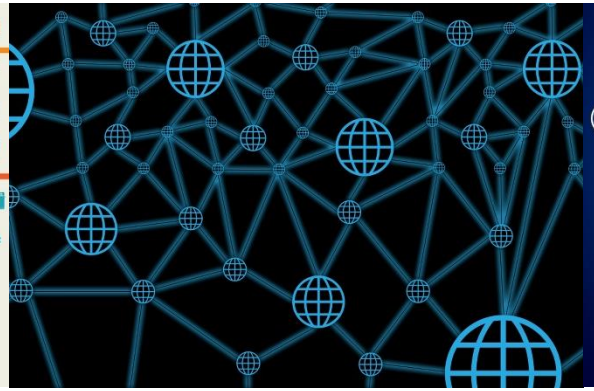
lis solutions
logistic intelligence & data analysis

Internet Distribuido:

de Blockchain a SOLID


Braian Gómez
Ingeniero de Datos

Técnico en Computación por el Instituto Universitario de Nuevas Profesiones y Diplomado en **Seguridad en Tecnología Informática y Telecomunicaciones** por el Instituto Universitario de Seguros.

Cuenta con una amplia experiencia en arquitectura, diseño, desarrollo y mantenimiento de sistemas informáticos.

Domina herramientas de desarrollo y lenguajes de programación como Java, .NET, PHP y Javascript, tecnologías de desarrollo como Spring, J2EE, AJAX y HTML5. Posee conocimientos de diseño y administración de bases de datos con tecnologías como Oracle, PL/SQL, MySQL y PostgreSQL.

Idiomas: inglés, castellano.

Experience Summary

Especialista en plataformas distribuidas usando tecnologías web y desarrollo de sistemas enfocados a gestión y almacenamiento de datos.

Algunos proyectos en los que ha participado:

- Desarrollo y puesta en producción de un sistema de gestión documental (proyecto MED) para **CVG EDELCA**, empresa de generación hidroeléctrica venezolana, utilizando software libre y realizando una migración total desde la plataforma NovaManage al sistema MED.
- Desarrollo de una plataforma de digitalización de documentos para **Movilnet**, compañía de telecomunicaciones venezolana.
- Desarrollo de aplicativos web con integración de la plataforma TronWeb en **Mapfre**.
- Líder Técnico del equipo Alfresco en **Incentro Spain**, liderando proyectos con empresas holandesas tales como **Infinitas Learning**, **VGGM**, **Blijfgroep** e **IBFD**.

Criptoanarquía

Definición

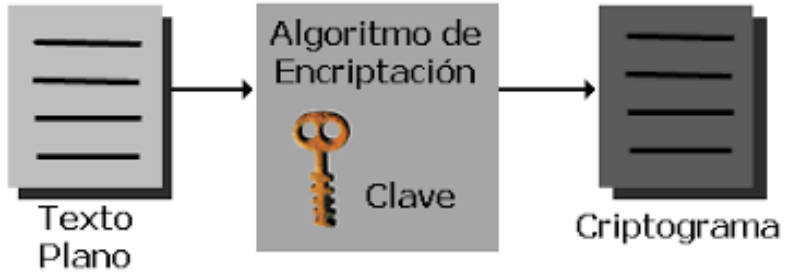
Ideología o estrategia que se muestra a favor de la utilización de la criptografía para hacer cumplir la privacidad y la libertad individual.

- Término acuñado por Timothy C. May en su Manifiesto Cripto Anarquista en el año 1988.
- La privacidad y el anonimato son valores fundamentales.
- Utilización de técnicas criptográficas como medio para garantizar la libertad.

