

Blockchains y otras formas de contabilidad distribuida (DLT) y su impacto en la protección de los datos personales



Dr. Oscar Raúl Puccinelli



XVII ENCUENTRO
IBEROAMERICANO
de Protección de Datos
Y 4^{to} FORO INTERNACIONAL



La evolución de los protocolos de internet hasta el BTC/XBT

De todos los protocolos utilizados por la industria de internet para transmitir diversos tipos de contenidos, faltaba un protocolo para transmitir dinero nativo digital (no Paypal que es dinero legacy de la industria bancaria).

Algunos protocolos:

TCP: (transmission control protocol) de control de transmisión.

IP: (internet protocol) de internet.

HTTP: de transferencia de hipertexto (acceso a las páginas web)

FTP: (file transfer protocol) de transferencia de archivos.

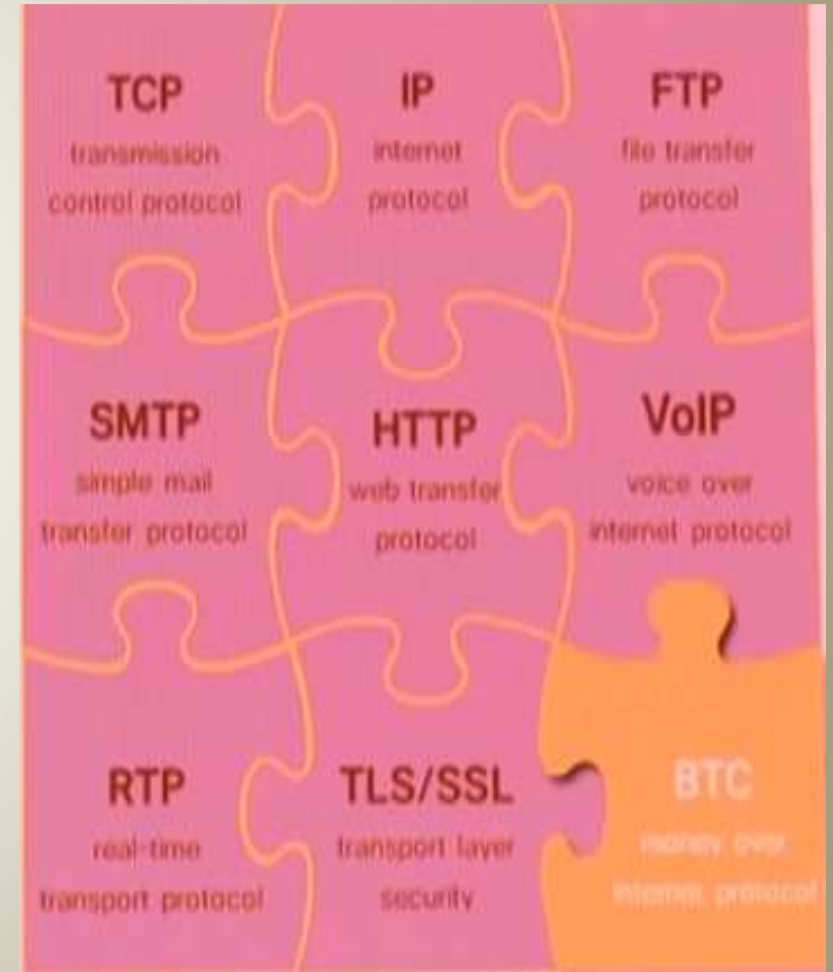
POP: (post office protocol), IMAP (Internet message Access protocol) y SMTP: (simple mail transfer protocol), de email.

VoiP: protocolo para transmitir audios.

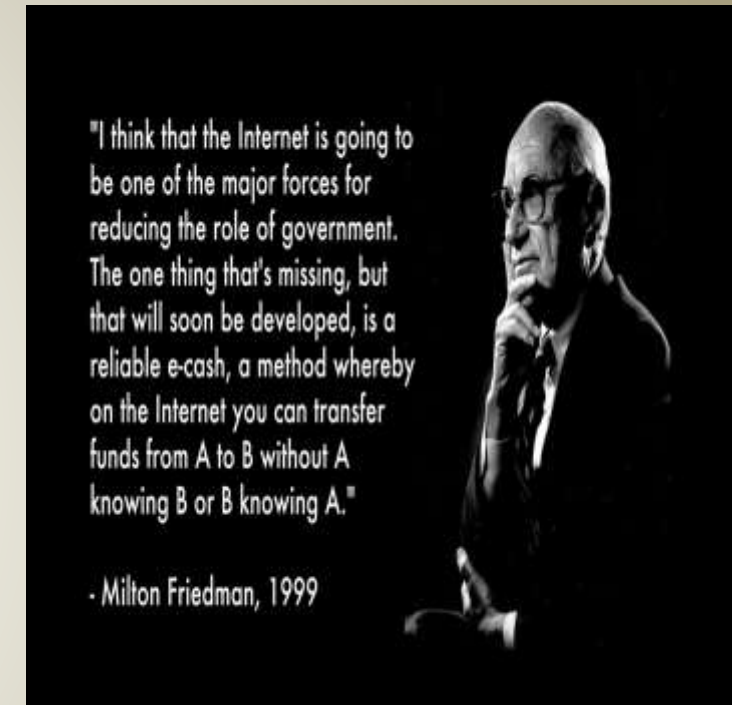
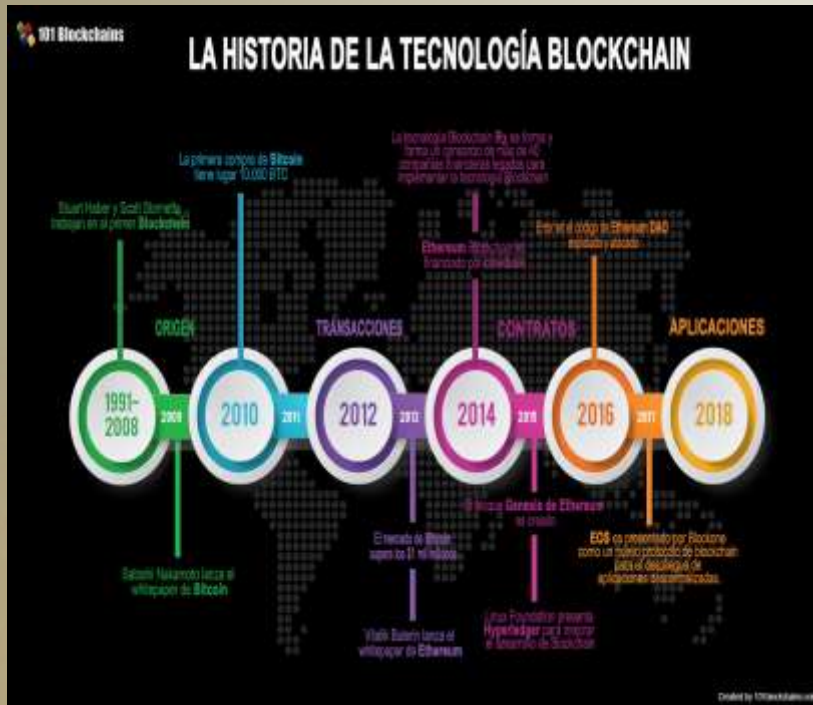
RTP: (real time transfer protocol)

TLS/SSL: (transport layer security)

BTC/XBT: es un protocolo y red P2P que se utiliza como criptomoneda



Las blockchains de Stuart Haber y W. Scott Stornetta (1991-1992) y la predicción de Milton Friedman (1999)



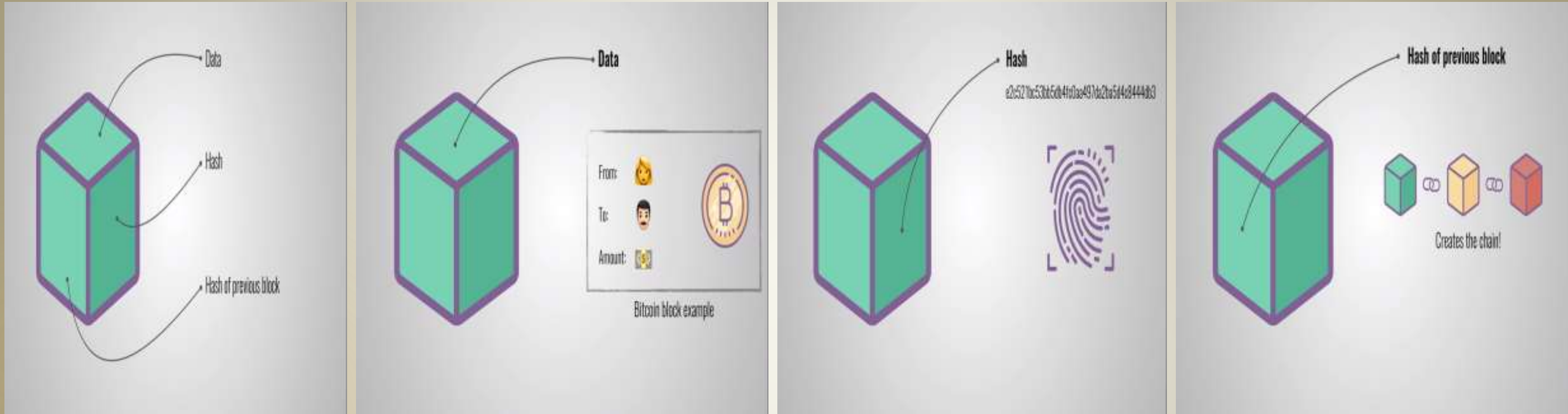
La tecnología blockchain fue descrita en 1991 por **Stuart Haber y W. Scott Stornetta** introdujeron la cadena de bloques con seguridad criptográfica para almacenar los documentos con sello de tiempo. En 1992 se incorporaron al diseño los árboles Merkle, lo que lo hizo más eficiente al permitir que varios documentos se reunieran en un solo bloque. Esta tecnología no se utilizó y la patente caducó en 2004.

