

# Curso de especialización en Inteligencia Artificial y Big Data

---

UD06. CONVERGENCIA TECNOLÓGICA

Carlos Sáenz Adán

## Tabla de contenido

<b>1.</b>	<b><i>Introducción a la convergencia tecnológica</i></b>	<b>1</b>
<b>2.</b>	<b><i>Visión general</i></b>	<b>2</b>
<b>3.</b>	<b><i>Ventajas de la convergencia tecnológica</i></b>	<b>5</b>
<b>4.</b>	<b><i>Plataformas para la conexión tecnológica</i></b>	<b>6</b>
4.1.	Power Platform	8
<b>5.</b>	<b><i>Sistemas Blockchain</i></b>	<b>9</b>
5.1.	Dificultades de los sistemas descentralizados	10
5.2.	El concepto de bloque	11
5.3.	Qué es el Proof of Work y ajustes	12
	Dificultad de conseguir premio	13
	El modelo de consenso de Nakamoto	14
5.4.	Seguridad en Blockchain	15
5.5.	¡Blockchain es una estructura de datos descentralizada!	15
<b>6.</b>	<b><i>Introducción a Ethereum (Para saber más)</i></b>	<b>17</b>
6.1.	Ethereum: Un blockchain de propósito general	18
<b>7.</b>	<b><i>Conexión entre tecnologías</i></b>	<b>19</b>
<b>8.</b>	<b><i>Sistemas IoT</i></b>	<b>20</b>
<b>9.</b>	<b><i>Seguridad en la convergencia tecnológica</i></b>	<b>22</b>
<b>10.</b>	<b><i>Bibliografía</i></b>	<b>24</b>
<b>11.</b>	<b><i>Referencias</i></b>	<b>24</b>

## 1. Introducción a la convergencia tecnológica

Para analizar correctamente la convergencia tecnológica, es importante comenzar con la idea de que existe un conjunto de tecnologías que se aceleran exponencialmente. Esto tiene su impacto tanto en el aumento de las prestaciones como en la bajada de precio a lo largo de tiempo. Un ejemplo clásico es el de la Ley de Moore, enunciada en los años 60 por Gordon Moore, uno de los socios fundadores de Intel. Predijo que cada dos años los ordenadores serían el doble de potentes manteniendo su precio. Aunque en su predicción original Moore habló de un escenario de corto plazo, esta ley sigue siendo válida aún hoy en día<sup>1</sup>



**Implicaciones de la Ley de Moore.** Esta ley explica por qué el móvil que tienes es mil veces más pequeño, mil veces más barato y un millón de veces más potente que un supercomputador de los años 70.

Los circuitos integrados no es la única tecnología que tiene este tipo de crecimiento. En 2004 el director de ingeniería de Google, Ray Kurzweil, enunció la que se conoce como "Ley del rendimiento acelerado" [Kur04] por la que cualquier tecnología que se vuelve digital empieza a acelerarse de forma exponencial. Además, esta aceleración genera una realimentación positiva sobre otras tecnologías que aceleran aún más la propia aceleración<sup>2</sup>.



**Ley de rendimiento acelerado.** Según la ley de Kurzweil en este siglo vamos a vivir el equivalente a unos 20.000 años de cambios tecnológicos. Será el equivalente a condensar todos los avances desde el descubrimiento de la escritura a la aparición de Internet en 30 años.

En los últimos años se está haciendo más notable el efecto de la convergencia tecnológica. Los avances tecnológicos están solapándose con efectos potenciadores en otras disciplinas. Por ejemplo el desarrollo de nuevas vacunas se está acelerando por los avances en biotecnología junto con nuevos paradigmas en inteligencia artificial, big data y nanotecnología entre otros.

¿Por qué ahora es el momento de hablar de convergencia tecnológica? La revolución de la IA y el Big Data nos permite procesar una cantidad de datos enorme, permitiendo inferir resultados en fragmentos de segundo. Esto tiene aplicación en multitud de ámbitos industriales donde se recopilan datos de diversos tipos de sensores centralizados o distribuidos (por ejemplo mediante IoT) y se procesan para dar resultados en tiempo real que optimicen procesos y servicios. El precio y

---

<sup>1</sup> Aunque hay ciertas noticias que alertan del fin de la Ley de Moore alrededor del 2025 por limitaciones físicas en la tecnología de fabricación de los propios chips, varios autores [Wal16], [McB19] apuntan de un modo muy optimista por nuevos enfoques basados en computación cuántica, técnicas de inteligencia artificial y nuevas arquitecturas de chip.

<sup>2</sup> Entre estas innovaciones podemos destacar la propia inteligencia artificial, la computación cuántica, la nanotecnología, el IoT, la realidad aumentada y blockchain entre otras

la rapidez de servicio son dos factores fundamentales en muchos ámbitos de consumo, con una conexión directa con la percepción de calidad. En estas dos dimensiones la convergencia tecnológica y la aplicación de IA juega un papel determinante.

Por desgracia, muchas de las empresas y organizaciones consolidadas tendrán problemas para seguir el ritmo de esta convergencia acelerada. Según Foster [FK11] el 40 % de las empresas que aparecen en el famoso ranking Fortune 500 desaparecerán en 10 años reemplazadas por empresas emergentes que aún no existen.

## 2. Visión general

La ley de rendimiento acelerado tiene un fuerte impacto en la convergencia tecnológica y en la evolución en la vida de las personas. La vida del tatarabuelo de tu tatarabuelo era más o menos igual a la vida de su tataranieto. Sin embargo, ahora la tecnología tiene un fortísimo impacto en el mundo global y exponencial en el que vivimos. La organización y costumbres de la vida de las personas puede cambiar en cuestión de meses. Desde la aparición en 2007 del iPhone el número de dispositivos móviles a internet ha crecido exponencialmente (ver figura 4.1. En 2012, el número de smartphones y tablets con conexión a internet superaba al número de ordenadores (entre escritorio y portátiles juntos). En pocos años, los hábitos de consumo y publicación de información en redes sociales por parte de la humanidad también lo han hecho.

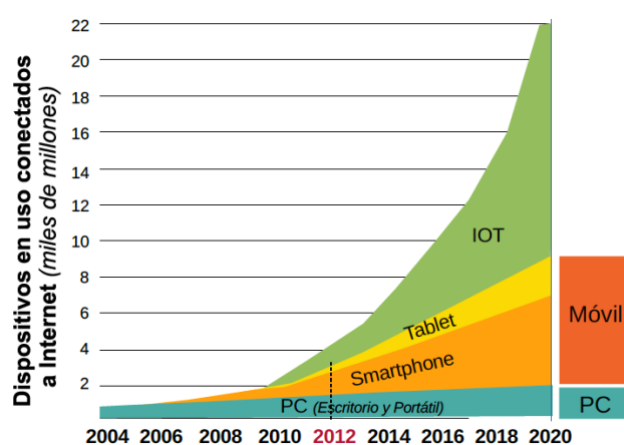


Figura 4.1: Evolución en el número de dispositivos conectados a internet. Fuente: Gartner IDC + Forbes (IOT). Diagrama de elaboración propia.

Diamandis y Kotler [DK20] identifican en su libro 9 tecnologías de crecimiento exponencial y una serie de agentes secundarios que están acelerando el ritmo del cambio en el mundo, así como el tamaño del impacto de esta convergencia tecnológica. Además de la Inteligencia Artificial y el Blockchain (cuya implicación será estudiada en secciones posteriores) las otras 7 tecnologías amplificadoras son las siguientes:

**Computación Cuántica.** A diferencia de la computación clásica donde un bit representa el fragmento más pequeño de información binaria (0 o 1), un cúbit (o bit cuántico) pueden estar en múltiples estados al mismo tiempo mediante superposición<sup>3</sup>. La computación cuántica despliega todo su potencial a la hora de manipular gran cantidad de datos de una vez, mientras que la computación tradicional se muestra eficaz en procesamiento secuencial. En 2002 Geordie Rose, fundador de una de las primeras empresas de computación cuántica - DWave enunció la Ley de Rose: “El número de cúbits de un ordenador cuántico se duplica cada año”. En la página de Rigetti Computing [www.rigetti.com](http://www.rigetti.com) se puede descargar el Toolkit.

Forest para desarrolladores cuántico. Forest se construye sobre Quil, un lenguaje con instrucciones híbridas para algoritmos con parte clásica y parte cuántica. Además, ofrecen el computador de 32 cúbits de Rigetti donde ejecutar los programas desarrollados.