Criptografía

Introducción a la criptografía

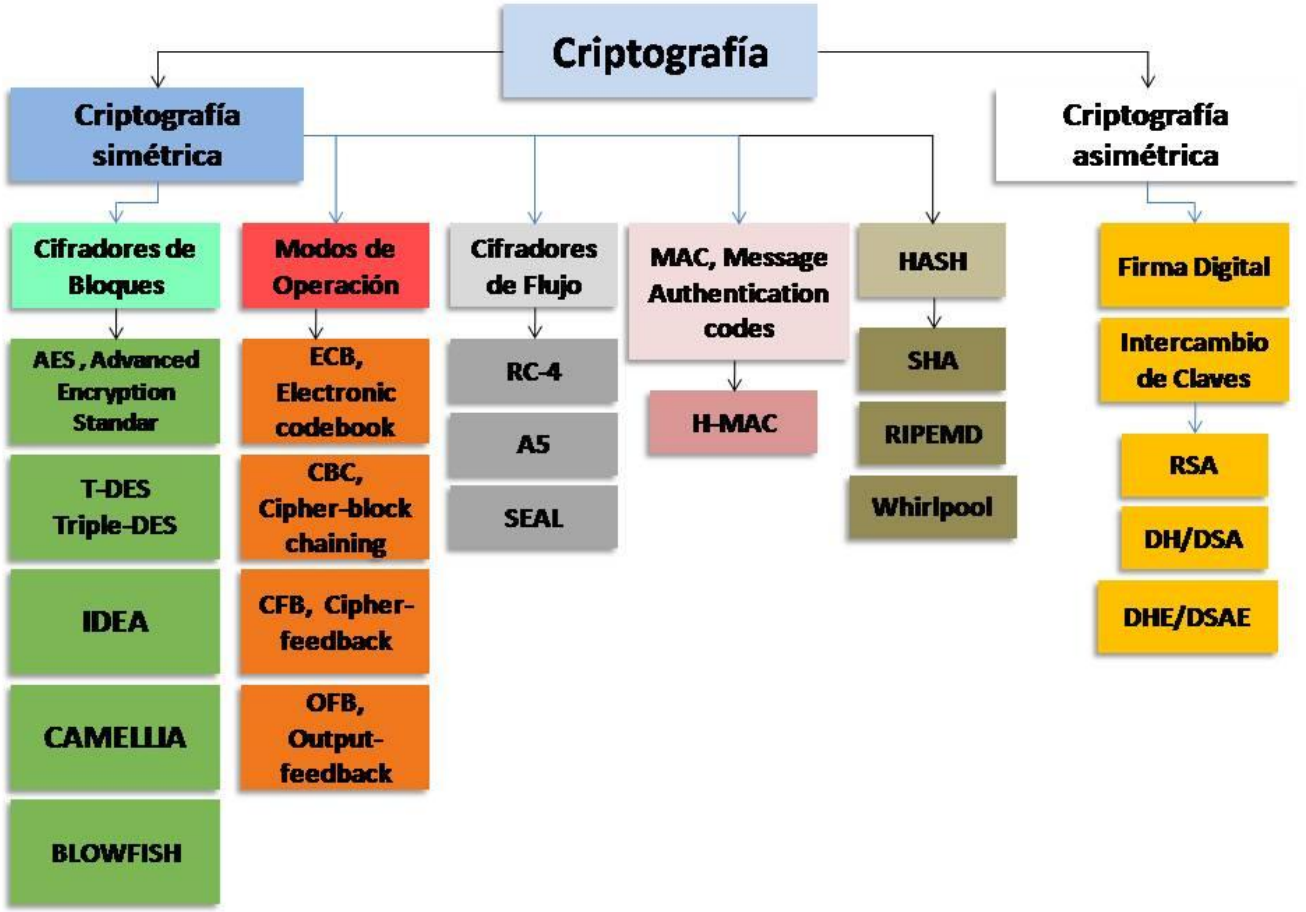
- Es una técnica para hacer que un mensaje sea confidencial.
- Proviene de las palabras griegas “krypto” y “graphos”, significa “escritura oculta”.
- Es el arte y la ciencia de cifrar información de modo que sólo pueda ser comprendida por los que tengan los medios para descifrarla.
- Requiere de un algoritmo de cifrado y una clave.



Criptografía

Tipos de algoritmos

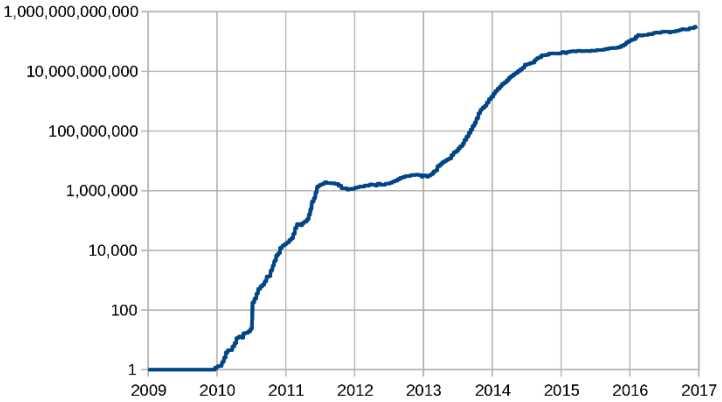
- **Simétrica:** Funciona con una sola clave secreta que debe ser compartida a todos los consumidores de la información.
- **Asimétrica:** También llamada de clave pública, permite trabajar con pares de claves: una clave compartida y otra secreta.
- **Hash:** Es un método que permite cifrar información de modo que no puede ser descifrada. Se utiliza para almacenar contraseñas de forma segura.