Satoshi Nakamoto y Bitcoin (2008 – 2009)



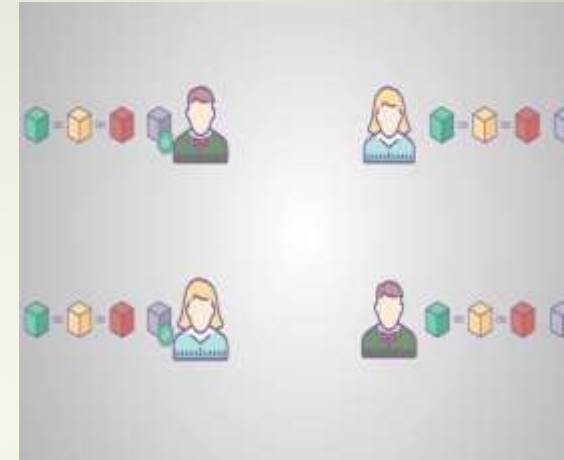
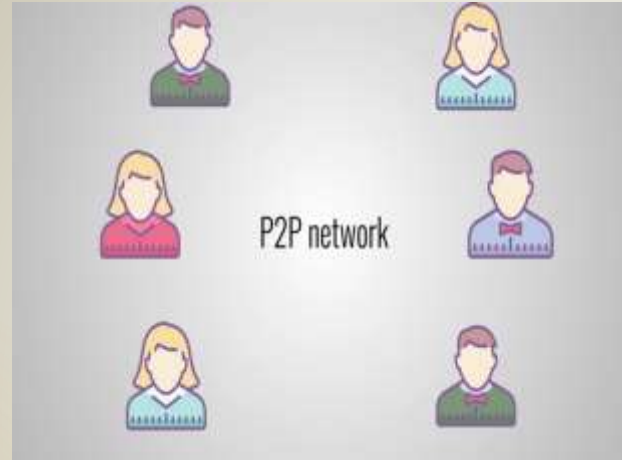
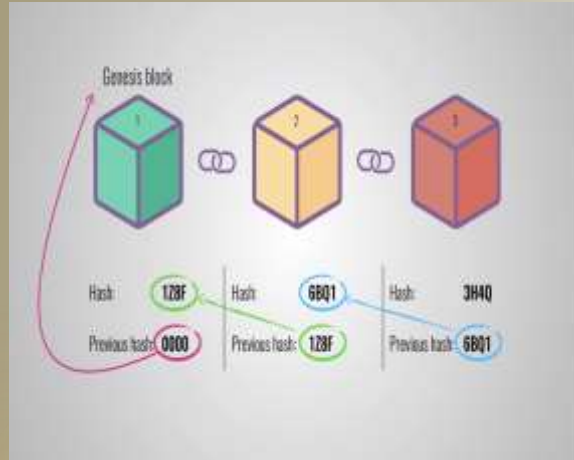
Satoshi Nakamoto es un seudónimo de una persona o un grupo de personas que desarrolló Bitcoin, escribió su libro blanco y el artículo "Bitcoin: un sistema de efectivo electrónico punto a punto" en octubre del 2008 y lanzó el primer software para la red Bitcoin en enero del 2009. Se especula que Satoshi Nakamoto puede ser Nick Szabo, desarrollador y primer receptor de transacciones de Bitcoin, Hal Finney, Craig Steven Wright, un científico y empresario australiano. Satoshi dejó de trabajar en el proyecto Bitcoin en el 2011 y desapareció de la vida pública. Otras criptomonedas se han lanzado al mercado, como Ethereum y Libra, de Facebook.

Qué son y cómo funcionan las *blockchains*

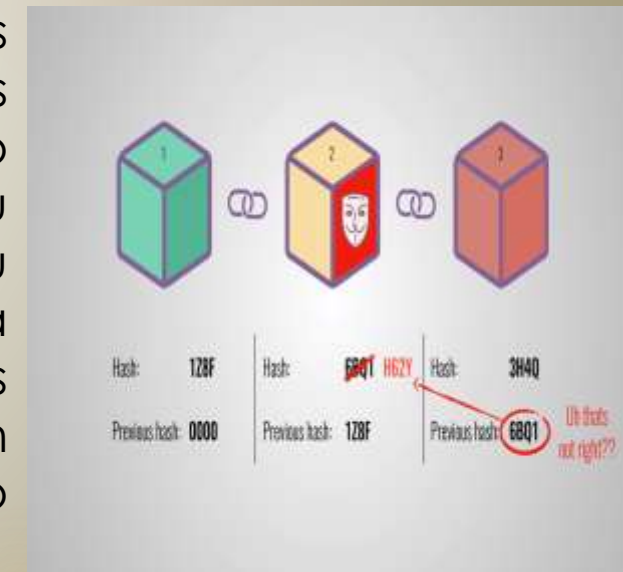


Una blockchain es una base de datos descentralizada, cuya información relativa a diversas transacciones se agrupa en bloques a los que se les añaden metadatos relativos a otro bloque de la cadena anterior en una línea temporal. Gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser editada modificando todos los bloques posteriores (hay una hoja de cálculo que se ha replicado miles o millones de veces en una red de ordenadores que actualiza de forma regular y simultánea esa hoja de cálculo). Cada vez que un bloque es completado el mismo es añadido a la cadena, y añadido un cambio, no puede ser editado o borrado, solo rectificado con otro cambio posterior. Además de las transacciones, los bloques incluyen otros elementos, como el hash del bloque anterior (una especie de huella dactilar en versión digital del mismo) y una marca de tiempo (día, hora, fecha).

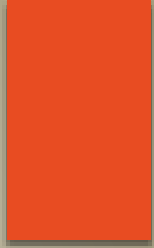
Qué son y cómo funcionan las *blockchains*



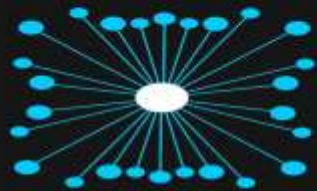
La misma base de datos se replica en cientos, miles o millones de ordenadores (también llamados nodos), lo que asegura su inmutabilidad, de modo que al no haber una localización central para su gestión se dificulta muy considerablemente su hackeo, se facilita su verificación y se distribuye la confianza sobre la veracidad de esos datos en todos los ordenadores de la red y no en una ubicación central, de modo que rompe con el modelo tradicional de bases de datos centralizadas.



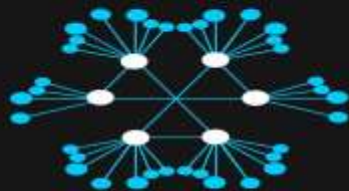
Qué son y cómo funcionan las *blockchains*



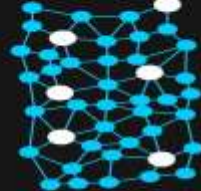
Red centralizada vs descentralizada vs red distribuida: Visión general



Red centralizada
Todos los nodos están conectados bajo una sola autoridad.



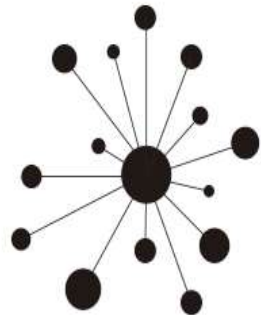
Red descentralizada
Sin servidor de autoridad único que controle los nodos, todos tienen entidades individuales.



Red distribuida
Cada nodo es independiente e interconectado entre sí.

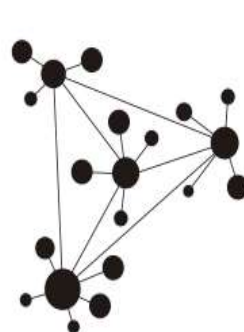
101 Blockchains
Created by COINTEGRATION.COM

RED CENTRALIZADA (banco)



Todo pasa por un nexo central

RED DESCENTRALIZADA (bitcoin)



Hay varios nodos principales interconectados

RED DISTRIBUIDA (blockchain)



La mayoría de usuarios están conectados entre sí (p2p)

¿Cómo se distribuyen los 10.253 nodos de bitcoin activos por todo el mundo?

15 países con más nodos activos

País	Nodos	País	Nodos	País	Nodos
1 Estados Unidos	2.490 (24,3%)	6 Canadá	389 (3,7%)	11 Singapur	173 (1,7%)
2 Alemania	1.815 (17,7%)	7 Reino Unido	367 (3,6%)	12 Corea del Sur	157 (1,5%)
3 China	847 (8,3%)	8 n/d	348 (3,4%)	13 Hong Kong	152 (1,5%)
4 Francia	675 (6,6%)	9 Rusia	345 (3,4%)	14 Suiza	148 (1,4%)
5 Países Bajos	489 (4,8%)	10 Japón	214 (2%)	15 Australia	124 (1,2%)



Nota: datos del 21 de mayo de 2018
Fuente: Bitnodes

INSIDER PRD

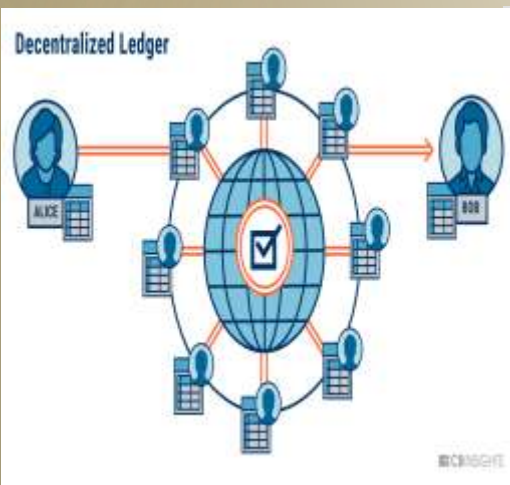
Hasta la fecha, hay 10.253 nodos de bitcoin repartidos por todo el mundo, un quinto de los cuales se encuentran en Estados Unidos. España ocupa el puesto número 18 con 77 nodos.

Un nodo es cualquier ordenador que participe en la red bitcoin y utilice un protocolo p2p que permite a los nodos comunicarse entre ellos en la red y distribuir información sobre transacciones y bloques. Todos los nodos son los que componen la red del blockchain.

