BLOCKCHAIN

Y su impacto en el mundo sanitario

Nicolás Barajas García

Jose Antonio Fuentes García

XI Jornadas de APISA

fppt.com

Indice de Contenidos

- Introducción
- Qué es Blockchain
- Cómo funciona Blockchain
- Carácterísticas de Blockchain
- Tipos de Blockchains
- Smart Contracts
- Aplicaciones en el mundo Sanitario
- Blockchain vs RGPD
- ¿Revolución industrial?

Introducción

Servicio Andaluz de Salud
CONSEJERÍA DE SALUD

ABYTES
Bytcoins

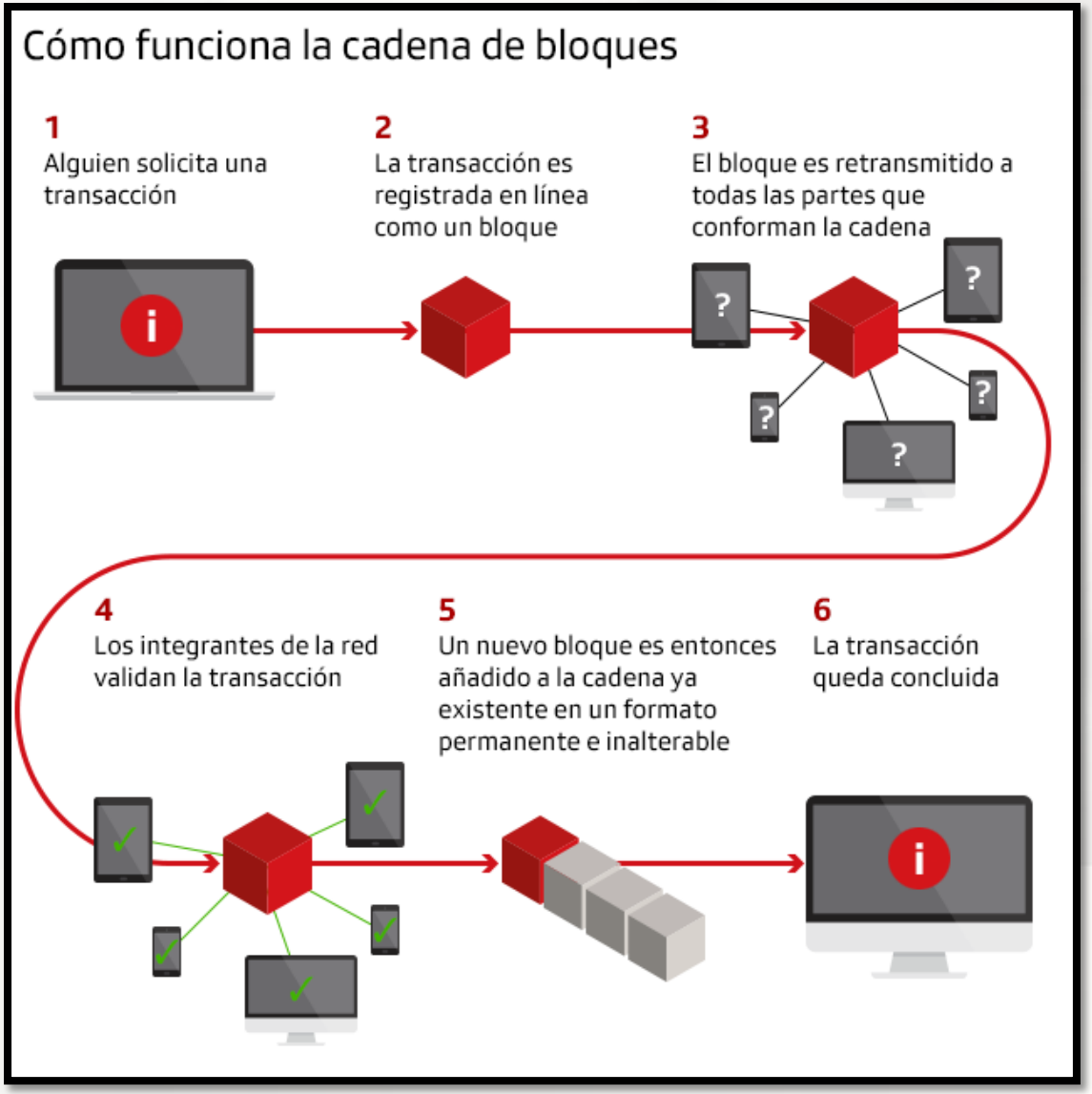
http://abytes.org

Qué es Blockchain

Una cadena de bloques o Blockchain, es una base de datos distribuida donde se pueden crear y guardar transacciones digitales seguras, encriptadas y firmadas digitalmente, en una red de nodos también distribuidos.

- Cada nodo mantiene su copia de la información y todos los miembros tienen que validar cualquier actualización de forma conjunta.
- Las entradas son permanentes, transparentes y buscables, lo que permite a los miembros de la comunidad ver la historia de las transacciones en su totalidad.