**Redes – IoT (Internet of Things).** En la actualidad más de la mitad de los humanos de la tierra están conectados a internet con unos costes muy bajos. Con el despliegue de 5G se consiguen tiempos de latencia y ancho de banda que permiten la teleoperación desde cualquier lugar. Se tardará menos de 2 segundos en descargar una película completa en HD. La nueva red de satélites fabricados por Boeing O3B dará cobertura a todas las personas que hoy en día carecen de acceso de alta velocidad a Internet. La previsión es que para 2030 tengamos unos 500.000 millones de dispositivos conectados a la red (cada uno con decenas de sensores). Esta implantación de sensores conectados proporciona una ingente cantidad de datos sobre la que se pueden aplicar técnicas de procesamiento automático basadas en IA.

**Robótica.** No cabe duda de que los robots están entrando en nuestras casas y forman parte de nuestro día a día, realizando trabajos que son aburridos o peligrosos. Los desarrollos de Boston Dynamics sorprenden a la comunidad con máquinas adaptables a situaciones inesperadas, con movimientos rápidos y precisos. La robótica industrial ha evolucionado de máquinas que eran peligrosas y debían estar separadas de los operarios humanos al concepto de cobot (robot colaborativo) que trabajan de la mano de operarios humanos.. En la convergencia con las tecnologías exponenciales anteriormente descritas, los drones suponen la conexión de la robótica con sensores conectados y el control de los dispositivos de vuelo y motores mediante métodos de inteligencia artificial.

**Realidad Virtual y Realidad Aumentada.** Aunque como muchas de las tecnologías que hemos visto anteriormente, la Realidad Virtual y la Realidad Aumentada no son desarrollos nuevos, pero la convergencia tecnológica ha conseguido que ahora hayan alcanzado un punto de eclosión. Para el 2025 la previsión es que el mercado del videojuego alcance 11.000 millones \$, seguido por las aplicaciones sanitarias con 5.000 millones \$ y el uso industrial con más de 4.500 millones \$.

---

<sup>3</sup> La superposición se alcanza con temperaturas de trabajo muy bajas.

---

Dispositivos de reciente aparición en el mercado como las Oculus Quest 2 de Facebook, con una precisión de tracking libre menor de 1 milímetro y un precio menor de 400 euros auguran una rápida adopción en hogares de todo el mundo. Por su parte, las HoloLens 2 de Microsoft se han convertido en el dispositivo más extendido en aplicaciones de Realidad Aumentada (Mixta) de ámbito profesional.

**Impresión 3D.** Desde la aparición de las primeras impresoras 3D en los años 80, la convergencia tecnológica ha permitido importantísimos avances en todos los aspectos. Actualmente podemos imprimir en cientos de materiales diferentes; desde materiales inorgánicos (todo tipo de metales, plástico, hormigón...) hasta compuestos orgánicos (células, cuero y alimentos). Actualmente se realiza impresión 3D de prácticamente todo, desde prótesis ortopédicas hasta piezas de motores a reacción e incluso bloques de pisos. La complejidad de las piezas impresas aumenta con tiempos de producción y costes cada vez menores. Existen decenas de sitios donde ofrecen servicios de impresión muy competitivos (como [www.shapeways.com](http://www.shapeways.com)), y diversos fabricantes ofrecen impresoras 3D domésticas. La convergencia tecnológica con la informática ha permitido sacar nuevos productos de impresión, como la impresora que fabrica placas bases de Nano Dimension. La convergencia con la biotecnología ha permitido ya imprimir piezas de recambio para órganos humanos, como la impresión del primer vaso sanguíneo producido en San Diego en 2010.

**Nanotecnología y ciencia de los materiales.** A finales del siglo XIX, Thomas Edison tuvo que probar en más de un año cerca de 2.000 materiales antes de encontrar un material que le permitiera fabricar la primera bombilla eléctrica. Tuvieron que pasar varias décadas hasta que nuevas pruebas dieron con los filamentos de tungsteno, mucho más brillantes y resistentes que permitían fabricar bombillas más duraderas y brillantes. Actualmente las pruebas de materiales se realizan mediante simulaciones empleando ordenadores. Lo que hace años requería meses de trabajo hoy en día se realiza en horas. En 2011 en la Universidad de Carnegie Mellon se presentó la iniciativa del Genoma de los Materiales que emplea la IA para cartografiar los millones de combinaciones posibles de elementos y predecir las propiedades de los nuevos materiales que aún no existen. Estos avances permiten generar un mapa del mundo físico que facilita la generación de nuevos materiales a nivel de átomo. Este nivel de convergencia tecnológica ha permitido construir materiales más ligeros, resistentes y nuevos biomateriales que pueden implantarse en humanos sin rechazo.



Sin convergencia no es posible. Como explica el director de Applied Materials, O. Nalamasu, si se hubiera intentando construir una versión de un smartphone actual en los años 80, el dispositivo costaría unos 100 millones €, tendría la altura de un edificio de 5 plantas con el consumo energético de 20 viviendas familiares.

**Biotechnología.** La biotecnología se basa en la idea de transformar los elementos básicos de la vida (genes, proteínas y células) en herramientas manipulables. En el cuerpo humano tenemos unos 40.000 millones de células. Cada una de estas células tiene unas 6.400 letras codificadas en el ADN (la

mitad de cada progenitor). Desde que finalizó el proyecto de secuenciación del Genoma Humano en 2001 y que costó 100 millones de dólares (ver Figura 4.2), los precios y plazos de secuenciación han caído. Actualmente secuenciar un genoma humano lleva unos pocos días y cuesta menos de 800 euros. Empresas como Illumina prometen hacer lo mismo en una hora y por menos de 100 euros. Secuenciar el genoma de un modo rápido y barato va a permitir que técnicas de edición genética que permiten reparar el ADN que hay en el interior de las células o terapias basadas en células madre lleguen al mercado.

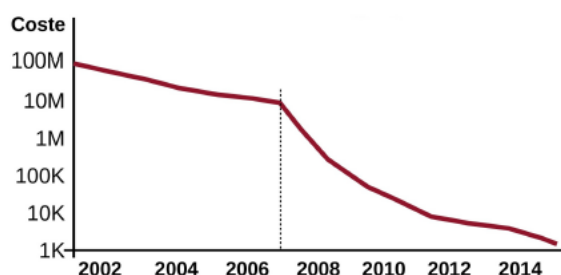


Figura 4.2: Evolución del coste de secuenciación del genoma desde 2002 en miles (K) y millones (M) de dólares. Fuente: Veritas Genetics 2015.

### 3. Ventajas de la convergencia tecnológica

En esta sección se identificarán algunas de las principales ventajas que presenta la convergencia tecnológica en el ámbito de la unificación de procesos, servicios, herramientas, métodos y sectores.

Como hemos visto en la sección anterior, gracias a la convergencia tecnológica es posible conseguir avances que de otro modo no serían posibles. Diamandis y Kotler [DK20] identifican una serie de ventajas que proporciona la convergencia:

- Ahorro de tiempo. El ahorro de tiempo puede verse como un motor de la innovación; realizar las tareas de un modo más rápido acelera el propio ritmo de progreso.
- Disponibilidad de capital. Nuevas posibilidades de financiación mediante crowdfunding, activos digitales que no podrá consumirse ni sustituirse (NFTs) e incremento de valor sin precedentes en empresas emergentes tecnológicas. Las 5 marcas más valiosas del mundo son los principales desarrolladores de IA: Google, Amazon, Facebook, Apple y Microsoft.
- Nuevos modelos de negocio. La convergencia tecnológica proporciona nuevos modelos de negocio. Hasta el momento de la convergencia tecnológica, los modelos de negocio habían cambiado lentamente a través de modelos de innovación sostenida (mejorar un producto o servicio a partir de pequeños pasos, muy costosos y constantes).
- Desmaterialización. La Wikipedia desmaterializó las enciclopedias. Primero iTunes y posteriormente Spotify desmaterializaron las tiendas de discos. Esto es lo que ocurre cuando los productos entran en contacto con tecnologías aceleradas.



**Decisiones estratégicas.** Una de las principales ventajas de la convergencia tecnológica está directamente relacionada con la mejora en la capacidad de toma de decisiones estratégicas en un negocio conectado. La disponibilidad de gran cantidad de datos y el análisis inteligente de los mismos pueden suponer una enorme ventaja a la hora de tomar decisiones estratégicas.

## 4. Plataformas para la conexión tecnológica

A continuación se comentarán algunas de las plataformas y sistemas más extendidos que facilitan la conexión tecnológica. En la sección 4.1 secciones se analizarán las características principales de las plataformas elegidas para realizar los ejemplos de este capítulo.