Plus, cualquier usuario de cualquier parte del mundo puede configurar su propio nodo tan solo con un ordenador que cuente con un procesador potente y conexión a

Tipos de nodos y tipos de cadenas de bloques (European Union Blockchain Observatory and Forum)

Nodos de validación (mineros): resuelven un conjunto de problemas criptográficos antes de incorporar un nuevo bloque a la cadena, siguiendo las reglas especificadas por el algoritmo de consenso de la cadena. Por su tarea (minería de datos) reciben una compensación.



Nodos de participación: almacenan copias sincronizadas de la información y pueden almacenar toda la información de la cadena o solo una parte según la capacidad de almacenamiento en el disco duro.

Si un usuario se conecta a un nodo de participación puede añadir datos a la cadena, pero esa transacción deberá ser validada por un nodo de validación.

Tipos de nodos y tipos de cadenas de bloques (European Union Blockchain Observatory and Forum)

Tipos de Cadenas de bloques

Blockchain públicas

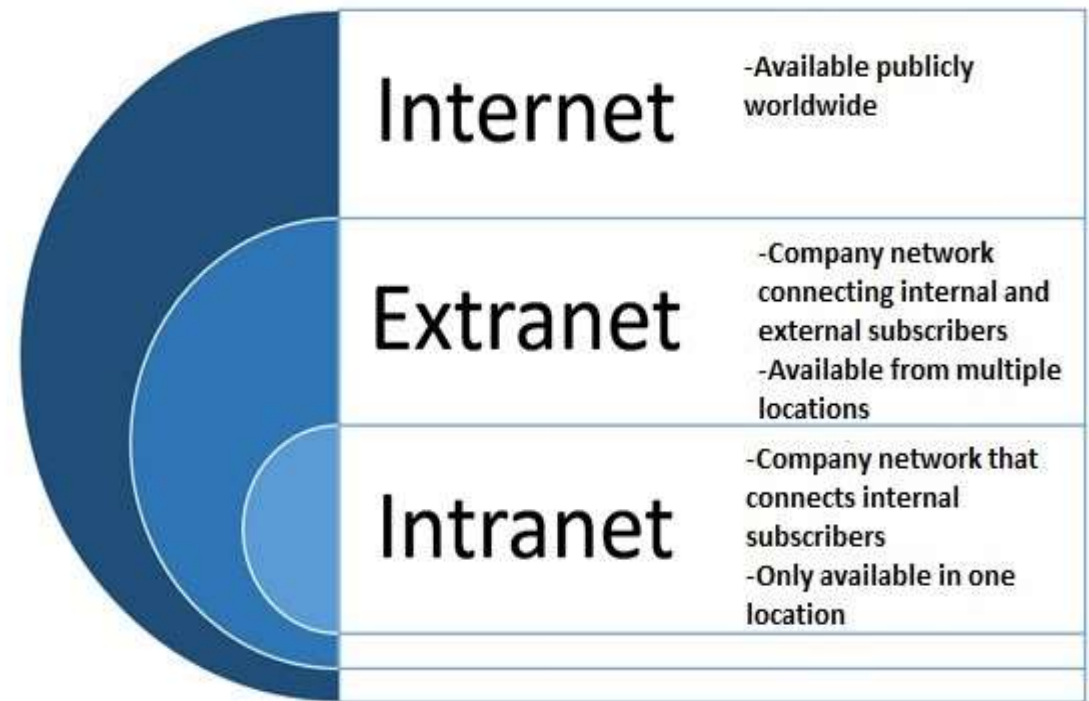
Son como Internet (abiertas a todo el mundo),

Blockchain públicas con permisos

Son como una gran extranet (tienen un punto de partida privado pero están abiertas al exterior en gran parte)

Blockchain privadas

Son como una intranet (solo para los que tengan permiso para entrar).



Tipos de nodos y tipos de cadenas de bloques (European Union Blockchain Observatory and Forum)

Tipos de Cadenas de bloques

Blockchains públicas sin permisos (Bitcoin o Ethereum)

No exigen requisitos a los usuarios para convertirse en un nodo o en parte de la red. Solo hay que instalar el software cliente (casi siempre de código abierto) y descargar una copia completa de la cadena de bloques. Desde ahí como nodo completo se puede participar en almacenamiento y/o agregación de información (participación o validación).

El contenido de una blockchain pública es transparente y visible para todos los usuarios (y en algunos casos no usuarios) pues no se exigen permisos o invitaciones para acceder y participar.



Tipos de nodos y tipos de cadenas de bloques (European Union Blockchain Observatory and Forum)

Tipos de cadenas de bloques

Blockchains privadas (WeTrade, Enerchain)

Requieren una invitación previa para acceder, comprobar y añadir transacciones. La validación puede hacerla: a) quien crea la red; b) un grupo limitado de creadores o c) ciertas reglas preestablecidas.

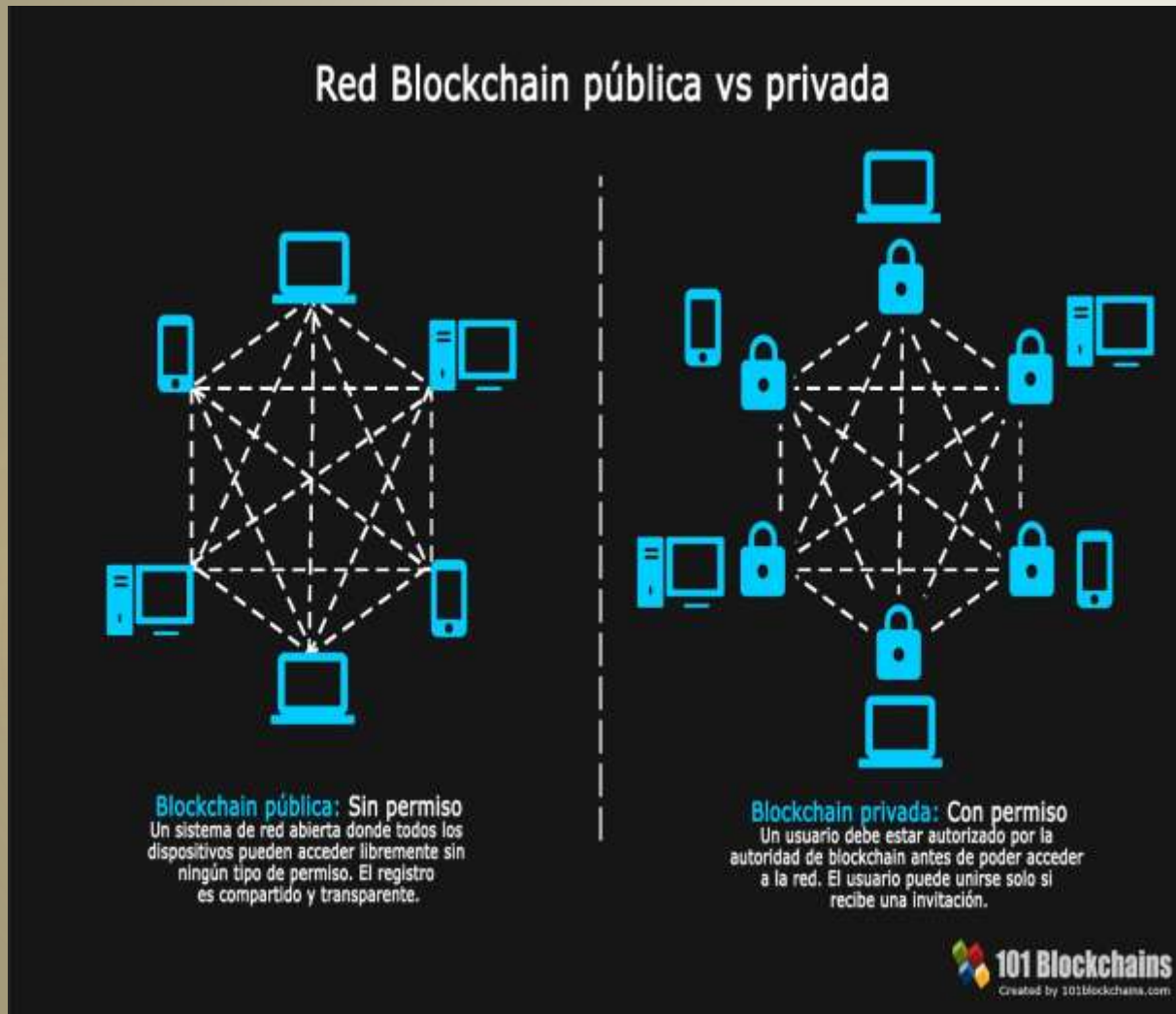
Se reducen los procesos de funcionamiento y el riesgo de sufrir ciberataques y brechas de seguridad. El proceso de validación de transacciones es más rápido que el de las redes públicas, y a su vez consumen menos energía.

we.trade es una empresa de 9 bancos europeos (Deutsche Bank, HSBC, KBC, Natixis, Nordea, Rabobank, Santander, Société Générale y UniCredit), disponible en 11 países europeos, aunque admite la incorporación de otros mercados del mundo. Su plataforma basada en la blockchain de IBM, busca simplificar las operaciones financieras, gestionar, hacer el seguimiento y asegurar las operaciones, ofreciendo a los clientes una interfaz sencilla que aprovecha los contratos inteligentes y simplifica las operaciones transfronterizas.

Enerchain es un consorcio de energéticas europeas que utiliza la tecnología blockchain para operaciones de compraventa en los mercados mayoristas de energía y gas natural.

