# Introducción a la BlockChain

**Antonio Sánchez**

# Antonio Sánchez

**CEO InforByt**

**Presidente BlockChain Andalucía**

**Embajador Cardano**

**Embajador Zilliqa**

**CISO BlockChain OpenLab**

**CTO KeopSafe**

# Introducción BlockChain

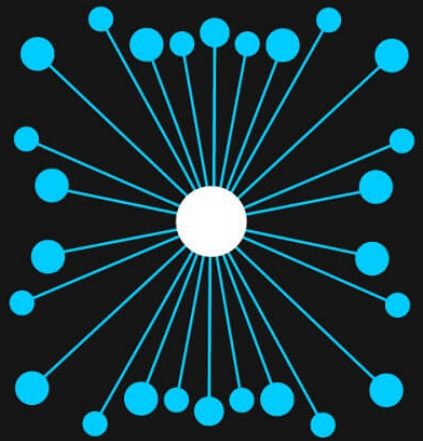
Una cadena de bloques es esencialmente un registro, un libro mayor de acontecimientos digitales que es compartido entre muchas partes diferentes de forma **Descentralizada** y que solo puede ser actualizado a partir del **Consenso** de la mayoría de participantes del sistema y, una vez introducida, la información nunca puede ser borrada.

# BlockChain

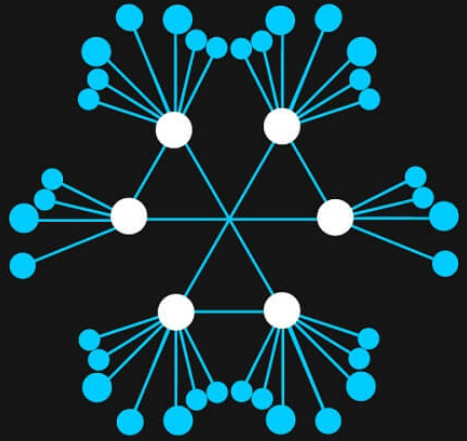
Imagina múltiples bloques que están conectados en forma de cadena. Aquí, todos los bloques estarán vinculados al bloque anterior y al bloque que está delante de él.

Además, todos los bloques en esa cadena contienen algún tipo de datos, y la cadena representa la estructura de enlace. En realidad, cada bloque se vinculará utilizando la criptografía. Además, todos los bloques en esa cadena tendrán una identificación hash criptográfica junto con datos transaccionales y marcas de tiempo.

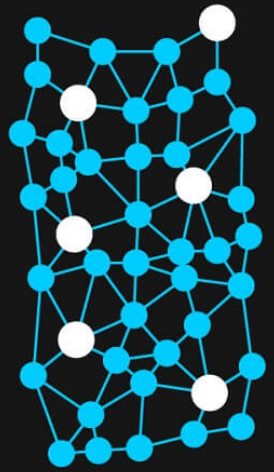
# Red centralizada vs descentralizada vs red distribuida: Visión general



