola la protección de los derechos informativos.

Palabras clave: transparencia; blockchain; protección de datos; privacidad; derechos arco.

Abstract: This communication offers a concise synthesis of "Transparency and Personal-Data Protection in Blockchain", assessing whether the technology's decentralised, immutable ledger can balance transparency and privacy. Its value for public audits is recognised; yet immutability complicates the exercise of ARCO rights and the right to be forgotten, while re-identification threats persist. Four technical paths are reviewed: controlled forks to amend ledgers, off-chain storage of personal data anchored by hashes, encrypted channels that preserve traceability, and deliberate destruction of private keys. The conclusion is clear: absent targeted amendments to Mexican data-protection statutes and robust governance standards, blockchain alone cannot safeguard informational rights.

Keywords: Transparency; blockchain; Data protection; Privacy; ARCO rights

INTRODUCCIÓN Y HOJA DE RUTA

Hoja de ruta.

1. Genealogía.

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 de Derecho Informático (Comunidad de derecho informático más grande de Latinoamérica, fundada en 2009 Creada con la finalidad de generar interés y brindar un aporte significativo en el progreso del derecho informático y ciencias afines). Actualmente se desempeña como consultor y abogado especializado en derecho y las nuevas tecnologías de la información y comunicación

3. Marco epistémico.

a) ¿Qué derechos pueden proteger por la tecnología blockchain? Definir que es Blockchain
b) ¿Dónde surge esta tecnología?
c) ¿Cómo funciona blockchain?
d) ¿Por qué se dice que la información que contiene es inmutable?
e) ¿Qué ventajas nos ofrece respecto a otras tecnologías?
f) Mencionar los problemas que aún tiene esta tecnología
g) Explicar los tipos de Blockchain que existen
h) Mencionar las normas jurídicas que lo regulan nacional e internacionalmente
i) Definir que es la nube
j) Definir que es la anonimización y seudonimización
k) ¿Qué posibles soluciones le podemos dar a los problemas que presenta?

4. Introducción.

Uno de los principales retos de la información 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. Doctrinalmente existen clasificaciones de los derechos, las cuales ponen en primer lugar los derechos universales absolutos (vida y libertad), en segundo lugar, los derechos universales relativos (salud o educación), en tercero los derechos singulares absolutos (propiedad y derechos reales) y finalmente los derechos singulares relativos (derechos personales). 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.

4.1. Derechos protegidos.

La tecnología blockchain puede proteger un gran número de derechos establecidos en la legislación internacional, tal es el caso de los derechos ARCO (acceso, rectificación, cancelación y oposición), habeas data y derecho al olvido, derecho a la intimidad, privacidad, anonimato, a la verdad, a encriptar, a la auditoría y a la gobernanza electrónica. Este avance tecnológico representa una intersección muy relevante entre el derecho y la tecnología ya que acarrea consigo principios de autodeterminación informativa, de privacidad y transparencia inmutable ante la sociedad.

5. Blockchain

5.1. 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.

5.2. 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. En su funcionamiento más primigenio, esta permite que los usuarios registren transacciones en un libro

mayor, el cual es compartido en una comunidad, de tal modo que el funcionamiento de esta red no permite que las transacciones registradas no sean modificadas una vez han sido publicadas. 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. Todo 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.

5.3. Conceptos relevantes
5.3.1. Sistemas centralizados y descentralizados.
Aquellos dependen de un ente central son centralizados, mientras que aquellos que dependen de un ente central, todos sus componentes se conectan entre ellos, pero si uno cae no afecta el sistema

5.3.2. Cifrado.
Transformar una información para protegerla y 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. Es ocultar información a través de un algoritmo, fórmulas matemáticas para cuando alguien distinto al receptor consigue la información este no pueda descifrar el mensaje. SHA-256 uno de los programas de cifrado más completos en la actualidad. En el cifrado, la información solo puede ser codificada, sin embargo, el código generado no puede ser usado para descifrar la información

5.4. Funcionamiento general
5.4.1. Definición.

"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" 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.