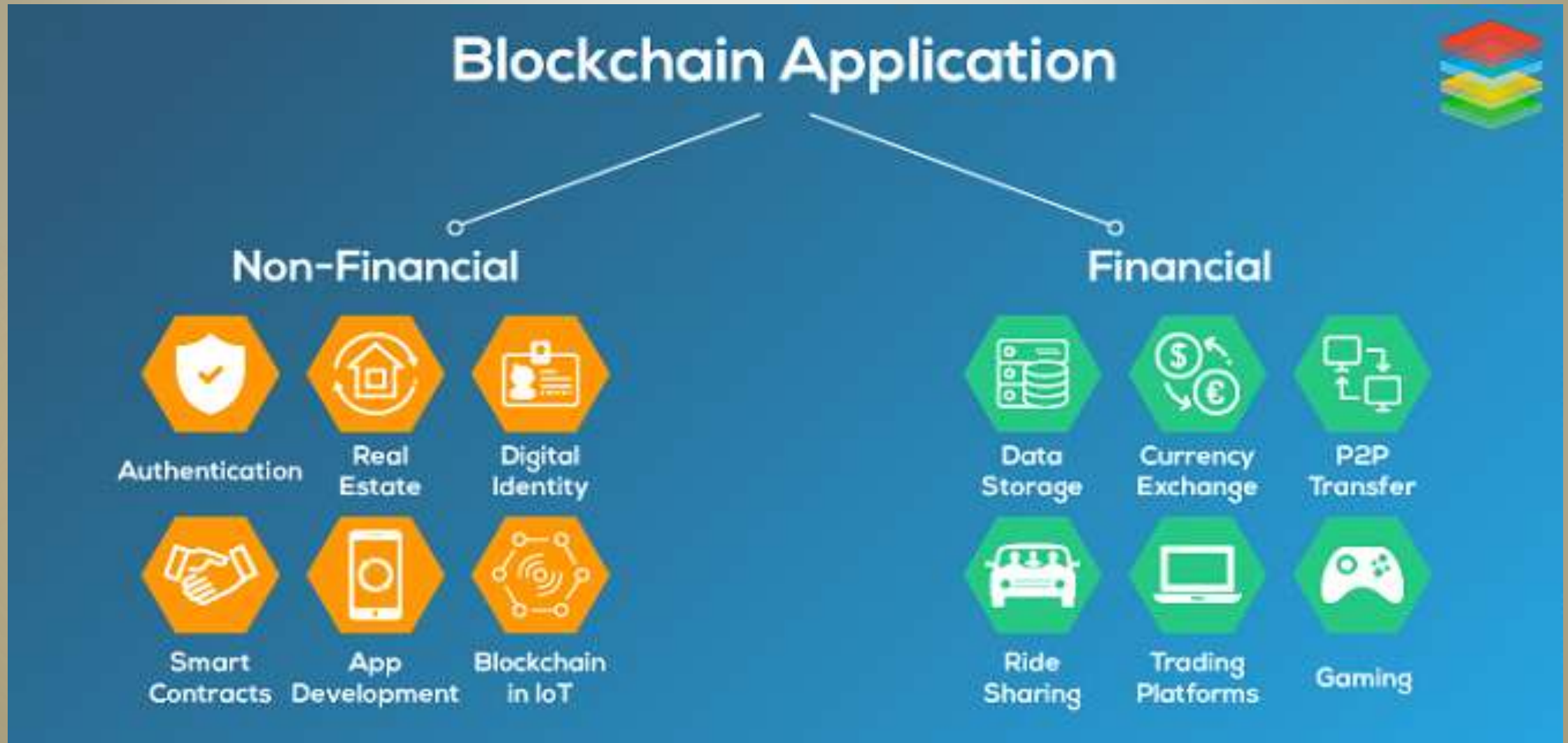


Blockchains públicas vs. privadas

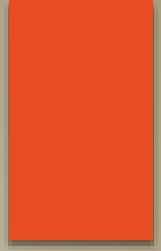


	Blockchain Pública	Blockchain Privada
Acceso	Lectura y escritura de carácter abierto o con permisos	Lectura y escritura con permisos
Velocidad	Más lenta	Más rápida
Seguridad	Prueba de trabajo, de participación y pre - aprobación	Pre - aprobación de los participantes
Identidad	Anónima/Seudónima	Identidades conocidas
Tipo de activos	Activos nativos	Cualquier activo

Diversas posibilidades de aplicación



Diversas posibilidades de aplicación



Consorcio R3: de entidades financieras para aprovechar la cadena en los sistemas financieros tradicionales.

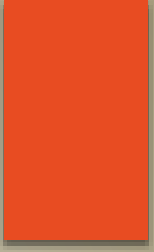
Registro de propiedades: **Japón** ha iniciado un proyecto para unificar todo el registro de propiedades urbanas y rústicas con tecnología de cadena de bloques, lo que permitiría contar con una base de datos abierta en la que se pudieran consultar los datos de las 230 millones de fincas y 50 millones de edificios existentes. **Dubai** planea algo muy parecido.

Pagos en el mundo real: la startup **TenX** creó una tarjeta prepaga recargable con distintas criptodivisas para pagar en cualquier sitio como si tuviera dinero convencional, sin importar si ese establecimiento acepta o no este tipo de monedas virtuales.

Almacenamiento en la nube: normalmente estos servicios están centralizados en un proveedor específico, pero la empresa **Storj** quiere descentralizar este servicio para mejorar la seguridad y reducir la dependencia de ese proveedor de almacenamiento.

Identidad digital: La cadena de bloques podría proporcionar un sistema único para lograr validar identidades de forma irrefutable, segura e inmutable. Hay muchas empresas desarrollando servicios en este ámbito.

Diversas posibilidades de aplicación



Carsharing: la empresa **EY**, subsidiaria de Ernst & Young Global Ltd está desarrollando un sistema que permite a empresas o grupos de personas acceder a un servicio para compartir coches de forma sencilla. **Tesseract** permitiría registrar quién es el propietario del vehículo, el usuario de ese vehículo y generar los costes basados en el seguro y otras transacciones en este tipo de servicios.

Música: La distribución musical se revolucionaría al implantar la cadena de bloques para gestionar su reproducción y distribución. **Spotify** está apostando por su propia cadena de bloques.

Servicios públicos/gubernamentales: con una transparencia absoluta en áreas múltiples: gestión de licencias, transacciones, eventos, movimiento de recursos y pagos, gestión de propiedades, gestión de identidades, etc.

El robo masivo de datos en Equifax provocó propuestas de sustitución de los números de la seguridad social con un sistema basado en la cadena de bloques. Hay iniciativas incluso para "descentralizar el gobierno", y "Bitnation" es uno de esos proyectos.

Seguridad social y sanidad: para registrar todo tipo de historiales médicos.

Gestión de autorías: **Ascribe** es una plataforma que trata de ayudar a creadores y artistas a atribuirse la autoría de sus trabajos a través de la cadena de bloques. Plataformas como **Bitproof**, **Blockai** y **Stampery** permiten generar tiendas para comprar trabajos originales.

Diversas possibilidades de aplicação



Brasil: Proyecto de ley nº 3443/19

**“Prestação Digital dos Serviços Públicos na Administração Pública – Governo Digital”.
(presentado en la Cámara de Diputados el 11/06/19)**

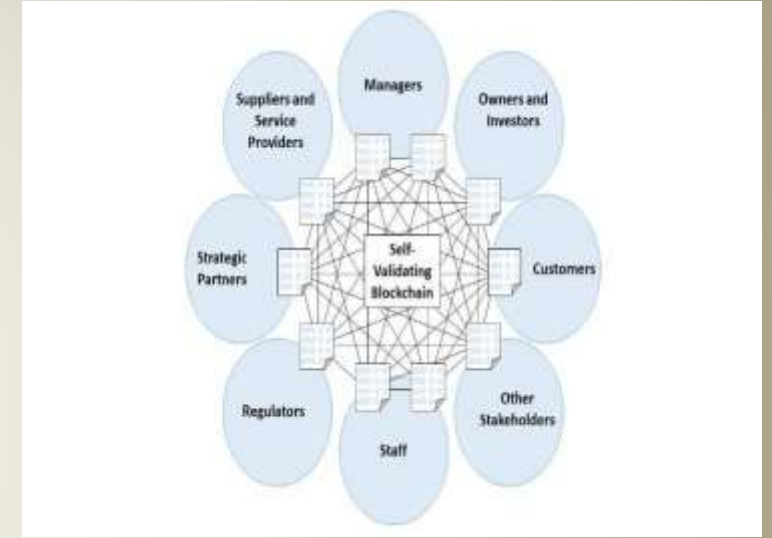
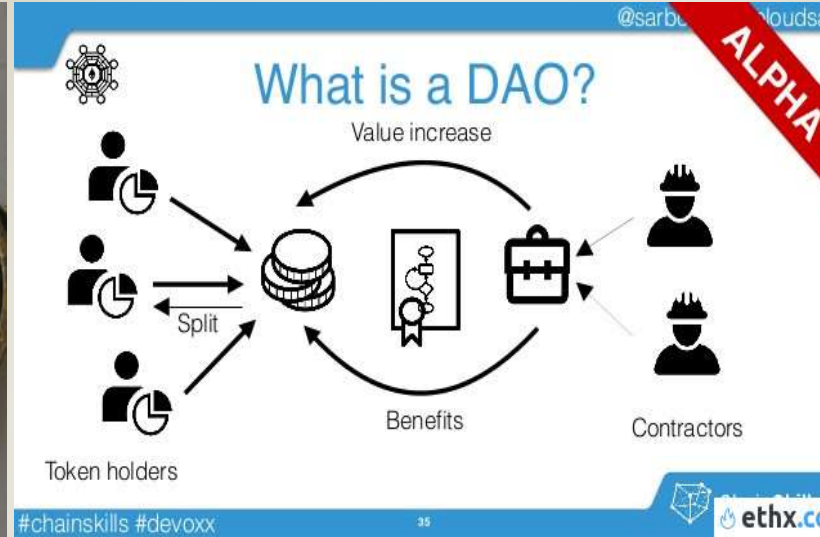
Art. 4º Para os fins desta Lei, considera-se:

X – blockchain: é o sistema que funciona como instrumento de registro em blocos, permitindo a transferência de informações criptografadas, sem a existência de autoridade central de validação;

Art. 9º Para contribuir com o alcance dos objetivos estabelecidos na Estratégia de Política de Prestação Digital dos Serviços Públicos, os órgãos e as entidades de que trata o art. 1º desta Lei elaborarão:

II – instrumento de planejamento de segurança da informação e cibernética, inclusive mediante a utilização da tecnologia blockchain, para os contratos públicos, registros de bens e prestação de contas, e a experimentação do uso da inteligência artificial para automatização de tarefas e a aceleração dos serviços públicos, tendo em vista o aperfeiçoamento e a confiabilidade do controle digital de atos, contratos e procedimentos administrativos, exigindo o máximo de transparência, ativa e passiva, no processo decisório público.