El término Glue Code se utiliza para definir el código empleado para conectar componentes de software que inicialmente no son compatibles. Habitualmente el glue code no se escribe en el mismo lenguaje en el que están definidas las aplicaciones a conectar, sino que suelen emplearse lenguajes interpretados de alto nivel<sup>4</sup> que permiten el desarrollo rápido (y normalmente con cierto impacto en el rendimiento y en la eficiencia).

Este tipo de código es habitual cuando es necesario integrar diferentes servicios en plataformas heterogéneas (por ejemplo Amazon y Google), de modo que el glue code sirve para conseguir la convergencia tecnológica entre los flujos de trabajo de estos servidores que, de otro modo, serían incompatibles. Para evitar que este código se transforme en el temido spaghetti code cuando aumenta su complejidad, es necesario utilizar frameworks que faciliten el desarrollo y garanticen la robustez y mantenibilidad de la solución.

Una tendencia muy extendida actualmente es el uso de tecnologías que facilitan la preparación y combinación de datos (incluyendo transformación, normalización y tratamiento de los datos) en un entorno sin servidores explícitos en la nube. Así, las plataformas Cloud facilitan la convergencia tecnológica escalando automáticamente los recursos necesarios para la ejecución de los trabajos de integración de datos. Algunas de las plataformas en la nube más extendidas para facilitar la convergencia tecnológica son las siguientes:

- AWS Glue. Servicio de integración de datos en la nube de Amazon. Incorpora mecanismos avanzados como el descubrimiento automático de esquemas de datos, definición de flujos de datos en streaming (en tránsito), definición visual de nodos de tratamiento (mediante AWS Glue Studio) y replicación de datos en varios almacenes de datos con vistas materializadas (soporte mediante AWS Glue Elastic View). Puede verse como una plataforma en la nube ETL (Extract, Transform, Load) que da soporte para mover los datos desde diversas fuentes a un data warehouse específico. En el caso de AWS Glue existe una conexión directa con el servicio específico de almacén de datos de AWS: Redshift.

---

<sup>4</sup>Algunos ejemplos de lenguajes utilizados para *glue code* son JavaScript, Perl, PHP, Python, Ruby, VBScript, Bash Script y PowerShell entre otros.



- Integrate.io. Plataforma que define un flujo de trabajo ETL en la nube. Al igual que AWS Glue dispone de servicios avanzados de replicación de datos en tiempo real. Proporciona flujo de trabajo visual y soporta integración en los almacenes de datos más extendidos: AWS Redshift y Snowflake.
- Microsoft Power Automate. Motor de integración de aplicaciones y de automatización en tareas de conversión y tratamiento de datos que forma parte de la suite Power Platform de Microsoft (ver sección 4.1). Será estudiado en detalle a lo largo del capítulo.
- Boomi. Comenzó a ofrecer sus servicios en 2007 siendo la primera plataforma en ofrecer servicios iPaaS (integration Platform as a Service). Fue la primera plataforma que definía un sistema de nodos visuales que permite construir procesos de integración mediante drag&drop. Recientemente la compañía ha sido adquirida por Dell y la plataforma forma parte de la nube AtomSphere.
- Zapier. Plataforma de automatización de tareas de integración de aplicaciones web. Puede entenderse como un traductor de APIs web que permite la definición de Zaps: flujos de conexión entre aplicaciones que definen acciones que son disparadas a partir de ciertos eventos (triggers).

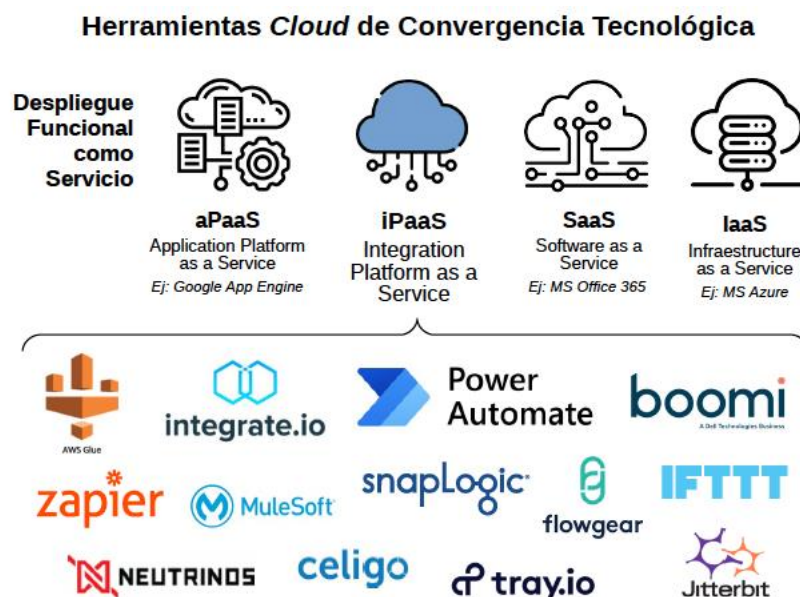


Figura 4.3: Desde el punto de vista de las plataformas de integración Cloud que podrían ser catalogadas como iPaaS, existe una amplia oferta de alternativas tecnológicas.

Existen multitud de proveedores que ofrecen servicios cloud para la integración de plataformas existentes y tratamiento de datos, como Mulesoft, SnapLogic, Celigo, Jitterbit, Flowgear o Neutrinos<sup>5</sup> dentro del ámbito profesional o IFTTT y Tray.io en el ámbito de usuario final entre otras. Dependiendo de las necesidades específicas de cada proyecto, puede ser conveniente analizar tanto las prestaciones como los costes asociados a cada proveedor. De igual modo también es posible combinar las soluciones proporcionadas por diferentes plataformas de iPaaS.

## 4.1. Power Platform

Una de las plataformas más populares de sistemas cloud para la conexión tecnológica es Microsoft Power Platform. En el ecosistema de Power Platform se cuenta con varios módulos y componentes que proporcionan servicios en la nube para crear e integrar aplicaciones empresariales existentes de forma rápida y eficiente (ver Figura 4.4). Algunos de los módulos principales de la plataforma son los siguientes:

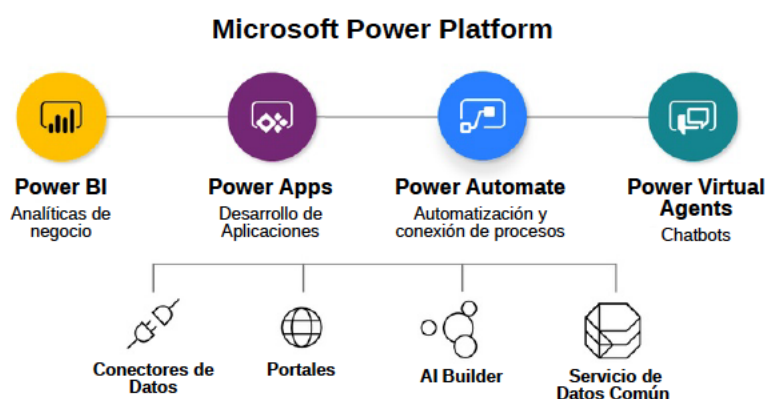


Figura 4.4: Principales módulos de la Microsoft Power Platform.

- **Power Apps**. Define un conjunto de componentes y plantillas de alto nivel para crear aplicaciones empresariales para PC y dispositivos móviles, así como portales web de acceso público utilizando el enfoque de desarrollo casi sin código.
- **Power Automate**. Permite la integración y conexión de aplicaciones existentes, así como la automatización de tareas de conversión y tratamiento de datos. Este motor de conexión de flujos se estudiará en detalle en la sección 4.5 y siguientes.
- **Power BI**. Herramienta de análisis y generación de informes empresariales muy consolidada y flexible. Ha sido estudiada en el capítulo correspondiente del módulo de Sistemas de Big Data de este curso.
- **Power Virtual Agents**. Herramienta que permite crear chatbots conversacionales que respondan preguntas de clientes o visitantes de una web. Construye bots que pueden desplegarse como componentes web, aplicaciones móviles o integrarse en diversas aplicaciones como Teams, Skype, Cortana, Facebook, Slack y Telegram entre otras.
- **AI Builder**. Proporciona un conjunto de modelos de IA precompilados que facilitan la realización de predicciones, detección de objetos, clasificación y análisis del lenguaje natural entre otras. Estos modelos se pueden incorporar casi sin código mediante conectores integrados en la Power Platform.