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

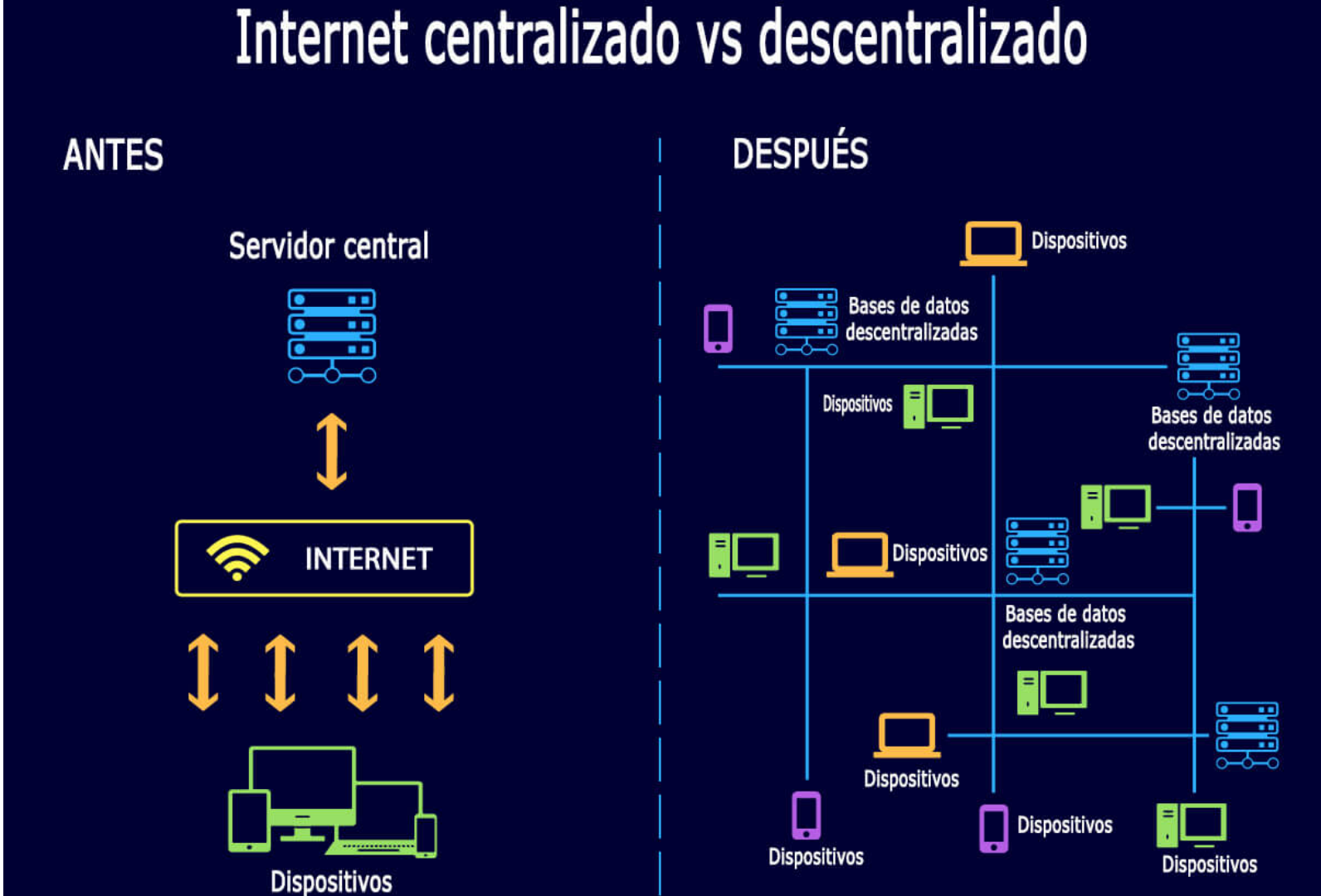


**Red descentralizada**
Sin servidor de autoridad único que controla los nodos, todos tienen entidades individuales



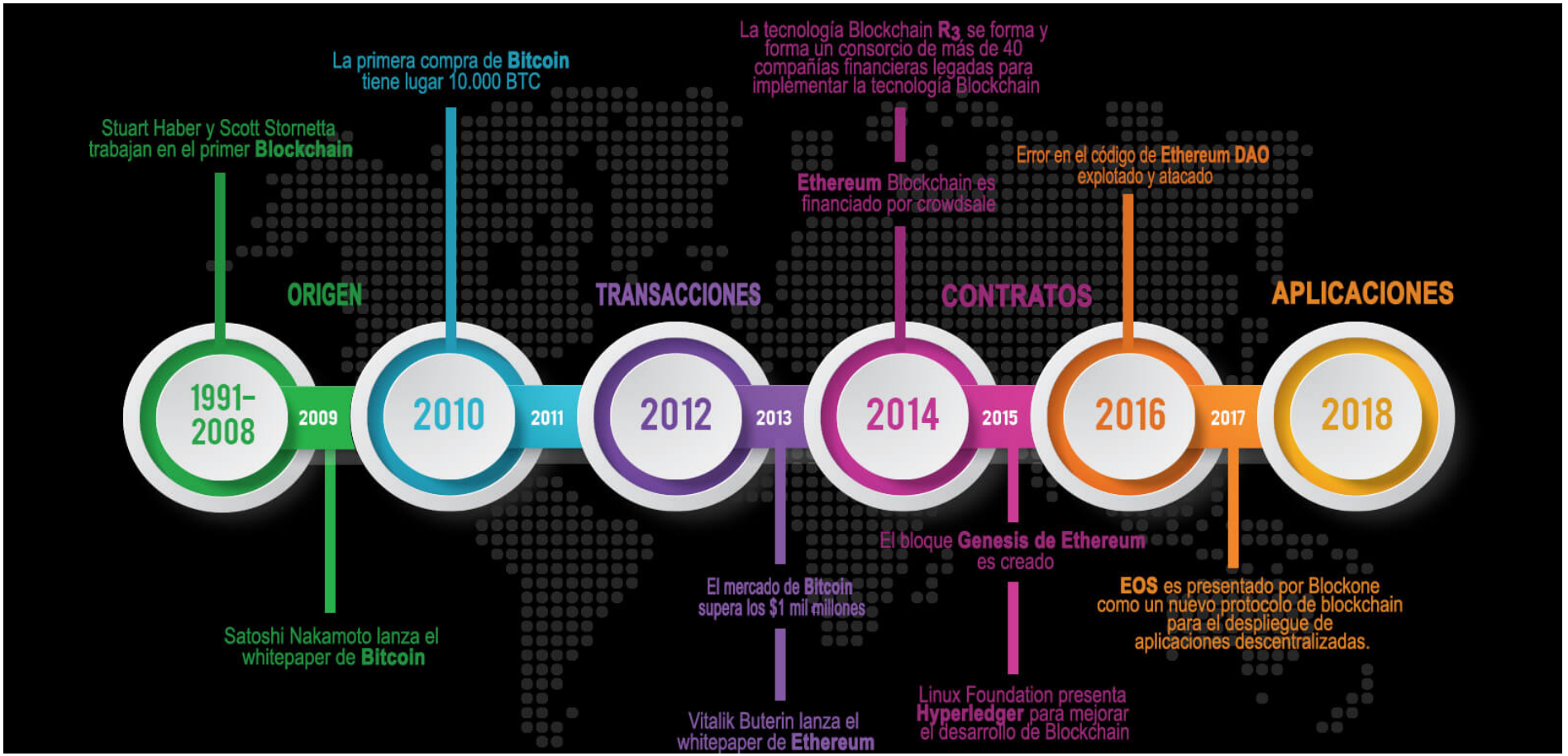
**Red distribuida**
Cada nodo es independiente e interconectados entre sí.