- Con blockchain, la criptografía sustituye a cualquier intermediario o tercero.

Cómo funciona Blockchain



Características de Blockchain

Distribuida y Descentralizada

Una blockchain, como ya se ha dicho, es una base de datos cuyos registros son almacenados por igual en nodos distribuidos que conforman una red, sin nodos centrales que controlen a otros o que posean información distinta al resto.

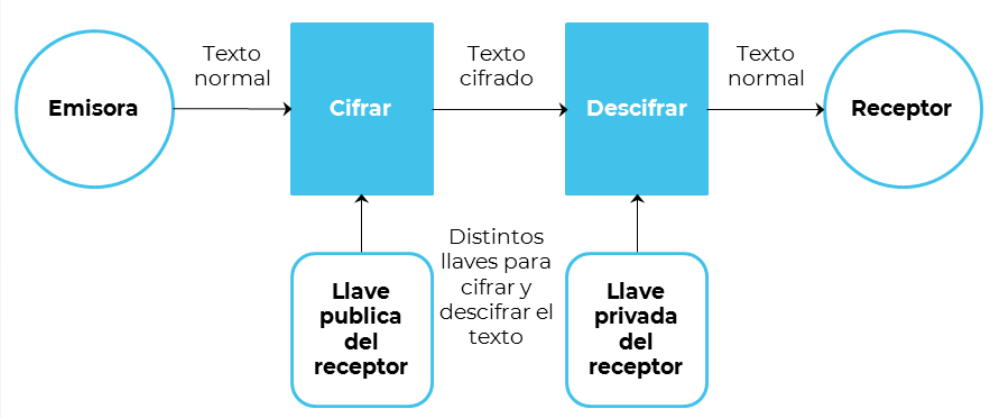
Este esquema distribuido es una de sus principales ventajas ante otras redes de almacenamiento: es prácticamente imposible de *hackear* debido a que no basta con atacar uno o dos nodos de la red, sino que tendrían que hacerlo con absolutamente todos para poder causar realmente daño.

Esta propiedad es inspirada en las redes de almacenamiento y comunicación ***peer-to-peer*** **(p2p)**.

Características de Blockchain

Criptografía y Seguridad

¿Cómo funciona la criptografía en Blockchain?