La Power Platform define dos nuevos conceptos que deben entenderse a la hora de integrar correctamente servicios y aplicaciones: el Modelo de Datos Común (CDM) (Common Data Model) y el Servicio de Datos Común (CDS) (Common Data Service).

El CDM está formado por un conjunto de esquemas (de datos) y un sistema de metadatos. El modelo define un conjunto pequeño de entidades principales que no están relacionadas con ningún ámbito de trabajo, además de un conjunto extenso de entidades que sí dependen de un dominio de aplicación concreto (banca, salud, educación, automoción, media y ONGs entre otros).



**Modelo de Datos Común (CDM).** El objetivo principal del CDM es definir una plataforma común para la integración de datos y el desarrollo de aplicaciones. Fue inicialmente presentado por el consorcio de Microsoft, Adobe y SAP como parte de la *Open Data Initiative*.

El CDS (ver Figura 4.4) se encarga de establecer la base sobre la que se construyen las aplicaciones basadas en modelos. Este tipo de aplicaciones se definen con dos componentes: un identificador (nombre y dirección), y un Site Map (esquema de navegación). En la construcción de estas aplicaciones basadas en modelos se establecen diversos modelos de automatización y conexión de componentes.



**Servicio de Datos Común (CDS).** El objetivo principal del CDS es dar la implementación necesaria del CDM para almacenar los datos para las aplicaciones.

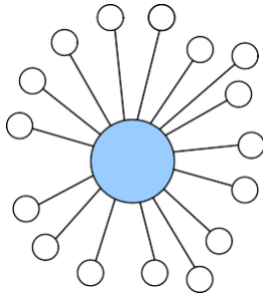
## 5. Sistemas Blockchain

Para explicar los sistemas basados en Blockchain es necesario primero introducir el concepto de los sistemas descentralizados frente a los sistemas centralizados.

En los sistemas centralizados, el servicio se construye a partir de un conjunto de nodos centrales que gestionan el procesamiento de la red. Esto facilita mucho la gestión del entorno de explotación, pero también tiene muchos aspectos negativos. Si hay algún fallo en los servidores centrales, el sistema deja de funcionar.

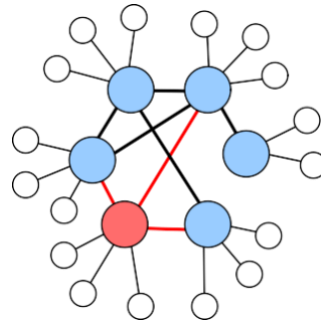
Por su parte, los sistemas descentralizados se basan en nodos donde cada uno de los equipos gestionan tanto los datos como el procesamiento, coordinándose de forma colectiva para la toma de decisiones. De este modo, si alguno de los nodos deja de funcionar, el resto de los nodos puede seguir operando sin ningún problema.

Sobre esta idea de descentralización se basan multitud de tecnologías actuales: criptomonedas, NFTs, contratos inteligentes e inteligencia artificial descentralizada entre otros.



Sistema Centralizado

Los nodos se conectan a un servidor central



Sistema Descentralizado

No existe servidor central.  
Todos son iguales

Figura 4.19: Sistemas centralizados Vs. Sistemas descentralizados. En caso de fallo de algún nodo de servicio (representado en rojo, en la figura de la derecha), los sistemas descentralizados siguen operando sin problemas.

## 5.1. Dificultades de los sistemas descentralizados

Aunque las ventajas de este enfoque descentralizado son claras, las dificultades para llevarlo a cabo también son igualmente relevantes. Hay que pensar en este tipo de redes como aquellas en las que todos los nodos se comportan como iguales. No hay la figura de ningún nodo que actúe de “coordinador” de la red.



**No te fíes ni de tu sombra.** Imaginemos por ejemplo que en un grupo de amigos queremos decidir qué película vamos a ver al cine. Lo más sencillo será establecer un sistema de votación, de modo que la película más votada será la que veremos todo el grupo. En un sistema descentralizado el método de votación tendrá que diseñarse de modo que nadie atesore todos los votos y tenga la capacidad de realizar el conteo final de votos. Si se hiciera así, tendríamos un sistema centralizado: ¿qué ocurriría si ese “amigo” quisiera salirse con la suya y hacer trampas en el proceso para ver la película *romantica* que sólo le apetece ver a él?.

Una de las principales ventajas que se persiguen con los sistemas descentralizados es que no es necesario confiar en nadie, el propio diseño de la red y el método de operar hace que el sistema funcione de por sí.

Este tipo de redes donde todos actúan y sirven como iguales se denominan redes Peer-to-peer (o P2P). Una red P2P muy extendida actualmente es Bittorrent. Cuando alguien descarga un archivo de esta red, el archivo no está alojado completamente en los servidores centrales de la red: hay un conjunto de usuarios que tienen fragmentos del archivo. Todos los nodos de la red comparten y descargan trozos de ese archivo, trabajando como iguales. Un archivo .torrent contiene la localización de las diferentes piezas que forman el archivo de destino. Estos pequeños fragmentos (normalmente de 256KB) se localizan en un número de máquinas diferentes, y se descargan

paralelamente. Cuando se han descargado todos los fragmentos se puede ensamblar el archivo final, que ya será utilizable.

Basándose en esta idea de P2P, en 2009 se publicó el paper titulado “Bitcoin: A peer-to-peer electronic cash system”, firmado por el pseudónimo de Satoshi Nakamoto. En este paper, que todavía no se sabe quién (o quienes) los escribieron, el autor proponía una solución para el intercambio de dinero entre personas sin ninguna institución central que controle las transacciones.

Puedes acceder al artículo en el siguiente enlace:

<https://assets.pubpub.org/d8wct41f/31611263538139.pdf>

De forma similar a como en Bittorrent los usuarios de la red comparten trozos de los archivos. En Bittorrent estos fragmentos se corresponden con el contenido de los archivos a descargar. En Bitcoin los usuarios comparten trozos de las transacciones económicas que se están realizando en la red. En realidad es un registro de movimientos de dinero que se realizan entre los usuarios de la red. La moneda no es más que ese enorme registro de transacciones. Por ejemplo, si el Sr. Satoshi me compra un chalet que vendo en la playa por 50 bitcoins, esa transacción (Satoshi

→ Carlos [50BTC]) primero se comprobaría que puede ser realizada (es decir, si el Sr. Satoshi dispone de esos 50 BTCs) y después se registraría, siendo propagada a todos los nodos de la red que mantienen el histórico de transacciones.

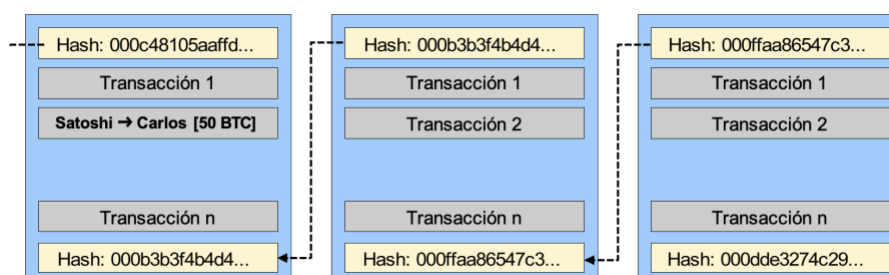


Figura 4.20: El concepto de bloque como conjunto de transacciones agrupadas con un enlace al anterior bloque que fue incluido en la cadena.

## 5.2. El concepto de bloque

El problema viene cuando se tienen que registrar todas estas transacciones en el mismo orden. Es muy fácil que, con tal cantidad de máquinas interviniendo a la vez, todo se desincronice, ya que cada máquina tiene su propio reloj interno.

¿Se pueden sincronizar relojes de modo que todos tengan exactamente la misma hora? Es muy complicado sin tener que depender de nodos centrales en la red. En el enfoque de blockchain queremos evitar cualquier nodo central de la red, por lo que un servidor de tiempo central no es posible en este enfoque. Una caída de este servidor de tiempo central y la red dejaría de operar de un modo correcto. Tampoco es posible que los nodos se comuniquen el tiempo entre ellos, porque

---

el hecho de tener que hacerlo por Internet y de un modo absolutamente distribuido entre todos, hace que la sincronización perfecta no sea viable.

Una posible idea es agrupar un conjunto de transacciones que ocurren en intervalos de tiempo cercanos en un bloque. El trabajo de cada nodo será estar escuchando todas las transacciones, verificando que son correctas (que el que realiza la transacción tiene fondos suficientes para realizarlos<sup>5</sup>) e ir agrupándolas en un bloque.