5.4.2. Partes que lo integran 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 imposible de resolver, la única forma de resolverlo es mediante prueba y error. (esta prueba y error se le llama minería, computadoras que están probando para resolver estas pruebas de trabajo) 10 minutos para la resolución del problema.

5.4.3. Actualización y sincronización.
Las transacciones son registradas mediante un mecanismo de concenso, existen muchos mecanismos de concenso, sin embargo 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. Protocolo de concenso es la forma en la que se ponen de acuerdo los mineros para llegar a un acuerdo de mayoría y poder sincronzar la red Blockchain. Cada uno de los bloques de la cadena es generado cada 10 minutos aproximandamente, tiempo en que los mineros tienen que cambiar el NONCE produciendo los hash de salida en el

cifrado SHA-256. Una vez generado el hash es enviado los demás mineros para su aceptación y validación

5.4.4. Adición de bloques. Estos son agregados en bloques unidos con una cadena criptográfica, lo cual brinda inmutabilidad a la información pues todos los bloques están unidos, del primero al último. 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.

5.4.5. Sistema asimétrico de cifrado. Otro punto importante a mencionar es que esta tecnología usa un sistema de clave pública o asimetrico de cifrado. Este sistema funciona de la siguente forma: secuenta 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 descrifrará 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.

5.4.6. Inmutabilidad de blockchain. Al estar conectados todos los bloques existen marcadores específicos para la información que impiden su manipulación, al ser un sistema descentralizado los usuarios en concenso expulsarían la información inválida o apócrifa

5.4.7. Permanencia en la red. Este es un sistema autopioético “sistema que dispone estructuras y procesos propios puede coordinar con estas formas del fortalecimineto de selección todos los elementos que produce y reproduce”, en el cual se generan bloques de manera constante al exixtir una recompensa a los usuarios al resolver las pruebas de trabajo, en su funcionamiento primigeneo la recompensa obtenida eran bitcoins.
6.4.8. Transparencia. 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.

6. Transparencia y blockchain
6.1. Ventajas y desventaja.
Gracias a su transparencia y descentralización, blockchain genera redes abiertas que funcionan en multiples dispositivos. 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. La información en la cadena se mantiene siempre a salvo y los metadatos y otra información sobre las transacciones es observable por los usuarios. Una de las grandes ventajas con que cuenta este sistema es que los registros son almacenados de forma sequencial con marcas de tiempo y autenticación en cada modificación, dando pie así a que sea el medio idoneo no solo para contener información financiera, sino todo tipo de información. Esta tecnología tiene el potencial para servir como pilar para albergar los registros gubernamentales, sin embargo es importante mencionar que 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 7.2. Problemas de blockchain.

6.2.1. Problema 1.
6.2.1.1. Tipos de Blockchain.
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 usuario 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.

6.2.1.2. Falibilidad
En los sistemas privados 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 sinerhia 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.

6.2.2. Problema 2.
Otro problema que surge con esta tecnología es su transparencia per se, que aunque es una de las ventajas más representativas que tiene, también representa un riesgo para los intereses jurpidicos 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 existen distintos tipos de clasificaciones de blockchain y derivado de la situación en que se quiera ocupar, debe seleccionarse entre público, privado e hibrida.

7.Protección de datos personales y blockchain
7.1. Marco jurídico internacional.
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.

7.2 Marco jurídico Nacional. Por otra parte, nuesro país cuenta los con los artículos 6 y 16 constitucionales en materia de protección de datos personales, de ellos se desprende la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de sujetos obligados (LGPDPPSO). Ambas leyes son incompatibles con la aplicación de la tecnología blockchain, sin embargo reconocen y aceptan el sistema de nube infomática.

7.2.1 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”.

7.2.2. Tipos de servicio de nube.
1. Software as a Service (SaaS) servicio que puede ser usado sin la necesidad de descargar un software, ejemplo de este es Google Drive. 2. Platform as a Service (PaaS) plataforma en la que se permite desarrolar aplicaciones y ofrecer servicios sin necesidad de instalar un software, ejemplo de este es Google App Engine. 3. Infrastructure as a Service (IaaS) servicio online que permite pagar por recursos de hardware, ejemplo de este es Amazon Web Services, el cual ofrece servicios de procesamiento. Derivado de la definición que nos ofrece nuestra legilación podemos concluir que esta permite la entrada de Blockchain as a Service, es decir que permitiría la entrada de blockchain como un servicio de nube que funciona sin la necesidad de descargar un software.