Bitcoin

Historia y Definición

- Paper publicado el 1 de noviembre de 2008 por **Satoshi Nakamoto: "Bitcoin: a Peer-to-Peer Electronic Cash System".** El 3 de Enero de 2009 se crea el primer bloque de la cadena.
- Resuelve el problema del **"doble gasto"** utilizando una plataforma de software distribuido.
- Introduce el concepto de "**Proof of Work**" (prueba de trabajo), en la que las transacciones son "minadas" por máquinas que deben **resolver un problema criptográfico**, obteniendo así un beneficio (tokens Bitcoin).
- Los mineros además de minar bloques **confirman las transacciones** que se efectúan en la red. En este caso, las transacciones son envíos de tokens de una cuenta a otra.
- Es la primera implementación de la tecnología de **cadena de bloques** (Blockchain).



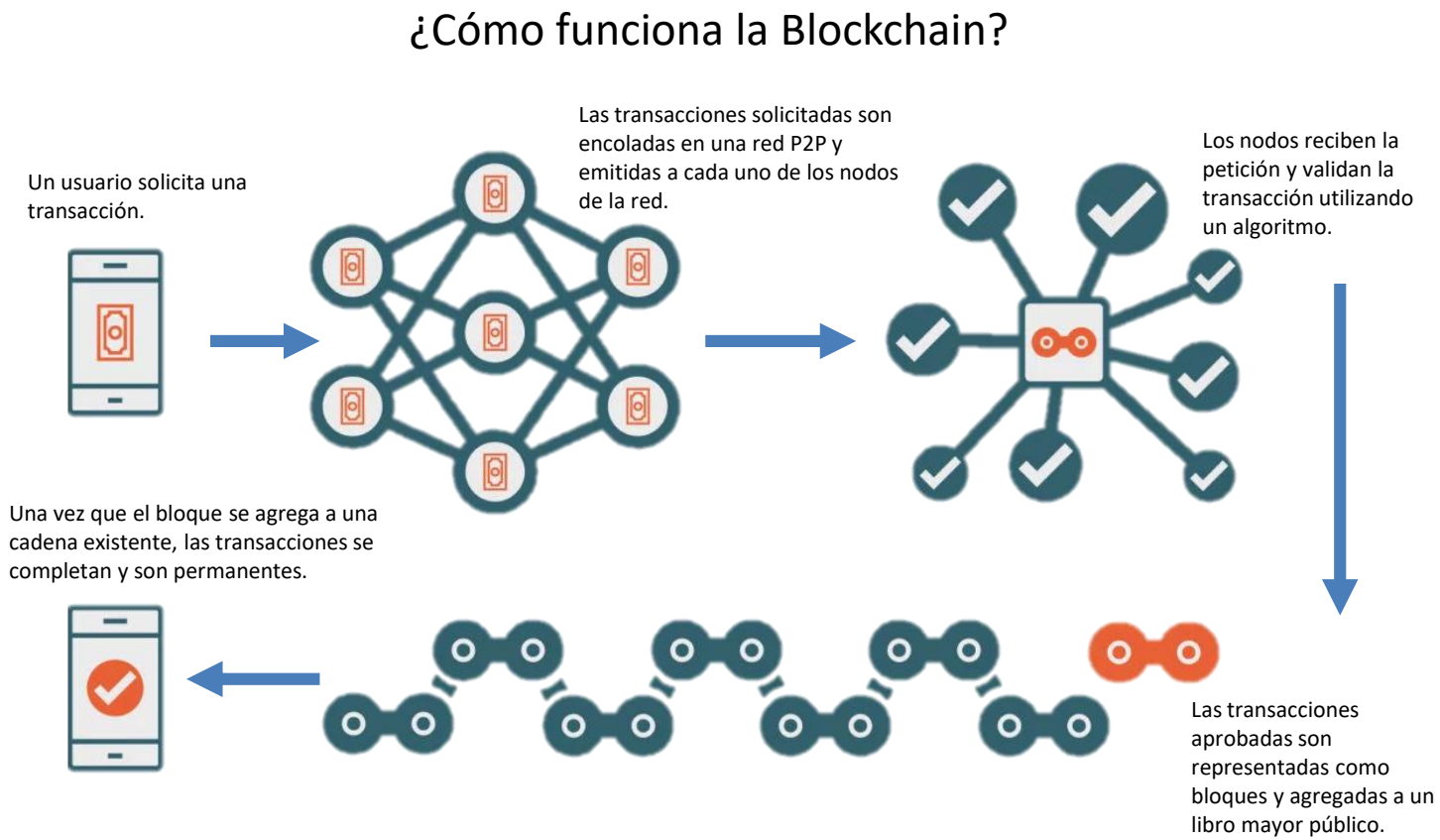
Dificultad de la minería de bitcoin (patrón logarítmico)


Precio histórico del bitcoin

Blockchain

Definición

- Blockchain significa "**Cadena de Bloques**": un método de almacenar datos de forma distribuida e inmutable.
- **Inmutabilidad**: una vez que el dato es almacenado no puede ser alterado o eliminado.
- **No repudio:** los datos almacenados tienen un origen identificable.
- **Confirmación:** los nodos validan que los datos almacenados sean correctos utilizando un mecanismo de **consenso.**
- Blockchain es un tipo de **DLT** (Distributed Ledger Tecnology).