# Internet centralizado vs descentralizado



# BlockChain VS Base de Datos

| | | |
|---|---|---|
| Blockchain es descentralizada y no tiene un enfoque centralizado. Sin embargo, hay blockchains privadas que pueden utilizar algún tipo de centralización. | AUTORIDAD | Las bases de datos son controladas por el administrador y son de naturaleza centralizada. |
| Blockchain utiliza una arquitectura de red de registro distribuido. | ARQUITECTURA | La base de datos usa una arquitectura cliente-servidor. |
| Blockchain utiliza operaciones de lectura y escritura. | MANEJO DE DATOS | Las bases de datos admiten CRUD (Crear, Leer, Actualizar y Borrar) |
| Los datos son compatibles con la integridad. | INTEGRIDAD | Entidades maliciosas pueden alterar los datos. |
| La blockchain pública ofrece transparencia. | TRANSPARENCIA | Las bases de datos no son transparentes. El administrador decide qué público accede a los datos. |
| Las blockchains son comparativamente más difíciles de implementar y mantener. | COSTO | La base de datos es una tecnología antigua y es fácil de implementar y mantener. |
| Blockchain es abatido por los métodos de verificación y consenso. | RENDIMIENTO | Las bases de datos son extremadamente rápidas y ofrecen una gran escalabilidad. |


Stuart Haber y Scott Stornetta trabajan en el primer Blockchain
La primera compra de Bitcoin tiene lugar 10.000 BTC
La tecnología Blockchain R3 se forma y forma un consorcio de más de 40 compañías financieras legadas para implementar la tecnología Blockchain
Ethereum Blockchain es financiado por crowdsale
Error en el código de Ethereum DAO explotado y atacado
ORIGEN
TRANSACCIONES
CONTRATOS
APLICACIONES
1991–2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Satoshi Nakamoto lanza el whitepaper de Bitcoin
El mercado de Bitcoin supera los $1 mil millones
Vitalik Buterin lanza el whitepaper de Ethereum
El bloque Genesis de Ethereum es creado
Linux Foundation presenta Hyperledger para mejorar el desarrollo de Blockchain
EOS es presentado por Blockone como un nuevo protocolo de blockchain para el despliegue de aplicaciones descentralizadas.

# Historia

# CARACTERÍSTICAS DE BLOCKCHAIN

**INMUTABLE**

Nadie puede alterar/eliminar los datos en el registro o agregar contenido nuevo sin ninguna validación. Esta característica asegura la inmutabilidad.

**DESCENTRALIZADA**

No hay una sola persona o autoridad gobernante que revise el marco.

**SEGURIDAD MEJORADA**

Todos los datos del registro están fuertemente encriptados. Por lo tanto, promueve un mayor nivel de seguridad.

**REGISTRO DISTRIBUIDO**

Todos los nodos mantienen el registro y, por lo tanto, la potencia computacional se distribuye entre ellos. Por ende, promueve un buen resultado.

**CONSENSO**

El algoritmo de consenso ayuda a la red a tomar decisiones.

**LIQUIDACIÓN MÁS RÁPIDA**

Blockchain ofrece un resultado más rápido en las liquidaciones. Así, podrás transferir dinero más rápido.

# Características BlockChain

## Inmutable

La inmutabilidad es, sin duda, una de las características más importantes de BlockChain. Significa que ningún desarrollador o usuario de BlockChain puede alterar/eliminar los datos en el registro o agregar contenido nuevo sin ninguna validación. Esta característica asegura la inmutabilidad.

# Características BlockChain

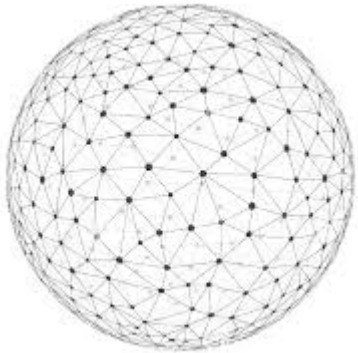
## Descentralizada

No hay una sola persona o autoridad gobernante que revise el marco. Pero en una estructura de red típica, todo depende en gran medida del modelo cliente-servidor.

# Características BlockChain

## Registro Distribuido

Otra característica interesante de BlockChain es la naturaleza distribuida del sistema. En realidad, todos los nodos mantienen el registro, por lo que la potencia computacional general se distribuye entre ellos.