El trabajo de un nodo básicamente es escuchar transacciones, verificarlas y crear un paquete de transacciones. Este paquete se denomina **Bloque**. Cuando el nodo lo tiene listo, lo compartirá con el resto de miembros de la red. De este modo todos los nodos tendrán el mismo registro de transacciones.

El problema viene en que otros nodos estarán haciendo justo el mismo trabajo, y tendrán también bloques con transacciones verificadas. Estos nodos también querrán compartir su registro de transacciones en un bloque con el resto de nodos de la red. ¿Cómo se llega entonces a un consenso de qué bloque aceptar?. ¿Cuál de ellos se adopta como el oficial?

Podemos pensar que una votación podría ser útil en este caso. Si cada ordenador votara eligiendo un bloque, resolveríamos el problema. Sin embargo, esta aproximación no es válida. Es muy sencillo para una máquina hacerse pasar por un alto número de ordenadores, generando IPs virtuales por ejemplo. Un ataque de este tipo permitiría generar miles de votos sin esfuerzo, corrompiendo así la integridad del sistema de voto.

### 5.3. Qué es el Proof of Work y ajustes

¿Cómo se resuelve en Blockchain entonces? Cada nodo tiene que resolver un problema criptográfico complejo de modo que para votar tiene que certificar que es una máquina de verdad (y que no se está haciendo pasar por múltiples máquinas). Esta votación basada en trabajo (ganarte la participación garantizando que eres una persona y no varias) es lo que se conoce como “Prueba de trabajo” (Proof of Work).



La prueba de trabajo en Blockchain se basa en el algoritmo SHA-256 que utiliza funciones *hash* criptográficas. Una función *hash* es un algoritmo que transforma un conjunto de datos diversos (en este caso un bloque de transacciones), en un único valor de longitud fija: el “hash”. En el caso de SHA-256, la longitud de la cadena es de 256 bits. Este hash es una cadena única para esa entrada. Cualquier modificación mínima; un único bit en la entrada, genera un hash totalmente distinto. El valor hash calculado es único y es irreversible, y puede ser utilizado para verificar la integridad de copias de un dato original.

---

<sup>5</sup> Este trabajo en realidad es sencillo, basta con analizar el histórico de transacciones realizadas y validar que esta se puede llevar a cabo

En Blockchain se utiliza este algoritmo de modo que la prueba de trabajo es la siguiente: en cada bloque hay un espacio reservado para incluir un número. Una vez construido el bloque con las transacciones, se puede cambiar este número mágico de modo que el resultado del Hash SHA-256 dé como resultado un valor hash con un determinado número de ceros al principio. El enigma criptográfico se reduce entonces a conseguir averiguar con qué número mágico incluido en el bloque conseguimos como salida un valor hash con un número determinado de ceros. La única forma de resolverlo es ir probando números hasta que alguno dé la solución correcta.

### Dificultad de conseguir premio

La dificultad representa lo difícil que es encontrar el hash necesario para minar un nuevo bloque en la Blockchain asociada a la prueba de trabajo. La dificultad representa el número de combinaciones diferentes que pueden darse para que los mineros adivinen el hash. A mayor dificultad, mayor será el trabajo que tendrán que hacerlo para crear un nuevo bloque. En el caso de bitcoin la dificultad se ajusta cada 2 semanas para que los nuevos bloques se añadan, de media, cada 10 minutos. Si más mineros se unen a la red Bitcoin, contribuyendo así con más poder de cómputo para el hash, la dificultad aumentará y se ajustará para que los mineros descubran el hash en aproximadamente cada 10 minutos.

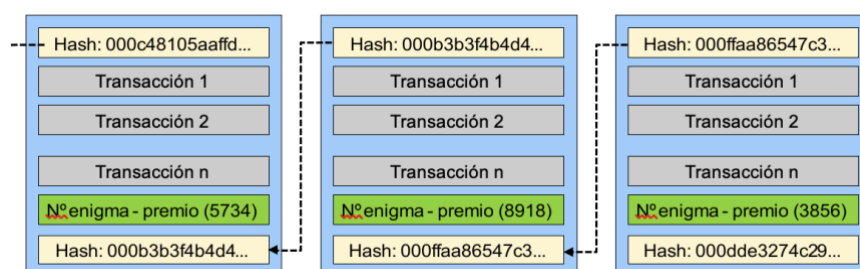



Figura 4.21: El concepto de bloque actualizado, incluyendo el número necesario para resolver el enigma criptográfico de modo que la nueva dirección de bloque tenga el número de ceros necesario al inicio.

La dificultad se ajusta cambiando el número de ceros que deben generarse consecutivamente al inicio del hash. A mayor número de ceros, mayor dificultad para que toque la lotería.

En <https://www.blockchain.com/explorer> se puede ver la cadena de bloques de Blockchain, que es totalmente pública. En el momento de escritura de este documento (7 abril 2024), el último bloque publicado es el 838156.





←

→

# Bitcoin Bloque 838.156

Minado el April 07, 2024 05:17:27 • [Ver todos los bloques](#)

AntPool

**Coinbase Message** • Mined by AntPool Q' z>mm m7N s0iX[BX''hYMX'p.; M]9hF8Dw

Un total de 3119,43 BTC (\$217,674.485) se enviaron en el bloque, siendo la transacción media 0,9773 BTC (\$0.00). AntPool ganó una recompensa total de 6,25 BTC (fiatsymbol)418.681. La recompensa consistía en una recompensa de base de 6,25 BTC \$418.681 con un pago de recompensa adicional de 0,1041 BTC (\$0.00) pagado como tasas de las transacciones 3192 que estaban incluidas en el bloque.

## Detalles

Función hash	00000-ee169 ☾	Profundidad	1
Capacidad	172.34%	Tamaño	1.887149
Distancia	14m 42s	Versión	0×2983e000
BTC	3119,4274	Raíz de Merkle	0d-97 ☾
Valor	\$217,674.485	Complejidad	83.126.997.340.024,61
Valor hoy	\$217,522.069	Número de un solo uso	3.386.921.587
Valor medio	0,9772642183 BTC	Bits	386,097.875
Valor mediano	0.000138618 BTC	Peso	3.993.696 WU
Valor de los ingresos	3119,53 BTC	Acuñado	6,25 BTC
Valor de los gastos	3125,78 BTC	Recompensa	6.35408247 BTC
Transacciones	3192	Minado el	07 abr 2024, 17:17:27
Testigo de Tx	3071	Altura	838.156
Ingresos	7689	Confirmaciones	1
Gastos	8745	Rango de comisiones	0-269 sat/vByte
Comisiones	0.10408247 BTC	Comisión media	0.00003261
Comisiones kB	0,0000576 BTC	Comisión mediana	0.000001484
Comisiones kWU	0,0000261 BTC	Minador	AntPool

En la anterior imagen podemos ver que tiene el hash (con 19 ceros):

```
0000000000000000000029fae6b92f4ed4741340231066b0972863d0c565ee169
```

El primer bloque que se crea en una red se llama el bloque génesis, si quieres saber más sobre ello puedes acceder al siguiente enlace (<https://www.diariobitcoin.com/glossary/bloque-genesis/>). En este enlace puedes encontrar alguno de los misterios que rodean al primer bloque de bitcoin.

## El modelo de consenso de Nakamoto

Lo que ocurre es que puede ocurrir que a la vez, en el mismo instante de tiempo, haya más de un minero que encuentre la secuencia correcta del hash y quiera añadirlo al registro general. Esto implicaría que hay dos versiones diferentes del registro con bloques que son correctos (verificados y validados), pero que son diferentes. ¿Qué hacer entonces?

No se pueden admitir los dos, porque una misma transacción podría quedar registrada dos veces (esto equivaldría en el ejemplo anterior a que se ha pagado dos veces por el chalet en la playa). En el paper original de Bitcoin se desempata de la siguiente forma. Se mantienen las dos versiones “provisionalmente” y se sigue trabajando en ambas, hasta que se rompa el empate porque una de las dos cadenas se hará más larga. En un momento, en una de las cadenas se incluirá un nuevo bloque y el algoritmo indica que nos quedamos con la cadena más larga, y pasará a ser la cadena oficial. La cadena más corta se quedará cortada en ese punto y los bloques que no se usen se quedarán huérfanos.



El modelo de consenso de Bitcoin, llamado **Consenso Nakamoto**, utiliza bloques ordenados secuencialmente ponderado en importancia (según la prueba de trabajo) para determinar la cadena más larga que define el estado actual.