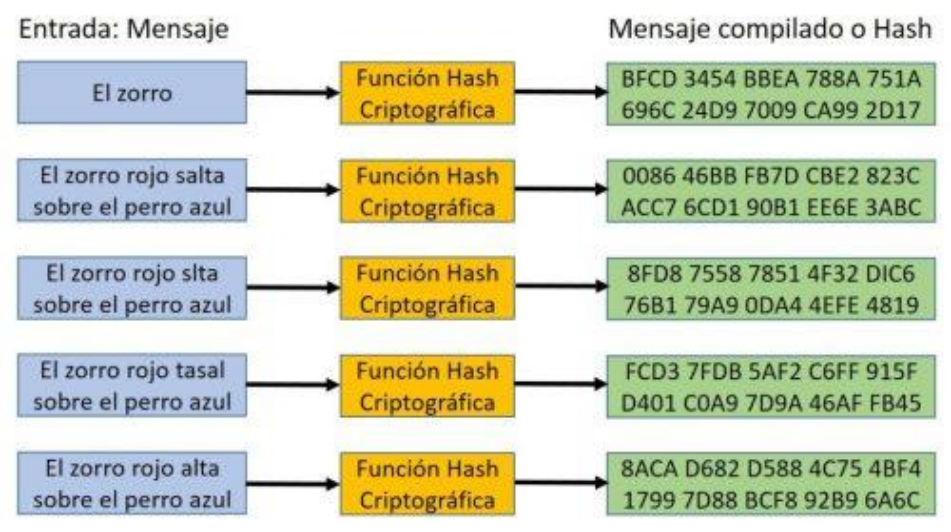
Sistemas criptográficos asimétricos basados en pares de claves, una pública y una privada. La clave privada es la que el usuario guarda y utiliza para descifrar los mensajes que recibe, así como para firmar los mensajes que envía. La clave pública es una clave que se pone a disposición de todos los demás usuarios, para que puedan cifrar los mensajes que quieran enviarnos, así como verificar nuestra firma digital.