Los daños colaterales de las *blockchains*



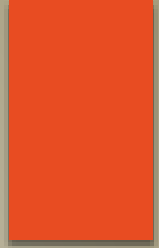
Hackear una Blockchain es extremadamente difícil pero no imposible.

La “DAO” (Decentralized Autonomous Organisation) fue creada por un grupo de desarrolladores liderado por Christoph Jentzsch, que desarrolló uno de estos 'Smart Contract'.

Se regía por su código fuente abierto del programa que fijaba las normas de funcionamiento, aceptado por más de 11.000 inversores anónimos sobre base de la criptomoneda Ethereum.

Contenía un error de programación que permitía extraer Ethers sin el permiso de los demás y a partir de ese error un hacker engañó a la red y transfirió a su cuenta gradualmente un total de 70 millones de dólares en Ethereum. Publicó luego una nota abierta en Internet aclarando que lo que hizo estaba en el código, y que si le retiraban sus Ethers los llevaría a los tribunales.

Los daños colaterales de las *blockchains*



Fortuna
Temas de hoy: Dólar, economía, Inflación, AFIP

U\$S 190 MILLONES INACCESIBLES 05/02/2019

Bitcoin: murió y no dejó la contraseña de la cuenta

El canadiense Gerald Cotten falleció repentinamente y no dejó a nadie el password de su billetera virtual y los inversores no pueden acceder a u\$s 190 millones en criptomonedas.



Gerald Cotten, CEO y creador de QuadrigaCX, quien murió repentinamente en la India.

Era el único que tenía la clave de la billetera electrónica, que contenía inversiones en diferentes monedas virtuales. No había otro que en la empresa **QuadrigaCX** podía tuviera la llave de esos activos. Y de repente de murió. Ahora nadie puede acceder a los u\$s 190 millones de esa billetera.

MÁS LEÍDAS

- Quiénes cobrarán el aguinaldo de ANSES
- ANSES informó fechas de cobro
- El dólar abre con una fuerte baja
- Cómo conseguir el descuento que da ANSES
- AFIP lanzó la "Multinota" digital
- Qué podés deducir del impuesto a las ganancias
- El dólar y el riesgo país cerraron a la baja
- ANSES comunicó fechas de cobro
- El dólar cerró debajo de los \$ 45
- ¿Cómo pedir los nuevos créditos ANSES?

Resumen Informativo
Los principales acontecimientos de la jornada.

+LEÍDAS EN PERFIL.COM

- Murió el periodista Sergio Gendler
- Felipe Solá: "La campaña de Macri-Pichetto va a costar 20 mil millones de dólares"
- Una nueva pista podría revelar quiénes ordenaron el triple crimen de General Rodríguez

LA NACION

LA NACION | TECNOLOGÍA | INTERNET

Creyó que compraba un juego de cama en oferta, pero terminó envuelta en una estafa con bitcoins



RECOMENDADOS

- La advertencia de los senadores del bloque que condujo a Pichetto: "El límite es Macri"
- Pichetto, vice de Macri: los tuits de Fernando Iglesias y cómo cayó el anuncio entre jóvenes militantes del Pío
- Una confluencia que acecha a los votantes de Macri
- Así quedaron definidas las principales alianzas para competir en las elecciones

MÁS LEÍDAS AHORA

1 El juego de cama ofertado, a un precio irrisorio, era en realidad una estafa para transformar el dinero en otra cosa

Las tensiones entre las *blockchains* y el RGPD

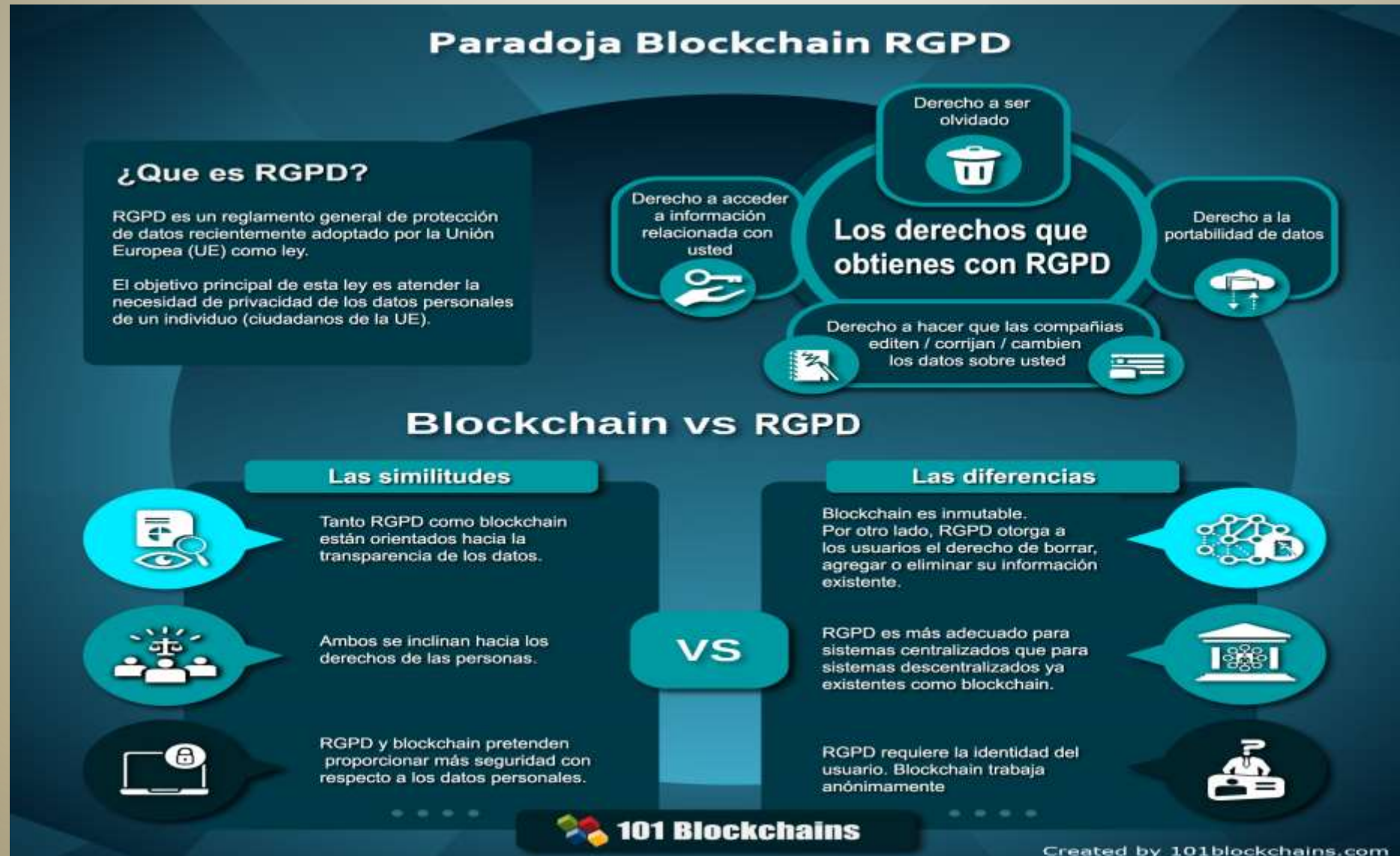
“La paradoja de la fuerza imparable contra el objeto inamovible”

El RGPD se asemeja a una fuerza imparable que todo el mundo debe aplicar (incluso más allá de la Unión Europea) y la tecnología blockchain se presenta como un objeto inamovible debido a su características inmutabilidad de los cambios.

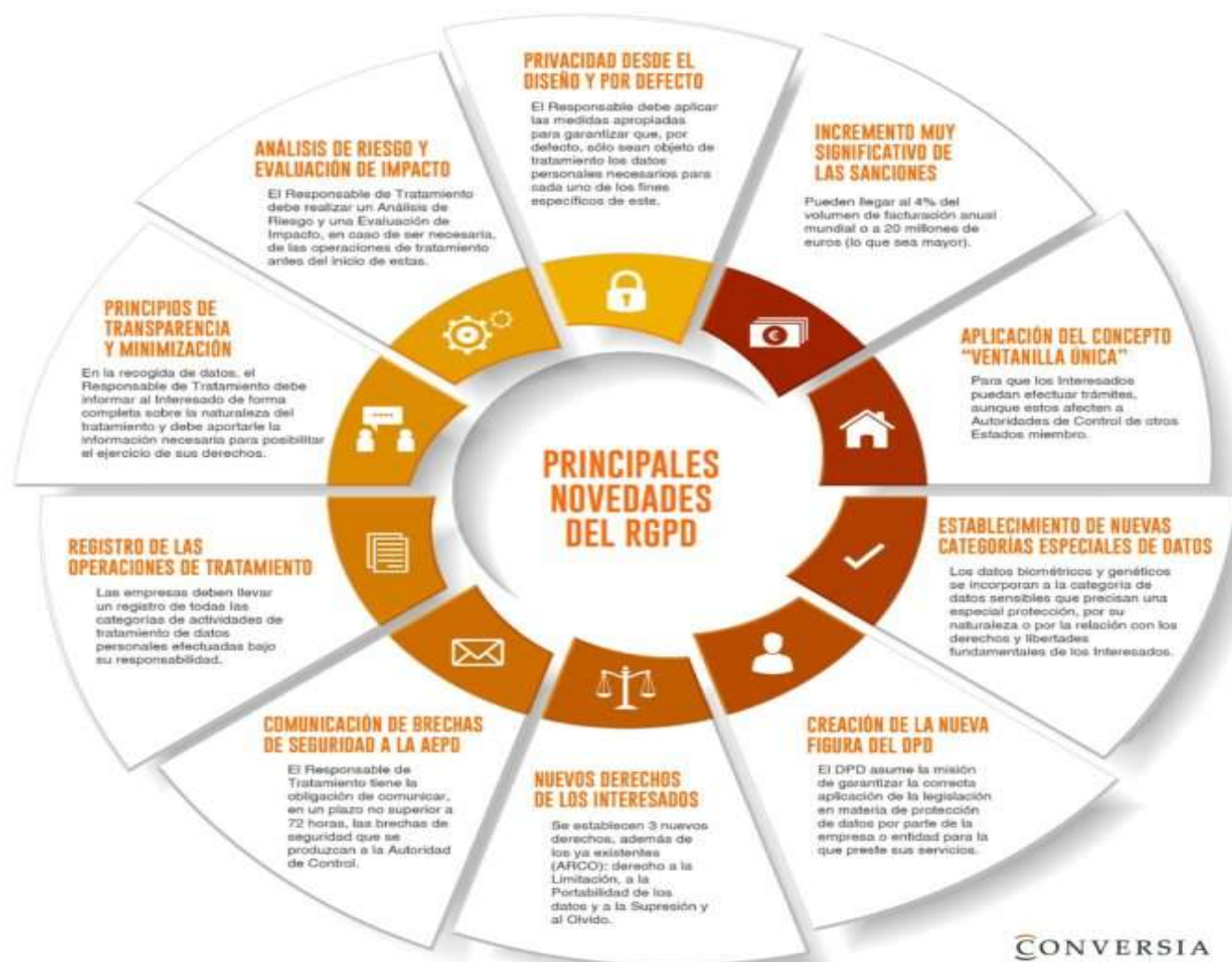
En su choque están presente además la tensión entre la protección de los derechos, la promoción de la innovación tecnológica y la libre circulación de los datos, en especial porque el RGPD se redactó bajo un modelo tradicional y centralizado en cuanto a la gestión de los datos (teniendo en miras los servicios de computación en la nube y las redes sociales), mientras que la ya existente tecnología parte de entornos en los que identificar a responsables, encargados o interesados es una tarea altamente compleja.