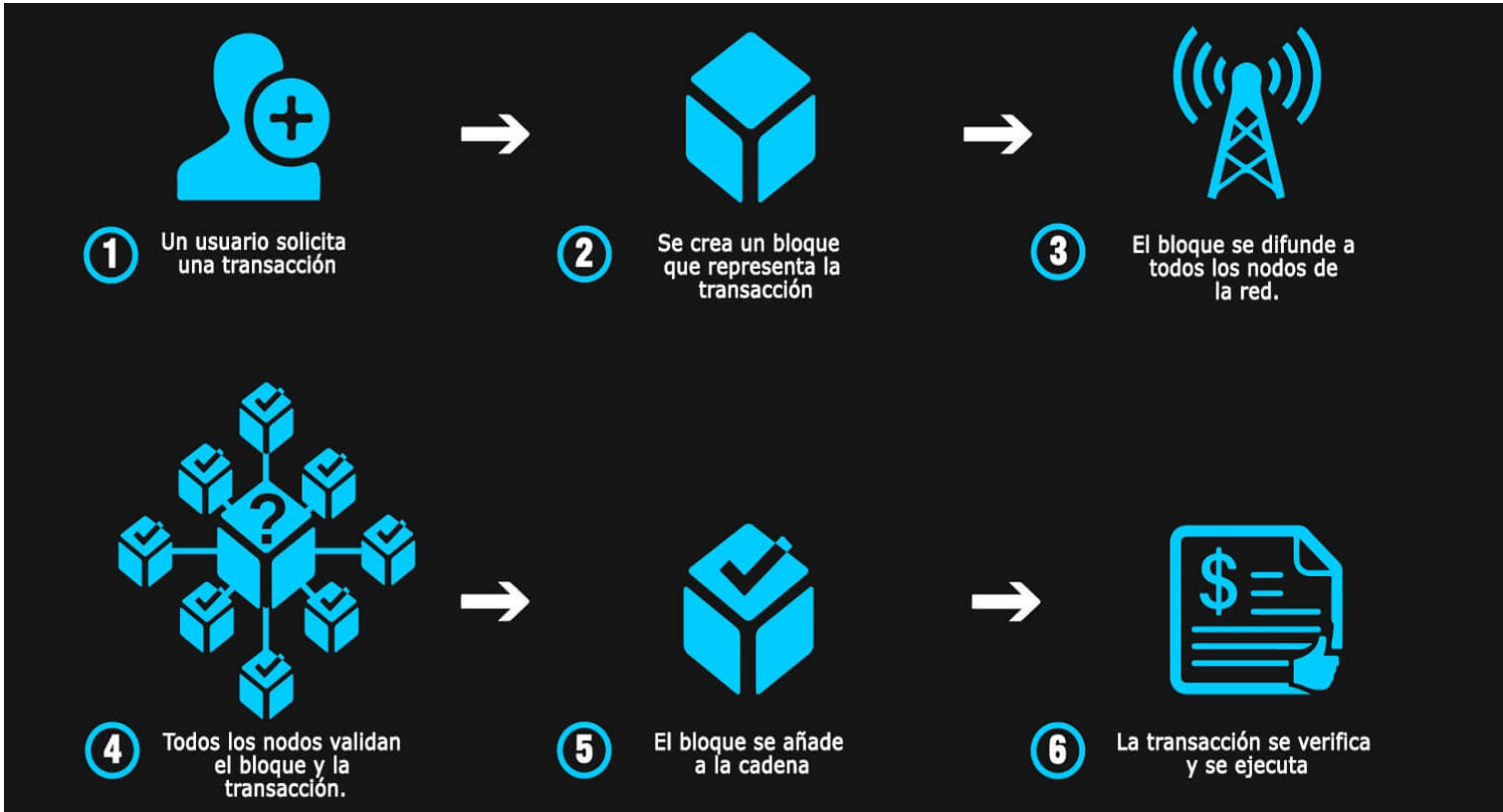


# Características BlockChain

## Consenso

El consenso es un factor crucial cuando se trata de BlockChain. Sin consenso, el sistema BlockChain no funcionará. En realidad, los algoritmos de consenso ayudan a la red a tomar decisiones. Sin ningún consenso, ninguna blockchain puede hacer un juicio justo de los bloques que se agregan.

# Como funciona BlockChain



# Tipos de BlockChain

Podemos clasificar la BlockChain en dos escenarios diferentes. En la clasificación general, obtenemos cuatro tipos de blockchain:

- Privada
- Pública
- Federada
- Híbrida

Y en base a la clasificación del nivel de permiso, obtenemos dos tipos:

- Con permiso
- Sin permiso

## CLASIFICACIÓN GENERAL

### ¿POR QUÉ UTILIZAR ESTO?

**Blockchain Privada**

- Preserva la privacidad
- Potencia eficiente en comparación con la blockchain pública.
- Red menos volátil
- Empoderamiento organizacional

**Blockchain Público**

- Mayor transparencia
- Verdadera estructura descentralizada.
- Empoderamiento del usuario
- Inmutabilidad

**Blockchain federada**

- Ahorra un montón de costos
- Ofrece tarifas de transacción más bajas
- Regulaciones de red
- Sin acceso criminal

## CLASIFICACIÓN GENERAL

**Blockchain con necesidad de Permisos**

- Adecuado para las organizaciones
- Las tasas de transacción son bajas
- No se requiere tener un activo nativo

**Blockchain sin necesidad de Permisos**

- Más potencia para los nodos.
- Nivel de privacidad abierto para todos.
- Libre participación en votaciones o consensos.