Características de Blockchain

Criptografía y Seguridad

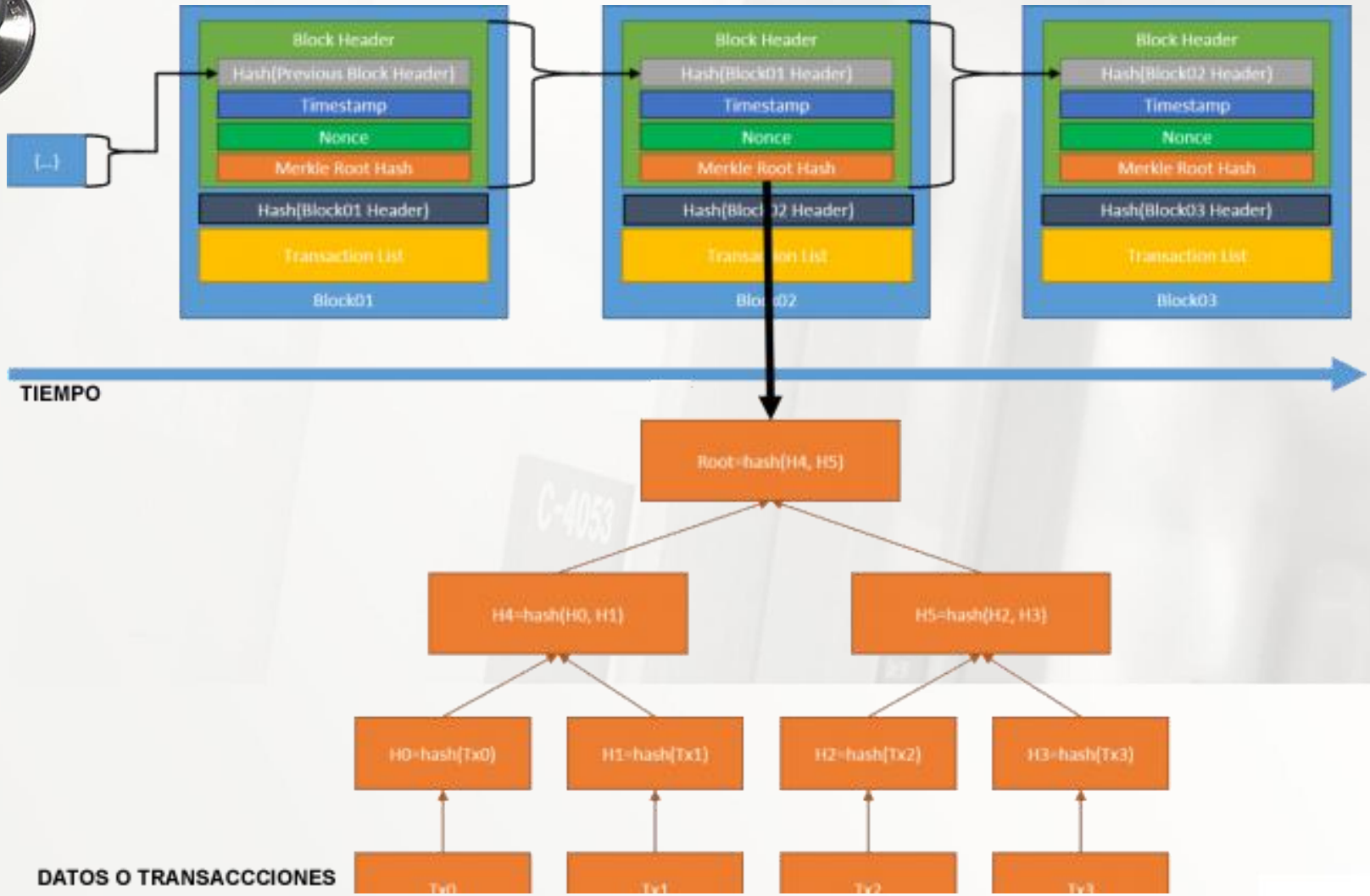
FUNCIÓN HASH

Las funciones “hash” son funciones criptográficas **unidireccionales** que son usadas para mapear datos de un tamaño arbitrario a datos de tamaño fijo.



Características de Blockchain

No Falsificable e Inmutable



Tipos de Blockchain

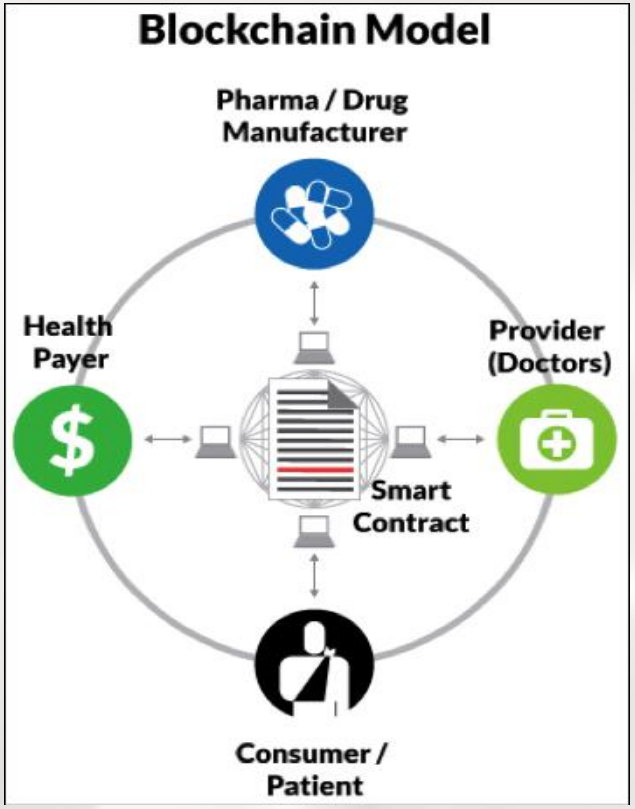
Públicas y Privadas

Las blockchain **públicas** son aquellas en las que no hay restricciones para participar, tanto en la lectura como en la escritura de sus datos.
Por el contrario, las blockchain **privadas** son aquellas en las que tanto la escritura como la lectura de los datos están limitadas a una lista predefinida de participantes conocidos y de confianza.