¿Blockchains vs. RGPD?



Principales novedades del RGPD



CONVERSIA
HFL GROUP

Top 12 Tips REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Aplicación del RGPD

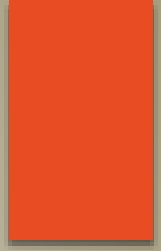


AyudaLeyProteccionDatos.es

Los principios, los derechos y las obligaciones en el RGPD



Tensiones entre las *blockchains* y el RGPD



Así como no hay una internet compatible con el RGPD, tampoco hay una versión de Blockchain que lo sea, aunque las blockchains privadas se llevan mejor con el RGPD

Informe del European Union Blockchain Observatory and Forum:

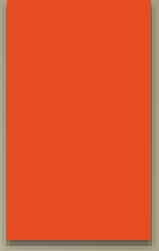
La compatibilidad o no de usos y aplicaciones que podrían llegar a ser compatibles con el RGPD debe realizarse caso por caso, verificando dónde aparecen los datos personales, cómo se tratan y quiénes son los responsables del tratamiento.

A) Las cadenas privadas suelen estar operadas por empresas, consorcios o entidades gubernamentales, por lo que están en posición de definir los roles de sus participantes y los flujos de información e imponer reglas estrictas de tratamiento de los datos personales al asegurarse de que todos los participantes de la red se vinculen con un conjunto de términos y condiciones, aunque esto no significa que todos tengan una razón legítima para ver los datos de cada uno de ellos.

B) Las cadenas públicas con permisos, son una de las formas más comunes de operar, y se sitúan en un punto intermedio a la hora de hacerlas compatibles con el RGPD.

C) Las cadenas públicas sin permisos presentan sin duda los mayores desafíos respecto al cumplimiento de RGPD, debido a su naturaleza extremadamente distribuida.

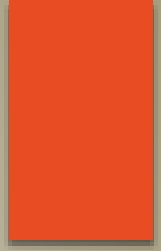
Los cuatro principales puntos de tensión



Las cuatro áreas aparentemente irreconciliables:

- 1) La identificación clara de responsables, encargados e interesados;
- 2) La minimización de riesgos para los interesados al subir datos a la cadena, de modo que deba recurrirse al cifrado de la información personal;
- 3) El ejercicio de los derechos, en especial el de supresión en un entorno de inmutabilidad de la cadena; y
- 4) la prohibición de decisiones individuales automatizadas en el caso de “contratos inteligentes” (*Smart contracts*) autoejecutables e irrevocables, ejecutados en la cadena.

Primer área de tensión: La determinación del responsable



Principio de accountability o responsabilidad pro activa (arts. 5.2 y 24, y considerando 74 RGPD, ya reconocido desde 1980 por la OCDE para los Códigos de conducta)
Requiere que los responsables del tratamiento pongan en marcha procedimientos y medidas eficaces.

Cadenas privadas y públicas con permisos

Es donde mejor encaja.

Informe de la CNIL sobre blockchain y el RGPD recomienda que en los consorcios de blockchain se identifique al responsable o corresponsables tan pronto como sea posible.

Hay corresponsabilidad entre el grupo de entidades o personas que decidan realizar un tratamiento de datos personales, pero esto no es aplicable si se crea una persona jurídica en representación de todos los participantes, que sería el responsable, al igual que cuando se designe a uno de los participantes como responsable del tratamiento.

Primer área de tensión: La determinación del responsable

Blockchain públicas sin permisos

Identificar a un responsable es mucho más complejo.

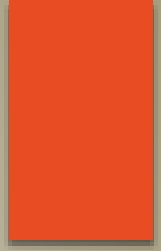
No deberían ser considerados responsables:

a) **los desarrolladores de protocolos** que crean y mantienen la tecnología de cadena de bloques de código abierto (Bitcoin) pues son voluntarios que trabajan en un proyecto de código abierto y en general no reciben una compensación directa por sus esfuerzos (si no sería como decir que Tim Berners-Lee es el responsable de todo lo que sucede en la World Wide Web).

b) **los nodos de validación o de participación** (aquí la cuestión no es tan pacífica), pues los nodos no determinan la finalidad ni los medios del tratamiento, ya que ejecutan el protocolo por una recompensa; para contribuir a la estabilidad de la red o para acceder a los datos que son relevantes para ellos sin depender de intermediarios externos.

La CNIL señala en su informe que los mineros no serían responsables ya que simplemente validan transacciones y no delimitan las finalidades ni los medios para su tratamiento (otros argumentan que a través de la acción de descargar y ejecutar activamente el software, los nodos determinan la finalidad y los medios del tratamiento y cuando se lanza una nueva versión de un protocolo, los nodos son libres de ejecutarlo o no, influyendo en cómo evoluciona la plataforma).

Primer área de tensión: La determinación del responsable



Blockchain públicas sin permisos

Serían responsables:

Quienes introduzcan datos personales en la blockchain (siempre que sea una persona física y el tratamiento de datos personales esté relacionado con una actividad profesional o comercial, o cuando los introduzca sea una persona jurídica) (CNIL).

Por ejemplo, si un notario registra el título de su cliente en un Blockchain, él es responsable de procesar. Además, si un banco ingresa los datos de sus clientes en un Blockchain como parte de sus procesos de administración de clientes, es responsable del procesamiento.

Los usuarios de la red que firman y envían transacciones a la cadena vía un nodo pueden ser considerados responsables si envían datos personales como parte de una actividad comercial (se incluye a las entidades que operan software y a productos o servicios que publican datos personales en una cadena de bloques).

Se excluye a quienes envían sus propios datos para su uso personal, como la compraventa de criptoactivos, pues se estaría ante la excepción del artículo 2.2 c) RGPD de tratamiento de datos para uso doméstico. Por ejemplo, una persona física que vende o compra Bitcoin por su propia cuenta no es responsable del tratamiento.

Primer área de tensión: La determinación del encargado

La CNIL entiende que podremos delimitar al encargado del tratamiento solo en supuestos concretos, por ejemplo:

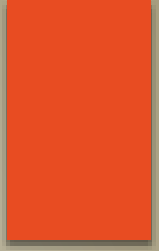
a) Los desarrolladores de smart contracts que tengan acceso a datos personales de los usuarios de sus smart contracts.

b) Los desarrolladores o validadores de transacciones, como son los mineros en las blockchain privadas o en las públicas con permisos, y bajo un protocolo de consenso de prueba de trabajo, cuando validan transacciones que contengan datos personales.

En esos casos sería necesario que los mismos cumplan con las obligaciones impuestas a los encargados del tratamiento en el artículo 28 RGPD, pero la CNIL reconoce que **esta obligación deviene prácticamente imposible en blockchains públicas sin permisos**.

Segunda área de tensión:

La anonimización de los datos en la cadena



El RGPD no se aplica al tratamiento de datos personales anonimizados bajo una técnica que impida, de manera irreversible, identificar a una persona física (no basta la seudonimización).

Dada la inmutabilidad de los datos en la mayoría de las redes de blockchain, almacenar datos personales sin cifrado contradice el principio de privacidad desde el diseño (art. 25 RGPD).

La CNIL advierte que el responsable del tratamiento debe evaluar cuidadosamente si el tratamiento mediante blockchain es apropiado, máxime cuando pueden producirse transferencias internacionales.

Este aspecto es más controlable en blockchains privadas o públicas con permisos, al poder aplicar cláusulas contractuales estándar, normas corporativas vinculantes, códigos de conducta o certificaciones, pero no en las blockchains pública sin permisos.

Los datos personales pueden subirse a blockchain mediante técnicas de ofuscación, cifrado o agregación para el tratamiento de datos personales.

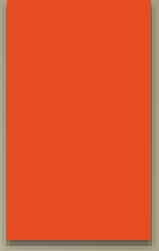
El informe del European Union Blockchain Observatory and Forum indica que deben evaluarse dos riesgos cuando se adoptan algunas de estas técnicas:

a) Riesgo de reversión: cuando pese a la técnica criptográfica utilizada, se puede revertir el proceso y reconstituir los datos originales (p.ej., mediante el descifrado de fuerza bruta).

b) Riesgo de vinculación: cuando pueden vincularse los datos cifrados a una persona mediante el examen de los patrones de uso o contexto, o por comparación con otras piezas de información.

Segunda área de tensión:

La anonimización de los datos en la cadena



Medios posibles de anonimización

I. Ofuscación de direcciones personales

En el DRAE “ofuscar” significa “oscurecer y hacer sombra” (entre otras acepciones).