Distributed Ledger Technology

Definición

- **Tecnología de Libro Mayor Distribuido**: permite almacenar datos como si se tratase de un libro contable, con movimientos, orígenes y destinos, teniendo un control de los datos que han entrado y salido de una entidad.
- La base de datos se distribuye en **nodos descentralizados**.
- Algunas implementaciones permiten desplegar **contratos inteligentes**.
- Es a lo que se le conoce como "Blockchain", aunque el término Blockchain es en realidad un tipo de DLT.
- Además de utilizarse para crear **monedas criptográficas**, puede ser utilizado para otros casos de uso como **certificación de origen**, **seguimiento de artículos físicos**, **identidad digital**, **cadena de suministro**, etcétera…

Smart Contracts

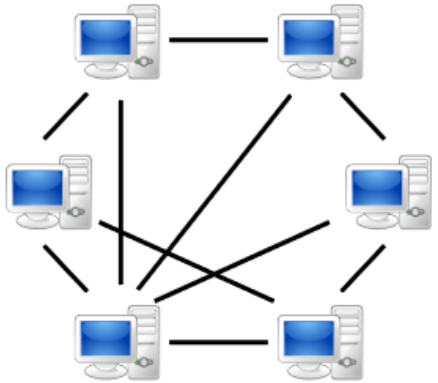
Contratos inteligentes – Ethereum

- Un contrato es un **acuerdo** entre dos o más partes que sigue una serie de reglas que deben cumplirse para que el acuerdo se realice.
- Un **contrato inteligente** no requiere de un tercero para garantizar el cumplimiento, sino que se ejecuta como un programa informático.
- Los contratos inteligentes son **invocados y ejecutados** a través de la red blockchain.
- Un contrato tiene como resultado **una serie de transacciones** que corresponden a las reglas estipuladas en forma de código informático.
- El lenguaje de programación para Smart Contracts en Ethereum es **Solidity**.

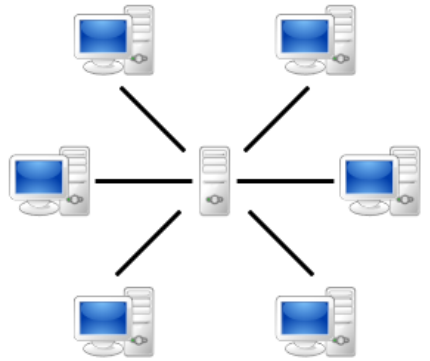
Redes Distribuidas

Definición

- Ausencia de un centro individual o colectivo.
- Los nodos se vinculan unos a otros de modo que ninguno tiene forma de filtrar o controlar la información que se transmite en la red.
- Requiere de una gran cantidad de recursos comparada con una red centralizada.
- El enrutamiento de los paquetes se hace a través de un algoritmo complejo (ej: DHT – tablas de *hash* distribuidas)



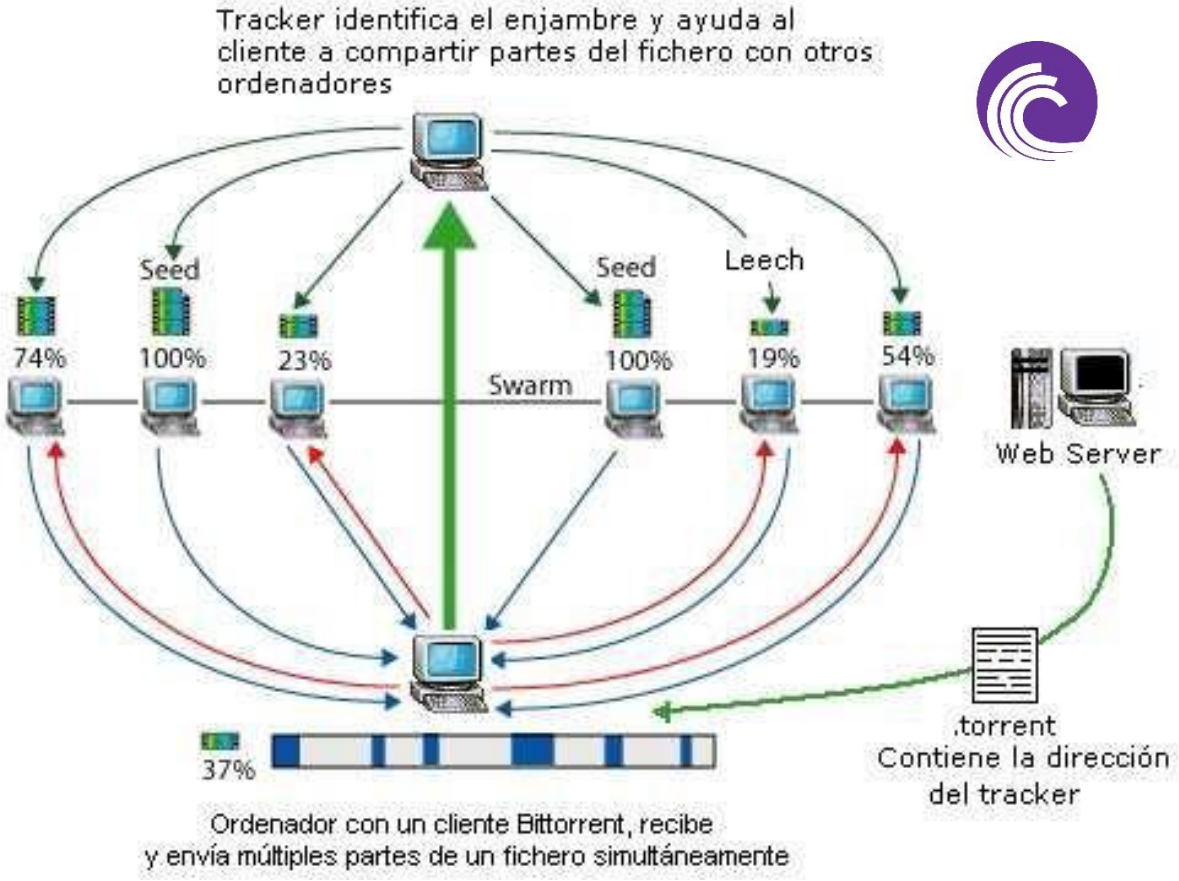
Red descentralizada (P2P)