El minero que consigue incluir un bloque que se añade a la cadena oficial recibe como recompensa una transacción a él como forma de pago. El minero que añade el bloque incluye, en el propio bloque que añade, esta transacción como forma de pago, ganando bitcoins como pago por el proceso de minado. Esta dinámica de pago es la principal responsable de que existan estas granjas dedicadas al minado de bloques.

En el momento de la escritura de este documento (7 de abril de 2024), la recompensa por minado de un bloque en Bitcoin es de 6.35408247 BTC, una cantidad nada desdeñable teniendo en cuenta que 1 BTC equivale a 69731.41 euros. A esta cantidad fija se le suman las comisiones por cada una de las transacciones. Un negocio interesante en definitiva (o no).

#### 5.4. Seguridad en Blockchain

Gracias al uso de SHA-256, si se cambia un solo bit del bloque de entrada, se modifica su resultado. Esto es de especial utilidad, ya que si alguien intenta cambiar algo en el bloque, su Hash cambiará y no será válido. Además, el diseño de este bloque incluye como parte de su contenido, además de las transacciones y el número de verificación (que permite generar los ceros necesarios en el hash de salida), también incluye el identificador del bloque anterior, de modo que cada bloque contiene un “puntero” al previo, al último bloque que fue aceptado; encadenado así cada bloque con el anterior, construyendo de este modo una Cadena de Bloques (Blockchain). La cadena de bloques es una estructura de datos que encadena cada bloque con su anterior por su Hash. Por el propio diseño de la red es inmutable. Si quieres modificar un bloque, estarás alterando su hash y, en cadena, la de todos los bloques que vayan a continuación. Si quisieras hacerlo, tendrías que volver a generar bloques válidos y competir con la cadena oficial (hasta ahora más larga), que seguirá creciendo. Y la condición de aceptación según el algoritmo es quedarse siempre con la cadena más larga. Esto solo lo podrá conseguir el atacante si tuviera más potencia de cálculo que el resto de los integrantes en la red; a esta condición se le conoce como ataque del 51%. En este punto el atacante tendría más poder computacional que el resto de los nodos de la red y podrían comenzar a imponer sus modificaciones.

A la escala de redes que se manejan hoy en día en Bitcoin (con cerca de medio millón de nodos) o Ethereum es absolutamente improbable que ocurra. Si la red es suficientemente grande tenemos garantizada la seguridad e inmutabilidad, sin necesidad de que organismos centrales velen por esta garantía.

#### 5.5. ¡Blockchain es una estructura de datos descentralizada!

El blockchain no es más que una estructura de datos y un modo de almacenamiento de esta estructura de datos descentralizado, de modo que se almacena en los nodos de todos los participantes de la red. Es un soporte de información que permite agregar datos. Esta cadena de bloques cumple una serie de propiedades garantizadas muy interesantes. Esta garantía viene dada

---

matemáticamente por el propio diseño de la estructura de datos, no es una “confianza” que el usuario deba tener en un tercero. Estas propiedades son:

- **Pública.** Cualquier persona del mundo puede fiscalizar la lista de transacciones que han ocurrido en el tiempo. Que sea pública no implica que no pueda ser confidencial. Por ejemplo, en Bitcoin aunque la información es pública ofrece protección criptográfica para ocultar la identidad de quién hace las transacciones (no es posible saber qué persona está enviando dinero a quién).
- **Inmutable.** Los datos no se pueden cambiar. No es posible que un dato que haya sido incluido en una cadena de bloques pueda ser modificada en el tiempo por ningún otro usuario. Cuando algo está en la blockchain, es definitivo. No se puede hacer Control+Z.
- **Validada.** La nueva información que se va agregando está validada, usuarios maliciosos no pueden alterar el uso añadiendo transacciones erróneas. Esta validación dependerá del uso concreto que se haga de la cadena de bloques. Por ejemplo, en Bitcoin si un usuario quiere gastar 2 bitcoins, la validación consiste en comprobar que ese usuario dispone de ese dinero antes de validar la operación.

Blockchain puede usarse con otras tecnologías, no tiene por qué ser algo totalmente independiente. Es habitual combinarlo con otras tecnologías frontend y backend. Por otro lado, cada usuario tiene asociada una identidad digital. Es mejor que no pierdas la clave privada, pues perderás todo lo que tengas en Blockchain. Como principal beneficio asociado al uso de esta tecnología, cabría destacar los derivados de la descentralización. No es necesario confiar en los nodos de la red, ni hay que preocuparse por un punto de fallo principal.

Aunque las ventajas son suficientes, también existen algunas dificultades asociadas al uso de Blockchain, y que deben estudiarse antes de decidir utilizar esta tecnología. Algunas de las más relevantes son:

- **Es costoso.** Si tratas de usar Blockchain donde no es necesario, estarás incurriendo en un coste importante.
- **No permite datos privados.** Sí permite privacidad, pero no datos privados (las cadenas de bloques son públicas). Esto puede solventarse añadiendo niveles adicionales de encriptación sobre los datos públicos.
- **No es centralizado.** Si se requiere centralización las cadenas de bloques no encajan en el modelo de desarrollo.
- **Tamaño de los datos.** Almacenar archivos de gran tamaño no es recomendable porque más computación significa más energía y más dinero. Es posible no obstante sacar los datos a almacenar en un sistema de almacenamiento externo con referencias únicas a los mismos que garanticen que no han sido modificados.

Para finalizar esta sección, a continuación analizaremos algunos de los usos y casos de éxito más relevantes de esta tecnología. Bitcoin es la criptomoneda por excelencia. Como hemos estudiado desde el inicio del capítulo, es el fundamento de Blockchain. Pero blockchain es una tecnología que se puede aplicar a muchos más entornos, como veremos a continuación.

- **Contratos inteligentes.** En lugar de almacenar transacciones monetarias, en Blockchain se almacenan scripts (piezas de código) que se van a ejecutar si se cumplen una serie de

condiciones. En el caso de que se cumplan las condiciones se ejecuta el contrato. Aquí el contrato está público, disponible dentro de los nodos de la Blockchain y se ejecutará automáticamente si las condiciones se cumplen.

- **NFTs** (Non Fungible Tokens). Este término se ha puesto totalmente de moda en los últimos meses. La cadena de bloques certifica la propiedad de ciertos activos digitales. Los artistas digitales ponen a disposición obras y los interesados ¿podrán adquirir su propiedad?. No es propósito de este módulo indagar en los NFTs pero te recomiendo indagar sobre la validez legal en la adquisición de obras.

## 6. Introducción a Ethereum (Para saber más)

Ethereum se denomina con frecuencia como La computadora global. Desde el punto de vista puramente informático puede describirse como una máquina de estado determinista prácticamente ilimitada [AW18]. Esta máquina consta de un estado accesible globalmente, y una máquina virtual que aplica cambios a ese estado.

En una descripción funcional más práctica se puede describir Ethereum como una infraestructura descentralizada de código abierto que ejecuta programas, que se denominan contratos inteligentes (Smart Contracts). Los contratos inteligentes son códigos que se escriben utilizando la Máquina Virtual de Ethereum (EVM), que se encarga tanto de automatizar como de ejecutar estos acuerdos en un libro de contabilidad inmutable.



*Ethereum es el Bitcoin del código. Es una cadena de bloques de desarrollador@s, construida por programador@s para programador@s. Ethereum utiliza una tecnología similar a la de Bitcoin, y cuenta con su propia moneda llamada Éter (Ether en inglés, con acrónimo ETH). No hay mucha diferencia entre Bitcoin y Ethereum salvo por los contratos inteligentes. Ethereum aplica blockchain para los contratos inteligentes y almacena la lógica (código) de un modo inmutable.*

Como hemos visto anteriormente, Bitcoin fue el primer blockchain, pero Bitcoin estaba pensado como dinero digital. Como la especificación y el diseño de Bitcoin estaba en abierto, en 2013 el programador Vitalik Buterin decidió empezar a desarrollar Ethereum sobre la blockchain de Bitcoin para tener una plataforma de desarrollo de aplicaciones descentralizadas y colaborativas<sup>6</sup>.

Construir directamente sobre el blockchain de Bitcoin implicaba aceptar muchas restricciones que intencionalmente se habían puesto en esa red: un conjunto muy limitado de transacciones, tipos de datos y tamaños de almacenamiento muy restrictivos. A la especificación inicial del proyecto se unieron otros entusiastas (como Gavin Wood), que definieron la cadena de bloques de propósito

---

<sup>6</sup> En la actualidad, Ethereum cuenta con su propia blockchain que elimina algunas limitaciones de la Blockchain original de Bitcoin

---

general que permitiera al programador abstraerse de todos los detalles subyacentes de redes P2P, algoritmos de consenso, etc.