# DIFERENTES TIPOS DE TECNOLOGÍA BLOCKCHAIN PARA EMPRESAS

| CLASIFICACIÓN GENERAL | CARACTERÍSTICAS ESPECIALES | ¿POR QUÉ UTILIZAR ESTO? |
|---|---|---|
| **Privada**<br>En las blockchains privadas, una sola organización tendrá autoridad sobre quién puede unirse y acceder a la red. Piense en ello como una red descentralizada centralizada. | • Acceso de lectura o escritura varía de un nodo a otro<br>• Salida más rápida<br>• Puede utilizar cualquier tipo de activo en la red<br>• No ofrece anonimato.<br>• Más barato en comparación con la blockchain pública | • Preserva la privacidad<br>• Potencia eficiente en comparación con la blockchain pública<br>• Red menos volátil<br>• Empoderamiento organizacional |
| **Pública**<br>En una blockchain pública, cualquier persona puede unirse y participar en la red. Todos tienen permitido ver el registro y participar en el consenso. | • Todos tienen acceso a la red<br>• Puede descargar y agregar nodos<br>• Totalmente descentralizada en la naturaleza<br>• Salida más lenta<br>• Ofrece anonimato | • Mayor transparencia<br>• Estructura descentralizada verdadera<br>• Empoderamiento del usuario<br>• Inmutabilidad |
| **Federada**<br>En la blockchain federada, múltiples organizaciones influyen en la red de blockchain. Es similar a un centro para que un gran número de organizaciones compartan y trabajen simultáneamente. | • Salida extremadamente más rápida<br>• Altamente escalable<br>• Energía eficiente<br>• Autoridad distribuida | • Reducción de costos<br>• Ofrece tarifas de transacción más bajas<br>• Regulaciones de red<br>• Sin acceso criminal |
| **CLASIFICACIÓN POR NIVEL DE PERMISO** | | |
| **Con necesidad de permiso**<br>En este tipo de red de blockchain, todos los nodos de la red no pueden participar en el proceso de consenso. Sólo pueden participar nodos predeterminados. | • En esta, la descentralización va a variar de una red a otra red<br>• Algunos nodos tienen mas autoridad<br>• Relativamente mas rapido<br>• Entorno de confianza | • Adecuado para las organizaciones<br>• Las tasas de transacción son bajas<br>• No se requiere tener un activo nativo |
| **Sin necesidad de permiso**<br>En este tipo de red de blockchain, cada nodo en la red puede participar libremente en el proceso de consenso. No hay restricciones a la participación. | • Generalmente descentralizado<br>• Ambiente libre de confianza<br>• Relativamente mas lenta | • Más poder para los nodos<br>• Nivel de privacidad abierto para todos<br>• Participación gratuita en la votación o el consenso |

# Red Blockchain pública vs privada

**Blockchain pública:** Sin permiso

Un sistema de red abierta donde todos los dispositivos pueden acceder libremente sin ningún tipo de permiso. El registro es compartido y transparente.

**Blockchain privada:** Con permiso

Un usuario debe estar autorizado por la autoridad de blockchain antes de poder acceder a la red. El usuario puede unirse solo si recibe una invitación.

# PLATAFORMAS DE BLOCKCHAIN EMPRESARIAL


## COMPARACIÓN DE PLATAFORMAS DE BLOCKCHAIN EMPRESARIAL

| | HYPERLEDGER FABRIC | QUORUM | ETHEREUM | RIPPLE | R3 CORDA |
|---|---|---|---|---|---|
| Tipo de registro | Con necesidad de permiso | Con necesidad de permiso | Sin necesidad de permiso | Con necesidad de permiso | Con necesidad de permiso |
| Gobernancia | Fundación Linux | Desarrolladores de JP Morgan y Ethereum | Desarrolladores de Ethereum | Laboratorios de Ripple | Consorcio R3 |
| Enfoque en la industria | Cross-Industry | Multi-industria | Cross-Industry | Industria financiera | Industria financiera |
| Rendimiento | > 2000 tps | ≥ 100 tps | ~ 20 tps | ~ 1500 tps | ~170 tps |
| Criptomoneda | Ninguna | Ninguna | Ether (ETH) | Ripple (XRP) | Ninguna |
| Mecanismo de consenso | Mecanismo conectable | Protocolo de votación | Proof of Work (PoW) | Protocolo de Votación Probabilística | Mecanismo conectable |
| Contrato inteligente | Si | Si | Si | No | Si |
| Lenguaje de contrato inteligente | NodeJS or Golang or Java | Solidity | Solidity | - | Java or Kotlin |
| Tipo de aplicación | Amplio alcance | De gran alcance | Amplio alcance | Adecuado para aplicaciones financieras | Aplicaciones financieras |

# ¿CUÁLES SON LOS CASOS DE USO DE BLOCKCHAIN EMPRESARIAL?

## TRANSACCIONES GLOBALES
- Procesamiento de pago más rápido
- Costes reducidos
- Mayor eficiencia en las transacciones

## ATENCIÓN MÉDICA
- Se deshace de las falsificaciones de drogas
- Seguimiento de la información del paciente
- Agiliza múltiples resultados de pruebas al mismo tiempo

## COMERCIO
- Mayor transparencia y confianza para la financiación comercial
- Más control para las manufacturas
- Reducción de papeleo y costo

## PETRÓLEO Y GAS
- Pago seguro de fletes y auditoria
- Mejora la eficiencia al calcular rutas de envío
- Ahorra 5% de ingresos con exactitud

## SEGURIDAD ALIMENTICIA
- Responsabilidad por la seguridad alimentaria
- Reducir el desperdicio de alimentos
- Deshacerse del fraude alimentario

## BIENES RAÍCES
- Reduce el costeo de la propiedad
- Promueve la propiedad fraccional
- Aumenta la escalabilidad

## CADENA DE SUMINISTRO
- Sistema de registro asegurado con visibilidad de toda la cadena
- Seguimiento de todos los productos
- Detectará rápidamente al personal corrupto