Una cadena de bloques usa el sistema de “clave pública/privada” para proporcionar o derivar direcciones de los remitentes y receptores de las transacciones (la clave pública sería como el número de un apartado de correos, donde puedo enviar información, pero solo el dueño de la clave privada puede abrirlo y obtener la información).

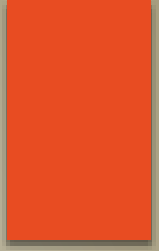
La clave pública consiste en una larga cadena de caracteres aleatorios, pero como en algunas blockchains públicas las direcciones de los remitentes y receptores de las transacciones pueden ser vistas por todos, según el RGPD dichas direcciones serían datos seudonimizados, especialmente cuando existe un claro riesgo de vinculación (p.ej., si se tiene la clave pública visible en la bio del Twitter personal).

La CNIL afirma que las claves públicas hacen al funcionamiento de blockchain, y que son un dato que no puede minimizarse más cuyo periodo de conservación está en línea con la existencia de la propia cadena (si se usa la misma dirección para varias transacciones, entonces comienzan a surgir patrones, los cuales combinados con otros tipos de información, permitirían identificar indirectamente a los individuos, aunque pueden utilizarse las técnicas de:

- a) servicio de direccionamiento indirecto de terceros y
- b) firmas de anillos.

Segunda área de tensión:

La anonimización de los datos en la cadena



Medios posibles de anonimización

II.- Cifrado de datos personales

A) Cifrado reversible: Solo la persona en posesión de la clave de cifrado puede descifrarla.
Varios tipos:

Cifrado simétrico (se usa la misma clave para encriptación y descifrado)

Cifrado asimétrico (se utilizan diferentes claves).

Por muy sólido que sea el cifrado empleado en los datos, mientras la llave para revertirlo siga existiendo, no hay dato anónimo.

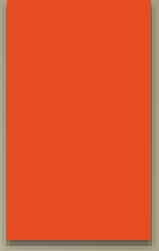
B) Hashing (cifrado no reversible):

Las cadenas de bloques hacen un gran uso de hashes criptográficos (técnica matemática que permite generar una cadena de caracteres alfanuméricos de longitud fija y única a partir de cualquier conjunto de datos digitales). Son como huellas digitales, si cambia el dato más pequeño, el hash será radicalmente diferente y dejará claro que los datos subyacentes se modificaron.

Un dato personal hashado puede o no ser un dato personal dependiendo de si el tiempo y la tecnología identifican posibles riesgos de reversabilidad o vinculación (el GT 29 expresó que un ataque de fuerza bruta puede reverir un hash si los datos originales son conocidos y no muy grandes).

Segunda área de tensión:

La anonimización de los datos en la cadena



Medios posibles de anonimización

II.- Cifrado de datos personales

B) Hashing (cifrado no reversible):

Reversibilidad:

Este riesgo se intenta mitigar mediante técnicas de “**salting**” (salado) y “**peppering**” (pimentado), que agregan información adicional a los datos para hacerlos lo suficientemente grandes como para que un ataque de fuerza bruta no pueda tener éxito.

La diferencia entre salar y pimentar radica en que al salar el creador del hash almacena fuera de la cadena la información salada y el hash. Mientras tanto, pimentar implica que la información pimentada se almacena de forma secreta, o que ni siquiera se almacena.

Vinculación:

Este riesgo derivado del análisis de patrones (p.ej, tiempo y frecuencia de las transacciones) Debe analizarse caso por caso para determinar si un dato personal hashado está o no sujeto a la normativa.

Segunda área de tensión:

La anonimización de los datos en la cadena

Medios posibles de anonimización

Opinión 5/14 GT29: Análisis caso por caso sobre tres aspectos clave para verificar que la anonimización es correcta:

Singularización: ¿es posible extraer de un conjunto de datos algunos registros que identifiquen a una persona física?

Vinculabilidad: ¿es posible vincular como mínimo dos registros de un único interesado o grupo de interesados?

Inferencia: ¿es posible deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos?

Segunda área de tensión: La anonimización de los datos en la cadena

Medios posibles de anonimización

Zero-knowledge proofs (ZKP o pruebas de conocimiento cero)

Son técnicas criptográficas avanzadas que permiten presentar pruebas de una declaración sin revelar los datos subyacentes (p.ej., ser mayor de edad, sin revelar la edad real).

Son muy prometedoras en lo que respecta a la privacidad desde el diseño y la soberanía de los datos personales, pero todavía necesitan rodaje.

Zcash las utiliza y también fue la primera criptomoneda en implementar zk-SNARK.

También Ethereum implementó zk-SNARK como parte de la actualización de Bizancio (el protocolo AZTEC).



Segunda área de tensión: La anonimización de los datos en la cadena

Medios posibles de anonimización

Encriptación homomórfica.

Método criptográfico ideado por Craig Gentry en 2008, donde los datos subyacentes nunca se revelan ni se comparten en la cadena de bloques. Se cifran, envían a la nube y se opera sobre ellos sin descifrarlos.

Con el cifrado homomórfico, una empresa podría cifrar toda su base de datos de e-mails, subirla a la nube, utilizar los datos guardados para hacer una búsqueda en la base de datos y entender cómo colaboran sus trabajadores. Los resultados se podrían descargar y descifrar sin exponer los detalles de ningún correo electrónico.

La nube no tiene la menor idea del contenido de los datos sobre los que está operando, La totalidad de los datos permanecen cifrados durante todo el tiempo.



Segunda área de tensión:

La anonimización de los datos en la cadena

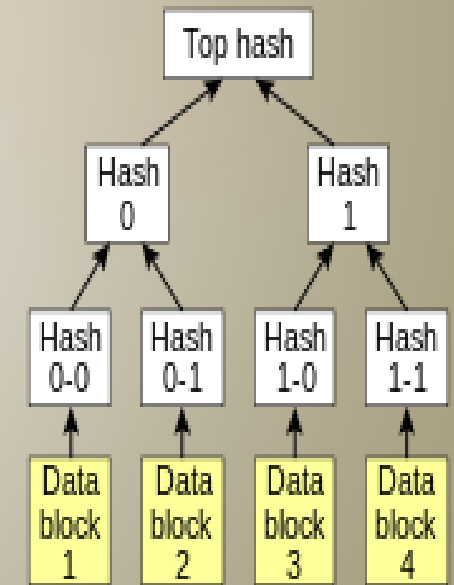
Medios posibles de anonimización:

La agregación de datos personales

Pueden utilizarse unto a las de ofuscación y encriptación, agregándose una gran cantidad de datos den una única firma digital que luego fuera incorporada a la cadena. Esa firma serviría luego como la prueba de la existencia de cada uno de los datos sumados.

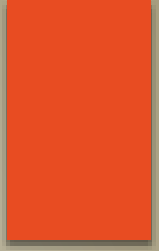
Estas técnicas de agregación dependen de los **árboles de Merkle** (estructura jerárquica que se compone de un hash de hashes), se toman todas las transacciones del bloque y se calculan sus hashes, una por una; los hashes resultantes se juntan por parejas y se calcula el hash de la pareja. Esta operación se repite sucesivamente hasta que solo queda un único hash de todo, la raíz de Merkle.

Se confía mucho en el potencial de estas técnicas de agregación a fin de anonimizar datos personales y facilitar que se comparta información anónima en una blockchain pública sin permisos.



Segunda área de tensión:

La anonimización de los datos en la cadena



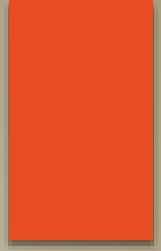
Medios posibles de anonimización:

La opinión de la CNIL

- 1) Al subir datos personales a blockchain se deben aplicar antes los principios de privacidad desde el diseño y por defecto;
- 2) Si no queda más remedio que usar la cadena de bloques, deben adoptarse soluciones que procesen los datos fuera de la cadena;
- 3) Si se sube el dato a la cadena, debe hacerse en forma de “commitment” criptográfico, o que se suba el hash generado al aplicar la técnica de hashing al dato o el ciphertext del dato;
- 4) si nada de eso es posible, la finalidad del tratamiento está justificada y la evaluación de impacto dice que el riesgo residual es aceptable, entonces se puede subir el dato personal en claro o simplemente hasheado.
- 5) En cuando a las medidas de seguridad, le preocupa el potencial fallo del algoritmo, de sus vulnerabilidades o la confidencialidad de la cadena, si la misma no es pública.

Tercer área de tensión:

Principios, obligaciones y ejercicio de los derechos



Consentimiento

Cadenas privadas y cadenas públicas con permisos

No hay inconvenientes con el consentimiento pues sería posible identificar una entidad que opera el producto o servicio y actúa como intermediario entre los usuarios individuales y la cadena de bloques.

Cadena pública sin permisos

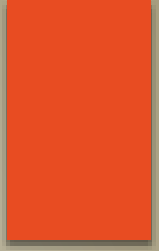
Es difícil determinar a quién se da el consentimiento pues no está claro quién es el responsable, aunque se argumenta que al elegirse una red descentralizada al completo, el usuario lo está dando, aunque el consentimiento no expreso no cuadra bien con el RGPD.

Cuando el usuario realiza una transacción puede argumentarse un tratamiento basado en una relación contractual, pero no se puede determinar quién está del otro lado del contrato y la parte informativa de esa contratación.

No se ha planteado el interés legítimo como base de legitimación, pero dada la particular naturaleza de la cadena de bloques (un sistema transparente, descentralizado, inmutable y sin intermediarios), tiene lógica pues todos los participantes en la cadena tienen un interés legítimo en que el sistema funcione.

Tercer área de tensión:

Principios, obligaciones y ejercicio de los derechos



1. Los derechos totalmente compatibles

El derecho a la información de las personas no plantea ninguna dificultad particular: el controlador de datos tendrá que proporcionar información concisa, de fácil acceso y formulada en términos claros a la persona en cuestión antes de enviar a la validación de los mineros un dato personal.

Los derechos de acceso y a la portabilidad: la CNIL considera que el ejercicio de estos derechos es compatible con las propiedades técnicas de Blockchain, pero no siempre será fácil saber quién es el responsable del tratamiento, y por tanto a quién dirigirse. Incluso si el interesado pudiera identificar y comunicarse con un nodo específico, el nodo no sería necesariamente capaz de responder estas preguntas.