En Julio de 2015 se lanzó la primera versión de Ethereum y fue minado el primer bloque. La computadora global comenzó a funcionar<sup>7</sup>.

En la siguiente tabla se puede ver una comparativa entre las principales características de Bitcoin y Ethereum.

	Bitcoin	Ethereum
Uso	Se utiliza para pagos	Se utiliza para código / lógica
Definición	Moneda digital	Plataforma de contratos inteligentes
Tiempo procesar bloques	10 minutos	17 segundos

A diferencia de Bitcoin que cuenta con un lenguaje de script extremadamente limitado (básicamente evaluación de condiciones booleanas sobre el gasto asociado a la moneda), en Ethereum el propósito principal es el de crear una cadena de bloques programable de propósito general que ejecuta una máquina virtual capaz de desplegar código de cualquier nivel de complejidad, definiendo un lenguaje Turing completo.

## 6.1. Ethereum: Un blockchain de propósito general

A diferencia de Bitcoin que solo rastrea el estado de la titularidad de la moneda, en Ethereum se rastrean también las transiciones de estado de un almacén de datos de propósito general. Este almacén puede contener cualquier valor arbitrario que pueda expresarse con una tupla clave-valor.

Ethereum tiene una memoria que almacena tanto código como datos, empleando blockchain para rastrear cómo cambia la memoria a lo largo del tiempo. Existen dos diferencias importantes con las computadoras tradicionales:

- (1) los cambios de estado en Ethereum siguen las reglas del consenso y
- (2) el estado se distribuye globalmente entre todas las máquinas que forman parte de la red.

Las transiciones de estado en Ethereum se procesan en la Máquina Virtual de Ethereum (EVM). Los programas de la EVM se denominan Contratos Inteligentes y se escriben en lenguajes de alto nivel (como Solidity), y se compilan posteriormente a código binario para su ejecución en la EVM.



El estado de Ethereum se almacena en cada nodo como una base de datos que contiene las transacciones y el estado del sistema. Toda esta información se serializa en una estructura de datos hash del tipo *Árbol de Merkle-Patricia*.

---

<sup>7</sup> En el artículo titulado. A Prehistory of the Ethereum Protocol, el propio Vitalik explica muchos detalles del inicio de la red <https://vitalik.ca/general/2017/09/14/prehistory.html>

Ethereum actualmente utiliza el mismo modelo de consenso que Bitcoin (consenso Nakamoto). Sin embargo, ya se han anunciado planes para migrar a un sistema de votación ponderado de pruebas colaterales (llamado Prueba de Participación - Proof of Stake).

Con la Prueba de Participación, los mineros comprometen una participación de moneda digital antes de poder validar las transacciones. De este modo, la capacidad de un nodo minero para validar bloques depende del número de monedas que haya puesto en juego y del tiempo que lleve validando transacciones. Cuantas más monedas posean, más poder tendrán para minar. El minero elegido para cada transacción se elige aleatoriamente mediante un algoritmo ponderado que tiene en cuenta la potencia relativa de los mineros. Mediante este enfoque de pruebas de participación se mitiga el impacto medioambiental que tiene la prueba de trabajo del algoritmo original. Algunos proyectos basados en Ethereum

A continuación se enumeran algunos proyectos que se basan en Ethereum. Se recomienda visitar la web oficial de cada proyecto para tener una visión más detallada de las características de cada plataforma.

- Gnosis. Según palabras de sus creadores, esta plataforma permite crear, comerciar y mantener de forma segura activos digitales en Ethereum. Básicamente hace predicciones de comercio, de modo que las predicciones correctas reciben los tokens que estaban en juego. Web: <https://gnosis.pm/>.
- Golem. La plataforma Golem funciona como un supercomputador descentralizado. Hace cálculos fuera de Blockchain, verificando los resultados online. Esto permite a los usuarios alquilar (si te sobra en tu ordenador) o contratar potencia de cálculo. Web: <https://golem.network/>.
- Fetch.ai. Plataforma de aprendizaje automático descentralizada creada en 2021 con el objetivo de convertirse en el ecosistema de soluciones IA sobre blockchain de referencia a nivel mundial. Los agentes de Fetch.AI son capaces de tomar decisiones en nombre de las partes interesadas (como individuos, empresas privadas o gobiernos), integrándose fácilmente en sistemas existentes. Se basa en una nueva criptomoneda: el token FET, que permite el pago de comisiones y proteger la red contra el mal uso de los recursos que están disponible en la misma.

## 7. Conexión entre tecnologías

En el inicio del capítulo estudiamos que las tecnologías exponenciales se amplifican de un modo mucho mayor cuando convergen. En esta convergencia es necesario la conexión de datos de tipos diversos: texto, imágenes y sonido. La IA se ha convertido posiblemente en la herramienta de colaboración más importante jamás creada. Además, proporciona las interfaces de usuario naturales más potentes que pueden existir para acceder a los servicios que proporcionan todas estas tecnologías exponenciales.

En los últimos años han ocurrido algunos hitos que ya aportaban alguna pista sobre los avances que están sucediendo en la actualidad.

---

En 2011, Watson de IBM ganó una partida de Jeopardy a los dos mejores campeones de todos los tiempos. Esto fue una demostración del poder del procesamiento del lenguaje natural, gestión del contexto y deep learning.

Desde entonces este tipo de sistemas han evolucionado mucho. Los asistentes virtuales como Siri y Google permiten resolver cualquier tipo de consulta e interacción en lenguaje natural. Actualmente, y como veremos en esta sección, plataformas como OpenAI con GPT-3 permite generar lenguaje natural y escribir textos con total coherencia semántica y de contexto.

Queda patente cómo los sistemas de deep learning permiten el aprendizaje no supervisado, con grandes progresos en este ámbito. En concreto, en reconocimiento e interpretación de imágenes los sistemas existentes ofrecen mejores resultados que las capacidades de los humanos. En 2016 por ejemplo el MIT Technology Review publicó la noticia de que una IA derrota a los mejores médicos en el diagnóstico de la retinopatía diabética basada en imagen".

El reconocimiento de imágenes se ha disparado en los últimos años. Facebook tienen miles de millones de imágenes en su plataforma. Estos datos se utilizan para el etiquetado automático, con resultados que hemos utilizado de un modo directo en sesiones anteriores del curso.

En la integración de los otros sentidos, la IA seguirá trabajando para lograr interacciones más naturales. El tacto, oído y olfato irán cobrando protagonismo en los próximos años. Por ejemplo, la integración con sistemas de Realidad Virtual está siendo ampliamente explorada en el nuevo ecosistema de Meta.

En última instancia, durante la revolución de la IA que está ocurriendo, la integración será completa en todo lo que nos rodea, combinando sensores y redes y haciendo que todos los sistemas sean inteligentes".

Para conseguir esta interacción completa será necesario lograr una conexión con todos los sectores económicos y sistemas informacionales (agentes conversacionales) y en todos los canales posibles (basados en texto, imágenes y sonidos).

## 8. Sistemas IoT

El término IoT proviene del inglés Internet of Things. Podría definirse como la interconexión de dispositivos (cosas) a través de una red, normalmente Internet<sup>8</sup>. En esta red los dispositivos pueden ser visibles e interactuar entre ellos. En la figura siguiente se muestra la evolución del número de cosas conectadas a internet en los últimos años.

---

<sup>8</sup> Aunque también se considera IoT la conexión de dispositivos en una red privada

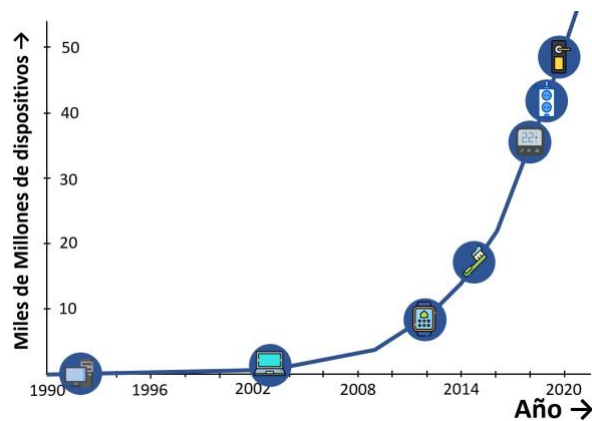


Figura 4.25: Evolución en el número de dispositivos IoT y algunos hitos tecnológicos asociados con su fecha de aparición en el mercado.  
Fuente: Elaboración propia a partir de datos de [sociedaddelainformación.es](http://sociedaddelainformación.es)

Estas cosas conectadas pueden ser dispositivos de tipos muy diversos: vestibles (calzado y ropa), frigoríficos, asistentes digitales, cerraduras e incluso cepillos de dientes. La idea subyacente es que las cosas puedan interactuar sin necesidad de la intervención humana (interacción M2M - machine to machine). Estas interacciones generan gran cantidad de datos digitales que, posteriormente, pueden ser analizados, tratados y utilizados para la toma de decisiones automática. Cuando la IA se añade al IoT surge un nuevo término: AIoT, que genera datos sobre IoT y extrae conocimiento a través de IA. La IA por tanto añade en análisis de datos y la tomar decisiones sin la participación de los humanos.