Con Permisos y Sin Permisos

Las cadenas de bloques **con permisos** (*permissioned blockchains*) son aquellas en las que la tarea de procesar transacciones es llevada a cabo por por una lista de participantes conocidos. Por ello generalmente no necesitan tokens nativos.
Por otro lado, las cadenas de bloques **sin permisos** (*permissionless blockchains*) son aquellas en las que no existen restricciones a la hora de procesar transacciones y crear bloques. Este tipo de cadenas de bloques necesitan tokens nativos para proveer incentivos a los usuarios y que éstos mantengan el sistema.

Smarts Contrats



Son contratos que se ejecutan y se hacen cumplir a sí mismos de manera automática y autónoma.

Smarts Contrats

Gestión del historial médico con Blockchain

Si el Blockchain controlase la gestión del historial médico de los pacientes, cambiaría de forma radical la forma en la que se realiza la gestión del historial médico.

El paciente, propietario de dicho informe, podrá acceder cuántas veces quisiera y decidir, por lo tanto, quién más podría acceder a su información.

Dicha aplicación se organizará a través de smart contracts (contratos inteligente), estos son mecanismos que eliminan intermediarios con el objetivo de ahorrar costes al consumidor.

Un smart contract tiene validez, sin depender de autoridades, es un código visible por todos y que no puede ser modificado al existir sobre la tecnología blockchain, la cual le otorga un carácter descentralizado.

Aplicaciones en el mundo Sanitario

Es imprescindible un cambio de concepción en la gestión de servicios y de cultura de trabajo, donde proveedores de servicios de salud deben adaptarse a un modelo relacional **enfocado en el usuario**, al que deben ofrecer servicios personalizados, adaptados a su contexto, necesidades, tiempo y lugar.

Por ejemplo, uno de los principales factores limitadores en la actualidad es la dificultad para obtener, gestionar e intercambiar información sensible de los pacientes. Esto es debido a la LOPD/RGPD y el carácter sensible de la información médica de los pacientes.
Una de las principales oportunidades que nos brinda el uso Blockchain, es la capacidad para almacenar y compartir de forma segura información sensible que, en todo momento, es propiedad del usuario.

Aplicaciones en el mundo Sanitario

Trazabilidad de los Medicamentos

Orientado en el mundo farmacéutico, el desarrollo de blockchains privadas en las que se involucre e integre a los diferentes elementos de la cadena de distribución (agentes productores, entidades sanitarias certificadoras, distribuidores y vendedores) origina que cada vez que un medicamento se fabrique, se genere un hash (huella digital criptográfica) que proporcionaría toda la información relativa a su origen, fabricación y componentes.

Cada vez que un agente interaccione con ese medicamento, se volverá a generar otro hash vinculado al anterior con más información, lo cual podría permitir una **trazabilidad total, fiable y transparente del medicamento en toda su cadena**. Aportando transparencia y certidumbre, y evitando falsificaciones.

Aplicaciones en el mundo Sanitario

Repositorios de Información

Con Blockchain cambiaría por completo cómo se realiza la gestión del historial médico de las personas, en primer lugar porque permitiría que el paciente sea el verdadero **propietario** de su información médica y quién decida en cada caso quién es el que puede acceder a dicha información y en segundo caso porque para que la asistencia sanitaria pueda obtener beneficios, **el Blockchain debería funcionar como administrador de control de acceso para registros y datos de salud.**

Hay que tener en cuenta que blockchain es muy ineficiente como almacén de datos debido a su carácter distribuido. La información contenida en la ella debería ser un índice, una lista de todos los registros de salud del usuario y los correspondientes datos de salud. Un catálogo de metadatos sobre el paciente y un lugar donde encontrar esta información. Las transacciones en los bloques contendrían un identificador único del usuario, un cifrado vinculado al registro de salud y un timestamp de cuando se creó la transacción. Para mejorar la eficiencia en el acceso a la información, la transacción contendría el tipo de datos contenidos en el registro de salud y cualquier otra metadato que facilite consultas frecuentes.