## HUMANITARISMO
- Asegura que la donación vaya al lugar correcto
- Ofrece transparencia a los ciudadanos donantes
- Promover la equidad y la confianza

## VENTAS AL POR MENOR
- Ayuda a combatir productos falsificados
- Realiza un seguimiento de todos los bienes de lujo
- Se ocupa de cuestiones de robo

## MEDIOS Y ENTRETENIMIENTO
- Mejor valor artístico
- Conecta a artista con un mejor sueldo
- Marketing eficiente en las redes sociales

## SERVICIOS GUBERNAMENTALES
- Manera segura de preservar los derechos de los ciudadanos
- Ofrece crecimiento exponencial de la economía
- Digitalización de la identificación ciudadana

## VIAJES
- Agilizar el procesamiento de pasajeros
- Promueve la identificación transfronteriza
- Agenda de todos los vuelos con mayor precisión

## PROPIEDAD INTELECTUAL
- Asegura marcas y patentes de propiedades intelectuales
- Ofrece pago por trabajo patentado
- Reducción del abuso de propiedad intelectual

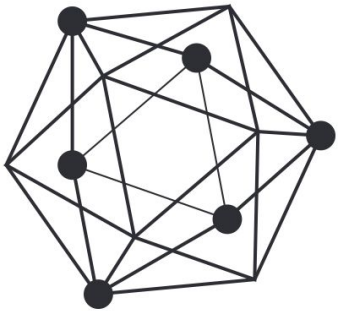
## SEGUROS
- Reduce el papeleo
- Reclamaciones de seguro más rápidas
- No más explotadores de los consumidores

# ¿HAY ALGUNOS RETOS DE IMPLEMENTACIÓN?

# Tipos de BlockChain

## Hyperledger

- Red autorizada que puedes usar para agregar privacidad en tu red.
- La alta escalabilidad garantiza que disfrute del mejor rendimiento de todos los tiempos.
- Protocolos de seguridad que salvaguardarán tu información.
- Disponibilidad de datos basada en la necesidad de conocer el concepto.



# Tipos de BlockChain

## Ethereum Enterprise

Ethereum Enterprise ofrece un canal privado en la arquitectura.

- Apoyo gubernamental a medida que implementas nuevos proyectos basados en Ethereum.
- Una plataforma abierta que puedes usar sin ningún problema.
- Actualizaciones rápidas para introducir nuevas adiciones y corregir errores mejor que otros.
- Ofrecer estándares para ayudar a otras compañías a construir su propia red.

# Tipos de BlockChain

## R3 Corda

Corda viene con dos versiones diferentes: Enterprise Corda y Corda.

En realidad, la empresa Corda es más adecuada para cualquier tipo de casos de uso empresarial, mas orientado a Banca.

- El firewall de la aplicación Blockchain que protege toda la red de cualquier tipo de ciber ataque.
- Alta disponibilidad que garantiza que tu red se mantenga en funcionamiento 24/7.
- Sistema de gobierno, que permitirá a las empresas tener reglas en el sistema.
- El sistema de monitoreo que permite a cualquier usuario localizar cualquier desastre y recuperarlo.

# Tipos de BlockChain

## Ripple

Ripple es otra tecnología blockchain en la banca que es más adecuada para los sectores financieros en la actualidad. Ripple es que ofrece una plataforma de transacciones casi gratuita y proporciona una producción relativamente más rápida.

- Nuevos mercados que ayudan a obtener ingresos rápidamente.
- Llega a más consumidores en poco tiempo promoviendo una excelente tasa de crecimiento.
- Escalabilidad que asegura que su sistema ofrezca el mismo rendimiento bajo presión.
- Plataformas con permisos que ofrecen más privacidad.
- Alto nivel de seguridad.

# Tipos de BlockChain

## Quorum

Quorum surgió en 2017 de manos de J.P.Morgan ofrece un algoritmo mejor y más rápido.

- Transacciones privadas que te permitirán realizar transacciones con otra parte en un canal seguro.
- Red con permisos, que asegura que tus transacciones personales estén lejos del registro.
- Gestión de nodos que te permitirá elegir qué nodos pueden ingresar a la red.
- Alta escalabilidad para una mejor experiencia.
- La solución más rápida que ahorra tiempo.

# HYPERLEDGER VS ETHEREUM

Al parecer, Hyperledger es bastante popular dentro del ecosistema de la blockchain empresarial. La comunidad cuenta con más de 260 socios de alto perfil que incluyen IBM, SAP y muchos más. Hyperledger es administrado por la Fundación Linux que creó el ecosistema en diciembre de 2015. La plataforma es de código abierto y admite una arquitectura modular. En Hyperledger, hay dos tipos de nodos; Los nodos de validación y los nodos de no validación. Los nodos de validación validan las transacciones, mantienen el registro y ejecutan el consenso que es el protocolo de consenso BFT.