Esta convergencia tecnológica tiene muchas áreas de aplicación. A continuación, se enumeran algunas de las principales:

- Aplicaciones industriales. AIoT puede realizar mantenimientos predictivos de maquinaria, evitando el tiempo de inactividad y mejorando así la vida útil de la misma.
- Comercio inteligente. Identificación de compradores en la entrada de un comercio identificando sexo, edad, flujos de tráfico en la tienda, etc. Analiza los datos para predecir el comportamiento de consumo, ofreciendo promociones personalizadas en monitores y paneles situados en lugares de la tienda.
- Aplicaciones domésticas. Reducción de costes energéticos haciendo que las viviendas sean más eficientes energéticamente. Por ejemplo, se pueden tener sistemas de climatización inteligentes, bombillas inteligentes, sistemas de diagnóstico predictivos, etc.
- Ciudades Inteligente. En las ciudades inteligentes hay muchos usos de la AIoT, como por ejemplo la supervisión del tráfico drones. Los atascos pueden reducirse si se puede monitorizar, realizando ajustes en límites de velocidad y tiempos de semáforos en tiempo real.
- Fabricación y logística. Los robots en las fábricas emplean diversos sensores integrados que permite hacer el análisis del proceso de fabricación identificando posibles mejoras de un modo automático. Por otra parte, la AIoT se emplea también con vehículos autónomos con

---

recopilación de datos sobre el entorno que facilita la toma de decisiones sobre la navegación en cada momento. En la actualidad muchos gigantes tecnológicos como Amazon, Google o FedEx ya cuentan con robots de entrega en el negocio minorista.

El artículo "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity" resume los principales métodos, técnicas y trabajos de investigación disponibles en la actualidad para atacar los sistemas IoT<sup>9</sup>.

## 9. Seguridad en la convergencia tecnológica

La Ley de Reglamento General de Protección de Datos (RGPD<sup>10</sup>) establece, en su artículo 5, la seguridad como principio básico en el tratamiento de datos personales. Según el RGPD, la seguridad es un requisito obligatorio (no es una opción, es una necesidad), y no aplicar las medidas de seguridad adecuadas es ilegal. Los aspectos de seguridad no pueden quedar relegados únicamente a un posible impacto económico relativo a su incorrecta aplicación.

El artículo 32 exige medidas de seguridad que deben aplicarse en función de la probabilidad del riesgo y su gravedad. Los datos personales deben protegerse de forma progresiva. Cuantos mayores sean los riesgos, más estrictas serán las medidas.

Los sistemas de IA pueden no ser totalmente coherentes y completos, lo que significa que no se puede predecir durante la fase de diseño todos los posibles factores contextuales que pueden alterar su funcionamiento. Esto expone a las personas a los riesgos de resultados inesperados en la ejecución de sistemas de IA.

Así, en sistemas basados en IA, es muy importante introducir mecanismos de seguridad técnica como anonimización de datos (de modo que los datos personales no puedan consultarse de un modo directo) y cifrado.

Como se ha comentado anteriormente, la seguridad no debe aplicarse únicamente para evitar pérdidas, sino para crear valor. Los sistemas de IA generarán confianza atrayendo inversores y usuarios si no existen incidentes de seguridad.

La Agencia de Ciberseguridad de la Unión Europea, ENISA, ha creado un informe titulado Retos de ciberseguridad de la AI: Panorama de las amenazas para la Inteligencia Artificial<sup>11</sup>. El contenido de esta sección está directamente extraído de los contenidos que se abordan en este informe.

El informe presenta las amenazas relativas a ciberseguridad en IA en tres líneas de trabajo principales:

---

<sup>9</sup> Un artículo relevante puede encontrarse en: <https://link.springer.com/article/10.1007/s43926-020-00001-4>

<sup>10</sup> <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

<sup>11</sup> El informe completo de ENISA está accesible en: <https://www.enisa.europa.eu/news/publications/artificial-intelligence-cybersecurity-challenges>



- Alcance de la IA en el contexto de la ciberseguridad prestando atención al ciclo de vida de las aplicaciones de IA.
- Identificación de los activos de las aplicaciones de IA para determinar lo que debe protegerse y lo que podría ir mal en términos de seguridad.
- Creación de una taxonomía detallada de posibles amenazas. Esta taxonomía sirve como base para la identificación de posibles vulnerabilidades y escenarios de ataque.

A su vez en el documento se analizan las interrelaciones entre el ámbito de la IA y la ciberseguridad. En concreto, se plantean tres dimensiones esenciales:

- Ciberseguridad para la IA. Esta dimensión analiza la posible falta de solidez y vulnerabilidades de los modelos y algoritmos de IA. En esta dimensión tendrían cabida la inferencia y manipulación de modelos por parte de terceros, ataques contra sistemas físicos impulsados por la IA, manipulación de los datos, etc.
- La IA para apoyar la ciberseguridad. Esta dimensión analiza el uso de IA como herramienta para crear añadir medidas de ciberseguridad desarrollando controles más eficaces. Algunos ejemplos de uso serían el uso de antivirus inteligentes, análisis forense inteligente, escaneo de correo electrónico, análisis automatizado de malware, etc.
- Uso malintencionado de IA. Uso de la IA para crear ataques más sofisticados. Ejemplos: malware basado en IA, ingeniería social avanzada, cuentas de redes sociales falsas con uso de IA, modelos generativos para crear datos falsos, descifrado de contraseñas apoyado por IA, etc.

#### **Para saber más...**

Queda fuera del alcance de este módulo analizar en detalle las consideraciones sobre seguridad en aplicaciones de IA. Se recomienda el estudio del informe de ENISA mencionando anteriormente. El informe profundiza en los aspectos esenciales en el desarrollo de sistemas seguros. En concreto, el capítulo 2 presenta un modelo de referencia general para el ciclo de vida de los sistemas de IA que identifica claramente los activos y procesos que intervienen. El capítulo 3 clasifica los activos del ecosistema de IA (teniendo en cuenta el ciclo de vida definido en el capítulo anterior) en 6 grupos: Datos, Modelo, Actores, Procesos, Entorno/Herramientas y Artefactos. El capítulo 4 presenta una taxonomía de amenazas y su asignación con los activos introducidos en el capítulo anterior. El capítulo final propone una serie de recomendaciones de alto nivel. Los anexos del documento incluyen unas tablas muy completas que incluyen la taxonomía de amenazas analizadas en detalle, así como la asignación de activos a las etapas del ciclo de vida del desarrollo de aplicaciones de IA.

---

## 10. Bibliografía

- 📄 Materiales formativos FP Online del Ministerio de Educación y Formación Profesional. Módulo de Programación de Inteligencia Artificial.
- 📄 Materiales formativos FP propiedad CIPFPD. Módulo de Programación de Inteligencia Artificial.
- 📄 OpenAI. <https://platform.openai.com/docs/introduction>
- 📄 Blockchain. <https://www.blockchain.com/explorer>

## 11. Referencias

[Kur04] Ray Kurzweil. The law of accelerating returns. In Alan Turing: Life and legacy of a great thinker, pages 381–416. Springer, 2004.

[FK11] Richard Foster and Sarah Kaplan. Creative Destruction: Why companies that are built to last underperform the market—And how to success fully transform them. Currency, 2011.

[Wal16] M Mitchell Waldrop. The chips are down for moore’s law. Nature News, 530(7589):144, 2016.

[McB19] Stephen McBride. These 3 computing technologies will beat moore’s law. Forbes, 23(04), 2019.

[DK20] Peter H Diamandis and Steven Kotler. The future is faster than you think: How converging technologies are transforming business, industries, and our lives. Simon & Schuster, 2020.

[AW18] Andreas M Antonopoulos and Gavin Wood. Mastering ethereum: building smart contracts and dapps. O’reilly Media, 2018.