Aplicaciones en el mundo Sanitario

Seguridad

En un sistema de naturaleza centralizada, alguien que posea el acceso al usuario administrador del sistema podría cambiar la medicación de miles de personas, con las consiguientes secuelas fatales, sin dejar rastro. De otra forma, los propios hospitales también podrían alterar la información sobre los tiempos de espera de los pacientes, sin que las autoridades sanitarias lo perciban.

En un modelo descentralizado en el que todos los hospitales cuentan con una base de datos distribuída, transparente y segura mediante criptografía y son los pacientes quienes tienen el control de la información, los problemas anteriores no pueden producirse.

Aplicaciones en el mundo Sanitario

Investigación Clínica

Blockchain puede tener un impacto global en la investigación clínica, ya que permitiría el seguimiento, el intercambio y la protección de los datos. Como ya hemos visto puede garantizar un seguimiento seguro y descentralizado para cualquier interacción de datos que pudiera ocurrir en el contexto del ensayo clínico. De igual forma podría ser una base para mejorar la metodología de investigación clínica y un paso adelante hacia una mayor transparencia para mejorar la confianza dentro de las comunidades de investigación y con los pacientes.

Aplicaciones en el mundo Sanitario

Plataformas Tecnológicas a nivel de Blockchain Sanitario:

- Para construir aplicaciones de atención médica:
  - GemOS Health asociada con Philips.
  - Pokitdok asociada con Intel.
- Para proveer servicios médicos descentralizados: HealthCombix
- Para conectar pacientes e investigadores médicos: Blockchain Health Co.
- Servicios asistenciales virtuales: PointNurse
- Gestión de registros médicos: MedRec prototipo favorecido por el MIT
- Registros personales de salud: Patientory
- Desarrollo de fármacos y suministro de medicamentos: iSolve

Blockchain vs RGPD

Preceptos en los que el blockchain cumple con el RGPD

- **Consentimiento**

El RGPD establece que el consentimiento debe ser expreso, es decir debe de darse con una clara acción afirmativa. En el caso del Blockchain cada usuario verifica y valida los datos antes de que se agreguen a la cadena de bloques, y el historial de transacciones proporciona una prueba de consentimiento, por lo que **no entra en conflicto** con el **RGPD**, sino que en este caso es la herramienta ideal.

- **Privacidad desde el diseño**

Con la introducción del RGPD, antes de realizar cualquier tipo de tratamiento de datos se debe pensar en la protección de los mismos. Es lo que se conoce como Privacy by Design. En las **cadenas de bloques**, una de sus principales características es el **uso de seudónimos.** La propia infraestructura impone el uso predeterminado de seudónimos y algoritmos de cifrado.

Blockchain vs RGPD

Preceptos en los que el blockchain NO cumple con el RGPD

- **Derecho al olvido**

Una de las principales características de la blockchain es que los **datos ingresados no son borrables ni rectificables**. Una vez que la transacción ha sido validada, no puede eliminarse.

Por tanto no podría ejercitarse el derecho al olvido en estos caso y por consiguiente se da un **incumplimiento** del RGPD.

- **Conservación limitada de los datos**

El artículo 5 del RGPD, enuncia que los datos personales solo deben mantenerse durante un periodo que no sea superior al necesario para los fines por los cuales se recogen.

Esto entra en conflicto claro con una de la **principales características** del blockchain, que es la inmutabilidad de los datos.

¿Revolución industrial?

Todas las revoluciones industriales se caracterizan porque el uso de tecnologías disruptivas, transforman la economía de los lugares donde se aplican y provocan el desarrollo económico del mundo.

"Con el blockchain pasamos del Internet de la información al Internet del valor",

La diferencia de esta cuarta revolución industrial con respecto a las anteriores es que en ésta las olas de innovación se producen simultáneas en el tiempo y no secuencialmente, como en las anteriores, con lo que el impacto será mucho mayor.