Red centralizada (Cliente-Servidor)

Redes Distribuidas

Bittorrent

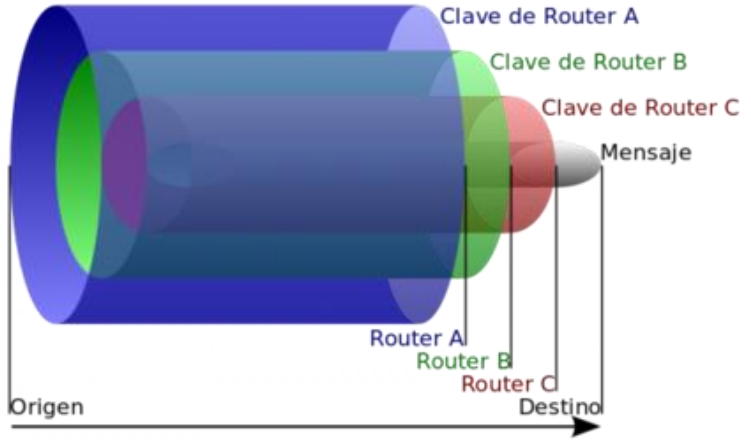


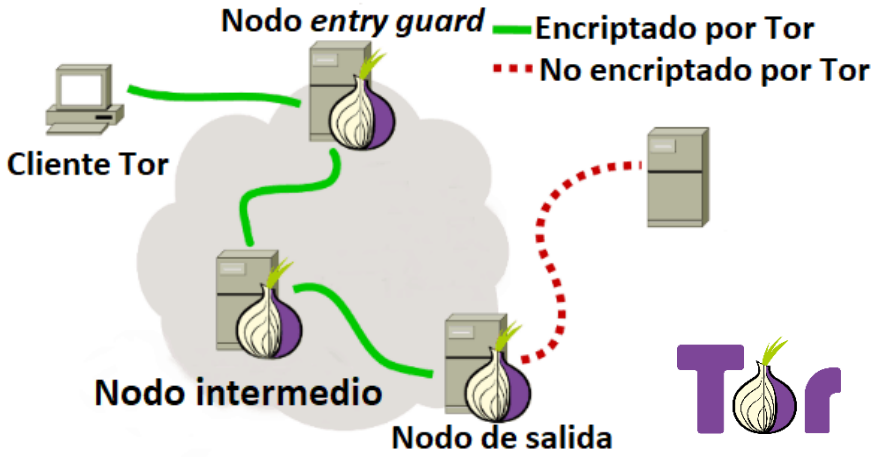
- Protocolo para intercambio de archivos punto a punto (*P2P*).
- Permite a los usuarios descargar y subir el archivo de forma simultánea en un "enjambre" (*swarm*).
- Cuando un cliente descarga el archivo completamente se convierte en una semilla.
- El archivo se distribuye a través de muchos nodos, proporcionando así redundancia y tolerancia a fallos.