2. Los derechos problemáticos

La minimización de los datos personales debe efectuarse de tal forma que el único dato personal en la blockchain sea la clave pública.

El período de conservación de una clave pública, admite que sea el de la propia cadena. Si bien el ejercicio efectivo de ciertos derechos no parece ser un problema, la aplicación del **derecho de cancelación, el derecho al olvido, el derecho de rectificación y el derecho de oposición** merecen un análisis más detallado.

Tercer área de tensión:

Principios, obligaciones y ejercicio de los derechos

El derecho de cancelación o supresión

Al ser técnicamente imposible la eliminación pero en algunos casos por derivación del hasheo o de un cifrado utilizando un algoritmo y claves de acuerdo con el estado de la técnica, el controlador puede hacer que el dato sea casi inaccesible, y por lo tanto se aproxima a los efectos de un borrado de los datos, aunque no lo son en sentido estricto en la medida en que los datos seguirían existiendo en el Blockchain

El derecho al olvido

Es también técnicamente imposible su utilización en cualquiera de sus versiones, ya sea como supresión o como desindexación en un ámbito de tecnología de blockchain

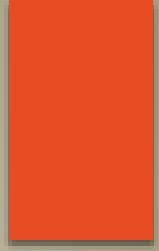
El derecho de rectificación

Es también técnicamente imposible la rectificación de los datos cuando se ingresan en una cadena de bloques, por lo cual se encarece no ingresar datos personales sin recurrir a métodos criptográficos.

Con respecto al derecho de rectificación, la imposibilidad de modificar los datos ingresados en un bloque debe llevar al controlador a ingresar los datos actualizados en un nuevo bloque, ya que una transacción posterior siempre puede cancelar la anterior, aun cuando siga apareciendo en la cadena.

También pueden aplicarse las mismas soluciones que para la eliminación de los datos personales podrían aplicarse a los datos erróneos .

Tercer área de tensión: Principios, obligaciones y ejercicio de los derechos



La transferencia internacional y la territorialidad del tratamiento de los datos.

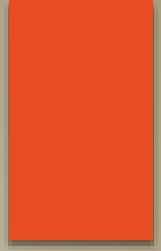
El RGPD especifica que los datos personales generalmente solo pueden transferirse a terceros países si estos se consideran “adecuados”, es decir, si se considera que brindan la misma protección que la de la Unión Europea. De lo contrario, el responsable puede introducir las garantías adecuadas de que los datos se tratarán de manera consistente y de conformidad total con el RGPD.

Esto puede ser muy problemático en una blockchain pública sin permisos e incluso en una privada que no cuente con las debidas autorizaciones.

La protección de datos desde el diseño y por defecto

El responsable del tratamiento debe aplicar, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas para aplicar de forma efectiva los principios de protección de datos, pero la tecnología blockchain está todavía inmadura y es desarrollada por comunidades de código abierto de todas las partes del mundo, pero como está todavía en construcción, es factible que se incorporen novedades que la hagan compatible con el espíritu y el contenido del RGPD.

Cuarta área de tensión: la prohibición de decisiones individuales automatizadas y los *Smart contracts* (autoejecutables e irrevocables)



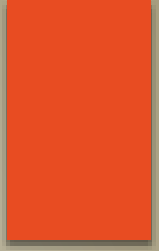
La limitación del tratamiento (art. 18, GDPR) y las decisiones totalmente automatizadas (art. 22, GDPR).

Sería posible limitar el uso de datos en contratos inteligentes mediante la planificación en el programa.

Una decisión totalmente automática de un contrato inteligente es necesaria para su ejecución, en la medida en que permite realizar la esencia del contrato (por lo que las partes se han comprometido).

De todos modos, el interesado debe poder obtener intervención humana, expresar su punto de vista y cuestionar la decisión después de que se haya ejecutado el contrato inteligente.

Reevaluación



BLOCKCHAIN PRIVADA

¿Quién es el probable responsable?

El consorcio de empresas creador, alguna de las mismas o una fundación. Sin descartar la corresponsabilidad en determinados casos (con los usuarios de la plataforma, por ejemplo) o que el consorcio actúe como responsable y encargado en determinadas circunstancias (cuando un servicio externo los contrate para operar sobre la cadena).

¿Quiénes son los probables encargados?

Los mineros/nodos y proveedores de servicios que operen en la misma, que a su vez podrían ser responsables en algunos casos.

¿Subimos datos a la cadena?

Teniendo en cuenta el tipo de blockchain, seguramente se podría hacer. Pero haría falta ver el caso particular, no olvidar la privacidad desde el diseño, la minimización de los datos o las medidas de seguridad adecuadas. Sin olvidar la opción preferente de cargar datos off-chain (es decir, fuera de la cadena).

¿Se pueden ejercer todos los derechos?

Debido al tipo de cadena, seguramente sí. Pero estará condicionada por su diseño, al final del día.

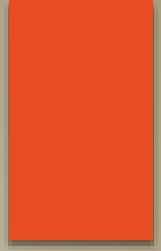
¿Podemos controlar las decisiones individuales automatizadas de los contratos inteligentes?

Debido al tipo de cadena, seguramente sí.

¿Hay transferencias internacionales de datos?

Es posible, pero deberían ser manejables con cláusulas contractuales tipo, códigos de conducta, certificaciones o normas corporativas vinculantes.

Reevaluación



BLOCKCHAIN PÚBLICA CON PERMISOS

¿Quién es el probable responsable?

El consorcio de empresas creador, alguna de las mismas o una fundación. En todo caso, y como el informe del Bundesblock señala, se recomienda explorar la idea de las “normas vinculantes de la cadena” para una blockchain que cumpla con determinados criterios. Tampoco debe descartarse la idea de que el interesado pudiera ser responsable de sus propios datos.

¿Quiénes son los probables encargados?

Algunos de los mineros/nodos y proveedores de servicios que operen en la misma, que a su vez podrían ser responsables en algunos casos.

¿Subimos datos a la cadena?

Teniendo en cuenta el tipo de blockchain, seguramente se podría hacer. Pero haría falta ver el caso particular, no olvidar la privacidad desde el diseño, la minimización de los datos o las medidas de seguridad adecuadas. Sin olvidar la opción preferente de cargar datos off-chain (es decir, fuera de la cadena).

¿Se pueden ejercer todos los derechos?

Debido al tipo de cadena, es probable. Pero debería verse el caso particular. De todos modos, y dado el tipo de cadena, podría valorarse la imposición de forks (una bifurcación en el desarrollo de la cadena) para el cumplimiento de algunas obligaciones del RGPD.

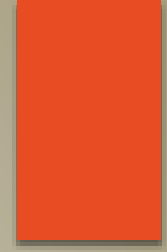
¿Podemos controlar las decisiones individuales automatizadas de los contratos inteligentes?

Debido al tipo de cadena, es probable. Pero debería verse el caso particular.

¿Hay transferencias internacionales de datos?

Es posible, pero deberían ser manejables con cláusulas contractuales tipo, códigos de conducta, certificaciones o normas corporativas vinculantes.

Reevaluación



BLOCKCHAIN PÚBLICA SIN PERMISOS

¿Quién es el probable responsable?

Difícil determinarlo. No son los nodos de participación ni de validación. Tampoco lo serían los desarrolladores de la cadena. Podrían serlo los servicios que funcionen sobre la cadena en su relación particular.

Los participantes en actividad no personal sino profesional podrían ser considerados responsables.

Unas “normas vinculantes de la cadena” crearían cierta corresponsabilidad entre todos los participantes para facilitar cierto ejercicio de derechos.

¿Quiénes son los probables encargados?

Los servicios o aplicaciones que operen sobre la cadena.

¿Subimos datos a la cadena?

Aplicando privacidad desde el diseño, no, pero si no queda más remedio, valorar la técnica para el cifrado o priorizar subir datos off-chain.

¿Se pueden ejercer todos los derechos?

No todos. Las propiedades de la cadena condicionan los derechos de supresión, rectificación, acceso, oposición y limitación del tratamiento, siendo el más sencillo el de portabilidad.

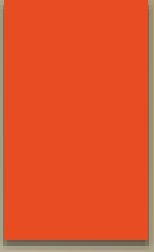
¿Podemos controlar las decisiones individuales automatizadas de los contratos inteligentes?

Es difícil debido al tipo de cadena, pero dependería del diseño del smart contract.

¿Hay transferencias internacionales de datos?

Sin duda, ilimitadas e incontrolables, lo que nos lleva a la privacidad desde el diseño y a almacenar los datos fuera de la cadena.

Conclusiones



Las propiedades del blockchain (transparencia, inmutabilidad, descentralización y desintermediación) no se llevan bien con el RGPD, pero las tensiones irán siendo resueltas por el European Data Protection Board (EDPB), legisladores, jueces, etc..

Si bien no son incompatibles e irreconciliables, los conflictos deben evaluarse caso por caso, y a la hora de aplicar esta tecnología responder a las siguientes preguntas:

- 1.- ¿Realmente necesitamos blockchain?
- 2.- ¿Qué tipo de datos se necesitan, quién puede consultarlos, con qué finalidad se tratarán, sobre qué base legal y durante cuánto tiempo?
- 3.- ¿Es aplicable la privacidad desde el diseño y por defecto del RGPD?
- 4.- ¿Realmente necesitamos almacenar datos personales en blockchain?
- 5.- ¿Qué técnicas podemos utilizar para anonimizar los datos personales o mantenerlos fuera de la cadena?

Pero además, se debe ser lo más claro y transparente posible con los usuarios y seguir innovando, tal como lo está haciendo la comunidad (tecnológica y legal).

Si bien la convivencia entre blockchains y RGPD es hoy compleja, el futuro de ambos es prometedor y parecen estar destinados a entenderse.

Conclusiones

En definitiva, si bien la respuesta compatibilizadora parecería requerir de ciertas dotes de magia, en realidad vendrá por el lado de innovaciones tecnológicas que no tardarán en llegar.



Palabras finales

Datos de contacto

oscarpuccinelli@gmail.com

+5493415458972