7.3. Asuntos por considerar en la cadena de bloques.
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 anaonimizados, siendo que de esta forma no podría aplicarsele el reglamento General de Protección de datos al no considerarse en nuestro país como información personal por no ser concerniente a una persona identificada o identificable al no poderse conocer su identidad de manera directa.

7.3.1. Tratamiento en Europa.

En europa datos personales se considera a toda información sobre una persona física identificada o identificable. Persona física identificable se considera 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".Esta legilación también 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.

7.3.2 Anonimización. Podemos definir la anonimización como las técnicas que se emplean en datos personales con el fin de ser disociados los datos sin la posibilidad de identificación a las personas de forma irreversible, por ello sus datos en ningun caso pueden tener vinculo con un dato que pueda identificar a la persona. La seudonimización hace que los datos personales no se puedan identificar a una persona, sin utilizar información adicional, por ello es reversible, mientras que en este procedimiento se reemplazan canpos de información personar mediante diversos medios pero se mantienen datos adicionales que pueden identificar a personas.

7.3.3. 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 atributos.

7.3.4. Datos seudonomizados. 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, LGPDPPSO). De su interpretación prodemos concluir que el proceso de disociación es un proceso realmente de anonimización.

7.4. Codificación, cifrado y hash. CODIFICACIÓN. Su finalidad es mantener la usabilidad de los datos y puede revertirse usando el mismo algoritmo sin necesidad del uso de una clave.CIFRADO. Su finalidad es mantener la

confidencialidad de los datos y requiere una clave para descifrar la infoormación. Su accióne es irreversible, sin embargo al ser identificable el titular de la clave se vuelve in método seudonimizado ya que los datos no se convierten irreversiblemente a anonimos.HASH. Sirve para validar la integridad del contenido y detectar sus modificaciones a través de cambios en la salida del hash, es una función matemática que rebibe un valos de entrada con un valor de salida fijo. Además de ello sus resultados si se convierten de forma casi irreversible en anónimos, pues solo mediante ataques de fuerza bruta y con computación cuántica se puede penetrar en la seguridad de los sistemas criptográficos.

8. Soluciones.

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.

8.1. Derechos ARCO y blockchain

8.1.1. Solución 1. Cambiar datos y tener bifurcaciones 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 ramaa distintas de información durante un periodo de tiempo. Estas bifurcaciones son llamadas Fork. Tipos de fork

1. HARD FORK. O bifurcacióndura, 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).

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

8.2.3. Solución 3. Canal privado de comunicación y los hash.

Otra solución propuesta es la creación de canales privados con datos cifrados, los cuales funcionarían de la siguente forma: 1. Dos nodos crean un canal privado 2. Los datos personales solo se comparten entre estos nodos en canal privado 3. El hash privado se almacena en un blickchain común, provocando que los demás nodos puedan conocer el intercambio de información pero no el contenido.

8.3.4. Solución 4. Eliminar claves de cifrado. 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.

8.2. Transmisión de datos en redes de blockchain

8.2.1. Solución 1. 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.

9. Reflexiones finales. 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 consciente 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.

9.1. Claves teóricas
9.2. Reflexiones prácticas
9.2.1 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.

9.2.2. Solicitud de información. Le fue solicitada a la autoridad, Secretarpia de Hacienda y Crédito Público información respecto a la erogación de recusrsos que representaban el FONDEN, esto mediante los siguentes cuestionamientos: 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 17,984.7 millones de pesos que correspondían a este fondo? ¿Qué desastres han ameritado que estos recursos sean erogados y a que dependencias han sido canalizados? ¿Quién se ha encargado de operar la aplicación de estos recursos en cada caso? ¿Qué acciones concretas de prevención se han financiado con estos recursos? ¿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.

9.3. Postura epistémica. Respecto a la fuente selecta consultada se presentaron algunos inconvenientes en la invetigación. Como primer punto podemos mencionar la falta de estructura de el 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.