Redes Distribuidas

TOR: Onion Routing

- Software de código abierto diseñado para mantener el anonimato en internet.
- Es una red superpuesta (red virtual).
- Utiliza nodos distribuidos y criptografía para ocultar el origen de la petición.
- Usa tablas de hash distribuidas (DHT) para garantizar el anonimato de los servicios ocultos (.onion services).
- Es una red distribuida en lo que respecta a los nodos, no siendo *peer-to-peer* completamente.

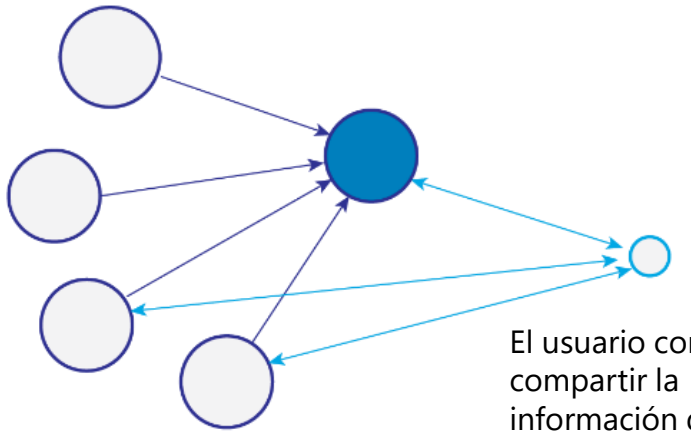




Redes Distribuidas

ZeroNet

Un usuario busca otros usuarios que tengan webs compartidas y descarga información desde los pares



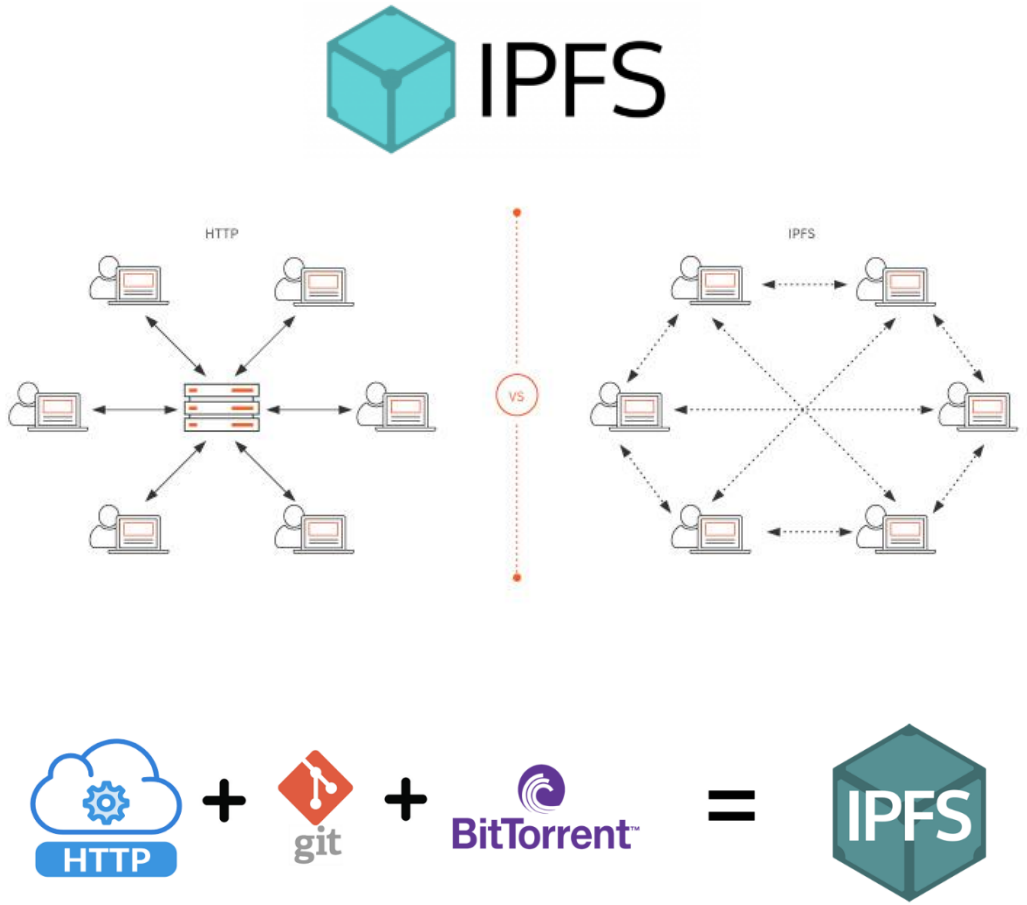
El usuario comienza a compartir la información descargada

- Red de internet descentralizada conectada con protocolo p2p.
- Utiliza la criptografía del Bitcoin para generar direcciones y la red de Bittorrent.
- Los websites son completamente descentralizados.
- Los usuarios alojan contenido por defecto a través de la red Bittorrent.
- El contenido se verifica usando hashes.
- No es anónimo por defecto, pero puede usar TOR.