Este ecosistema es bastante genérico y sirve para una amplia gama de propósitos. Se basa en el consenso de PoW para validar las transacciones. Además, está claro que Ethereum es ideal para aplicaciones B2C, ya que los usuarios no requieren permiso para participar en transacciones. Además, la plataforma tiene una criptomoneda nativa para facilitar las transacciones junto con los contratos inteligentes.

| | | |
|---|---|---|
| Es ideal para transacciones B2B ya que la participación es permitida. | USABILIDAD | Tiene un propósito genérico y es compatible con plataformas públicas y privadas, por lo que es ideal para transacciones B2C |
| No tiene un mecanismo de consenso. Los usuarios crean sus propios algoritmos de consenso debido a la naturaleza conectable de la arquitectura | CONSENSO | Utiliza Prueba de trabajo (PoW) como mecanismo de consenso |
| No tiene ninguna criptomoneda / token incorporado | TOKENS | Viene con Ether (ETH) |
| El registro no es público | NATURALEZA DE TRANSACCIONES | Todos los participantes pueden acceder al registro de transacciones. |
| Escrito en Go, Java, Node.js | LENGUAJE DE CONTRATO INTELIGENTE | Escrito en Solidity |
| Accenture, AirBus, American Express, Cisco, Daimler, J.P. Morgan, Intel, IBM, SAP etc. | PARTNERS | IC3, Microsoft, Accenture, J.P. Morgan, Consensys, Intel, Santander, CME Group etc. |

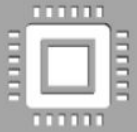

bitcoin

# Bitcoin

¿Qué es Bitcoin?

# Componentes básicos del protocolo Bitcoin

Un activo digital (bitcoin) de oferta limitada, conocida de antemano e inmutable.



Un conjunto de computadoras interconectadas (red Bitcoin), a las que puede unirse cualquiera.

Un cliente de software (Bitcoin), que cualquiera puede correr en su computadora y convertirse en participante de la red.

# Características Bitcoin

**P2P**: de par a par // Se trata de un sistema en el que una persona puede interactuar con otra sin intermediarios.

**Open source**: cualquiera puede examinar cómo funciona y contribuir a su desarrollo

**Descentralizado**: El protocolo no se ejecuta y controla por una empresa sino por una red de individuos y empresas de todo el mundo.

**Sin confianza**: La sustituye por pruebas criptográficas que son fáciles de verificar por la persona que las recibe, pero a la vez son imposibles de falsificar.

**Seudónimo**: Al igual que en el efectivo, no es sencillo relacionar la transacción con las personas que intervienen en la misma.

**Escaso**: No cabe la devaluación del valor de este dinero, porque se creará un número fijo de unidades. Hacia 2140 se habrán emitido 21 millones de bitcoins (2.100 billones de satoshis).

**Imposible de falsificar**: Todos los nodos de la red guardan los saldos de todos los participantes en el protocolo, y no existe una entidad central que lo controle. Evitan de forma centralizada que se pueda gastar dos veces el mismo dinero (doble gasto)

# ¿Qué es la minería de bitcoins?

Al proceso de realizar la Prueba de Trabajo para obtener el derecho de introducir un bloque en el libro registro se le llama **minería**.

Quien consigue introducir el bloque añade una transferencia llamada **coinbase**, es decir, crea una cantidad determinada de bitcoins nuevos (ahora son 12,5 BTC) que se abona como recompensa por la Prueba de Trabajo.

# Halving

- El objetivo de Satoshi Nakamoto fue crear una moneda que no se devaluara.
- El programa de emisión de Bitcoin tiene un crecimiento rápido al inicio y se ralentiza con el tiempo hasta llegar a un límite de emisión.
- Recompensa original: 50 BTC
- Cada 210.000 bloques (aproximadamente 4 años), se reduce la recompensa a la mitad.
  - 2008: 50 BTC
  - 2012: 25 BTC
  - 2016: 12,5 BTC
  - 2020: 6,25 BTC
  - ...
  - 2140: Fin recompensas

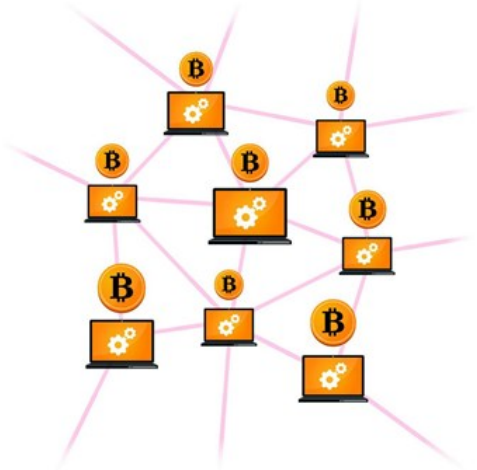
# Ajuste de la dificultad de minado

- Cada 2016 bloques (aproximadamente 2 semanas) se suma el tiempo de generación de los bloques y se divide por el número de bloques (2016).
- Si esta media es inferior a 10 minutos, se ha minado muy rápido, y ajustaremos el número objetivo a alcanzar para que cueste más lograr la recompensa (incremento de dificultad)
- Si esta media es superior a 10 minutos, se ha minado muy lento, y ajustaremos el número objetivo a alcanzar para que cueste menos lograr la recompensa (disminución de la dificultad).
- El nuevo número objetivo sirve para la Prueba de Trabajo de los siguientes 2016 bloques.

# Tipos de Nodos Bitcoin

Por lo general, un nodo consiste en un dispositivo de red físico, pero hay algunos casos específicos en los que se usan nodos virtuales.