Redes Distribuidas

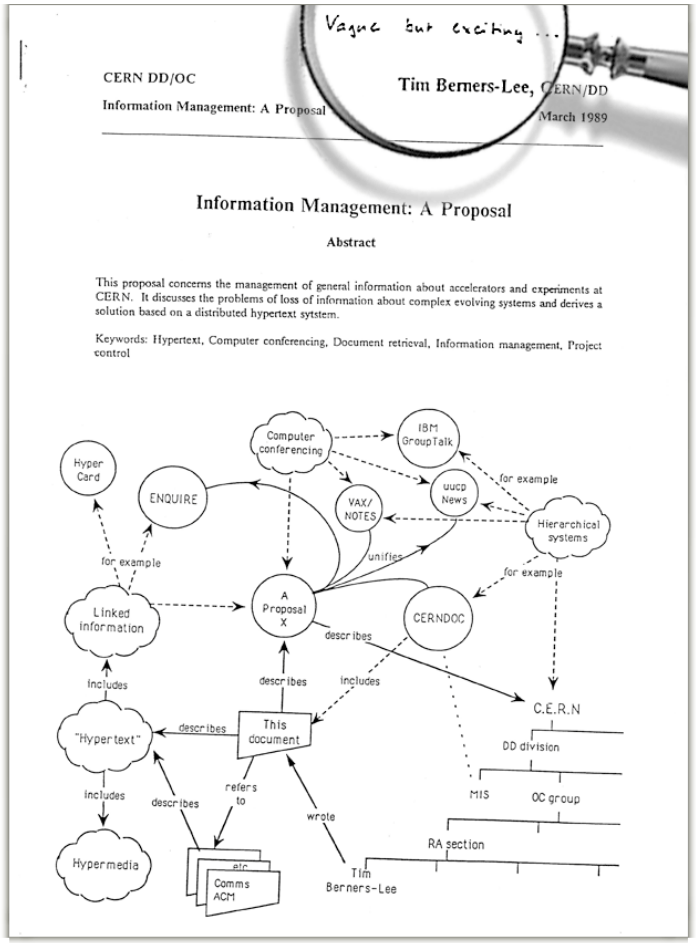
IPFS: Inter Planetary File System

- Protocolo para almacenamiento y distribución de *hipermedia* en un sistema de ficheros completamente distribuidos.
- Utiliza distintos protocolos y técnicas: HTTP, GIT/Merkledag, BitTorrent, DHT
- Los nodos actúan como cliente y servidor al mismo tiempo y están conectados con todos los demás nodos.
- Aspecto similar a la *web* actual.



SOLID

Historia

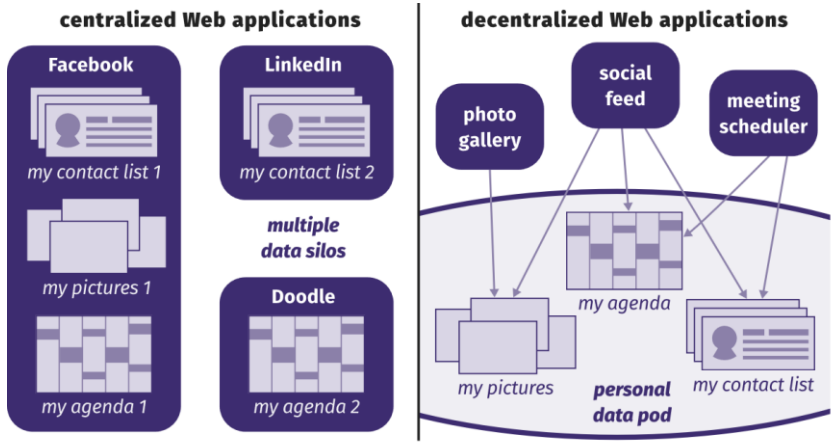


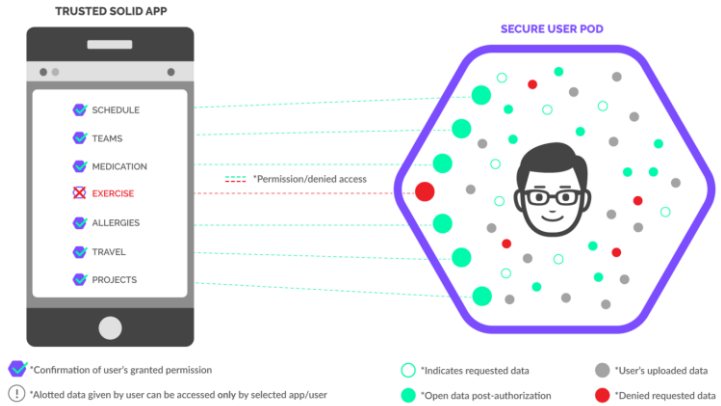
- Sir **Tim Berners Lee** – Creador de la web
- A raíz del escándalo de **Cambridge Analítica** con Facebook decide crear la startup **Inrupt**
- Propone un concepto de **web descentralizada** llamado **SOLID** (Social Linked Data)

SOLID

Características

- **Propiedad de los datos:** los usuarios tendrán la libertad de escoger dónde se almacenan sus datos y quienes están autorizados para consumirlos. Esto se logra separando el contenido de las aplicaciones.
- **Diseño modular:** Ya que las aplicaciones están separadas de los datos que producen, los usuarios serán capaces de cambiar de aplicaciones y servidores de almacenamiento sin perder datos o contenido.
- **Reutilización de datos existentes:** Los desarrolladores podrán crear nuevas aplicaciones o mejorar las existentes, todo mientras reutilizan los datos creados por otras aplicaciones.

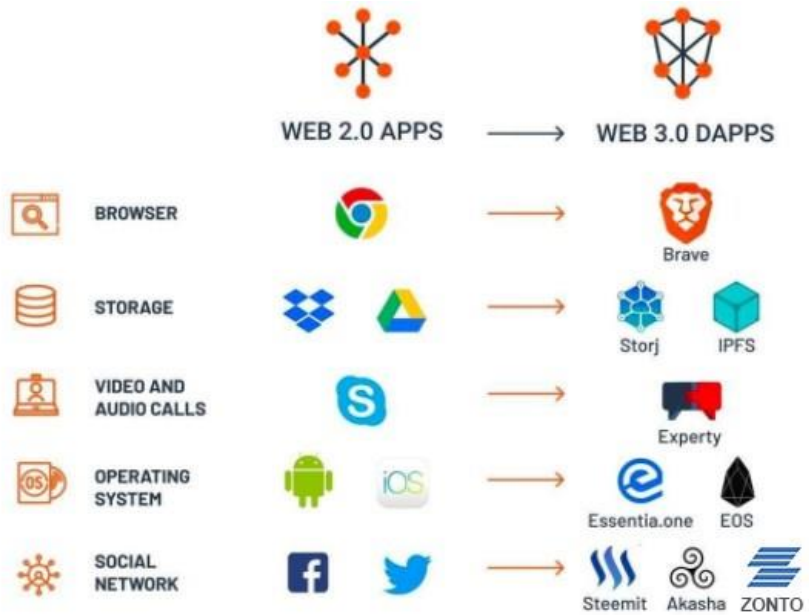




Internet del Futuro

Web 3.0

Web 3.0 – semántica y descentralizada

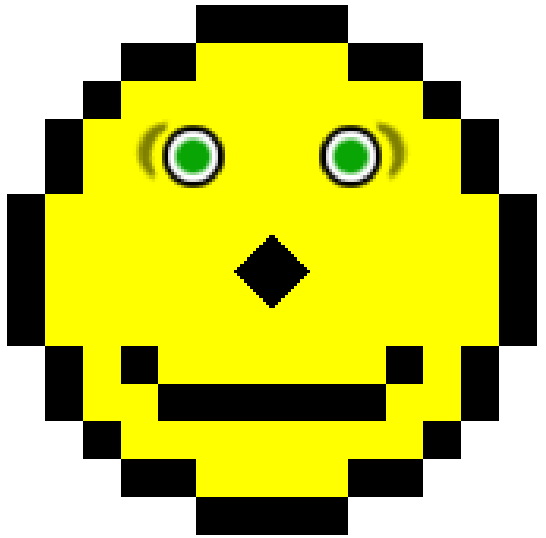


- **Información semántica:** a través de metadatos se categoriza la información de forma semántica, es decir, crear las conexiones simbólicas utilizando los metadatos para contextualizarlos. Por ejemplo, el estándar **RDF** de la **W3C** permite crear modelos semánticos a partir de metadatos.
- **Aplicaciones Descentralizadas:** las aplicaciones descentralizadas utilizan tecnologías de comunicación distribuidas, dando más control al usuario sobre sus datos, y evitando la dependencia de un solo proveedor de almacenamiento (Google, Facebook, Amazon…). Las aplicaciones descentralizadas **conectan directamente proveedores con consumidores**, sin necesidad de un servidor central u organismo que controle las conexiones.

Conclusiones

Necesidad de la Web 3.0

- Preservar el anonimato.
- Aumentar la privacidad.
- Evasión de la censura y control por parte de organismos centralizados.
- Control por parte del propietario de la información.
- Información contextualizada.
- Tolerancia a fallos ocasionados por falta de redundancia.



lis solutions

logistic intelligence & data analysis

www.lis-solutions.eu
Info@lis-solutions.es
+34 945 06 59 50