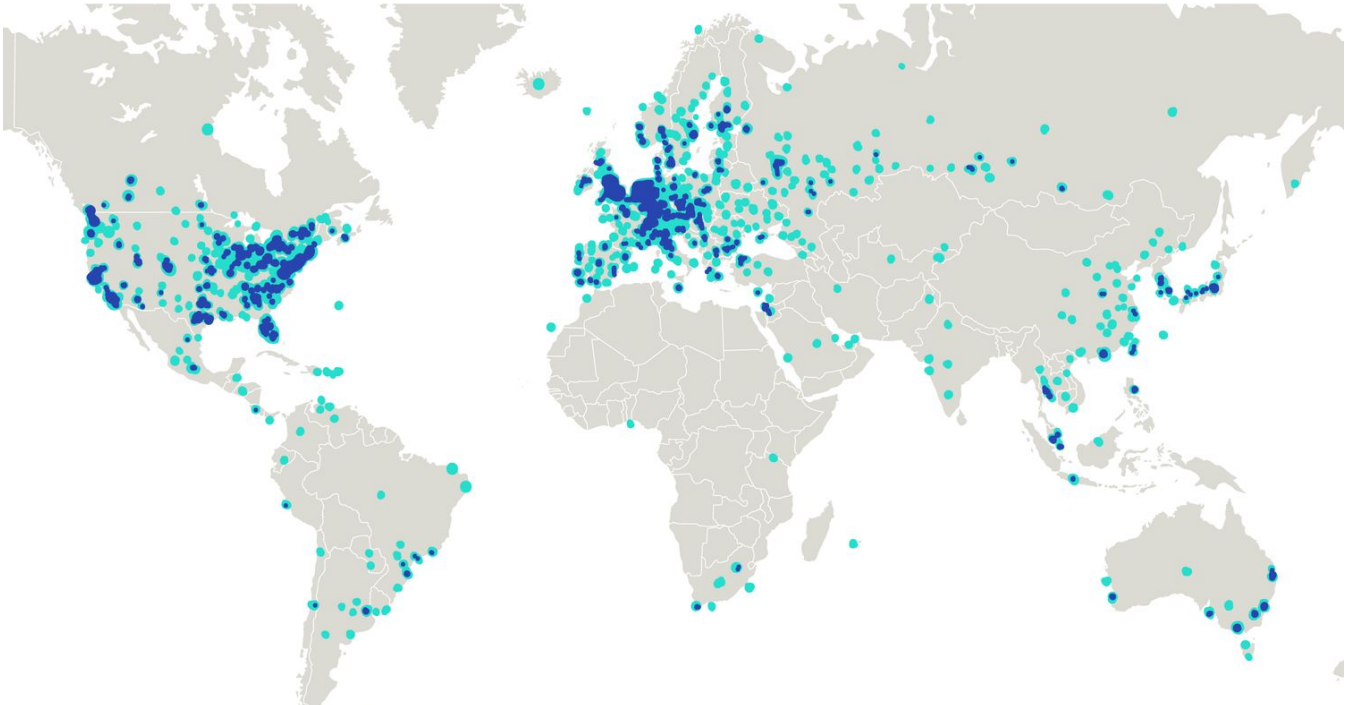
Cualquier computadora o dispositivo que se conecte a la interfaz de Bitcoin puede considerarse como un nodo en el sentido de que se comunican de alguna manera entre sí.



# ¿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 | 380 (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%) |

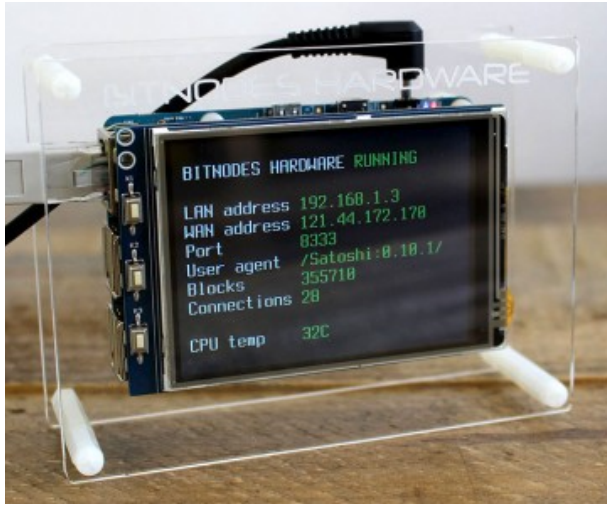


# Nodo Completo

Los nodos completos son los que realmente admiten y proporcionan seguridad a Bitcoin y son indispensables para la red. Estos nodos también se conocen como nodos de validación total a medida que se involucran en el proceso de verificar las transacciones y los bloques con respecto a las reglas de consenso del sistema. Los nodos completos también pueden transmitir nuevas transacciones y bloques a la blockchain.

# SuperNodo

Esencialmente, un nodo de escucha o supernodo es un nodo completo que es públicamente visible. Se comunica y proporciona información a cualquier otro nodo que decida establecer una conexión con él. Por lo tanto, un supernodo es básicamente un punto de redistribución que puede actuar como fuente de datos y como puente de comunicación, conectado 24/7/365.



# Nodo Minero

Para poder minar Bitcoins en el escenario competitivo actual, uno tiene que invertir en hardware y programas de minería especializados. Estos programas de minería (software) no están directamente relacionados con Bitcoin Core y se ejecutan en paralelo para probar y minar bloques de Bitcoin. Un minero puede elegir trabajar solo (minero solo) o en grupos (Pool de minería).