



BLOCKCHAIN

Claves para decidir si es un camino adecuado para la transformación.

Andrés Barrantes Bernal
CEO HighTech
[@abarrantesb](#)



Imagen Vívida



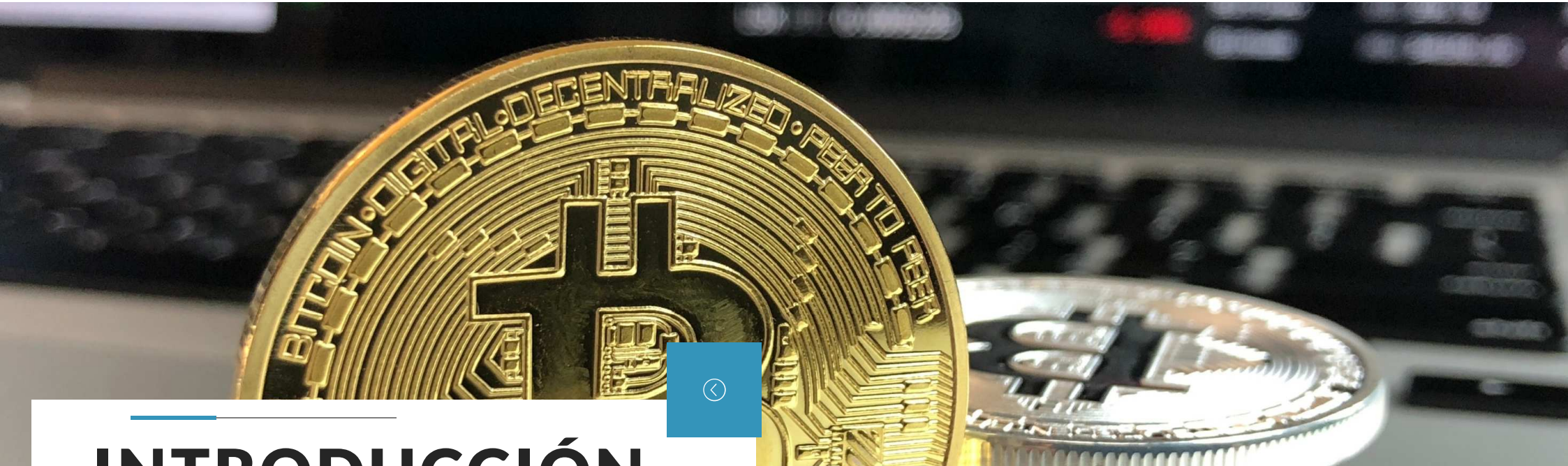
En 20 años, el papel y las filas habrán desaparecido.



Propósito central

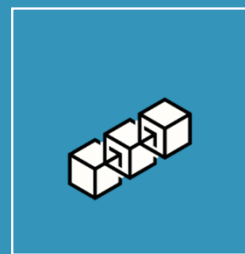
“Eliminar la brecha entre lo físico y lo virtual de todos los negocios que sean alcanzados por nosotros”



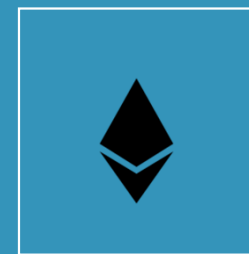


INTRODUCCIÓN

- Definición
- Conceptos Básicos
- Historia de Blockchain
- Mitos y Realidades



Definición



Historia



Mitos y Realidad

↓

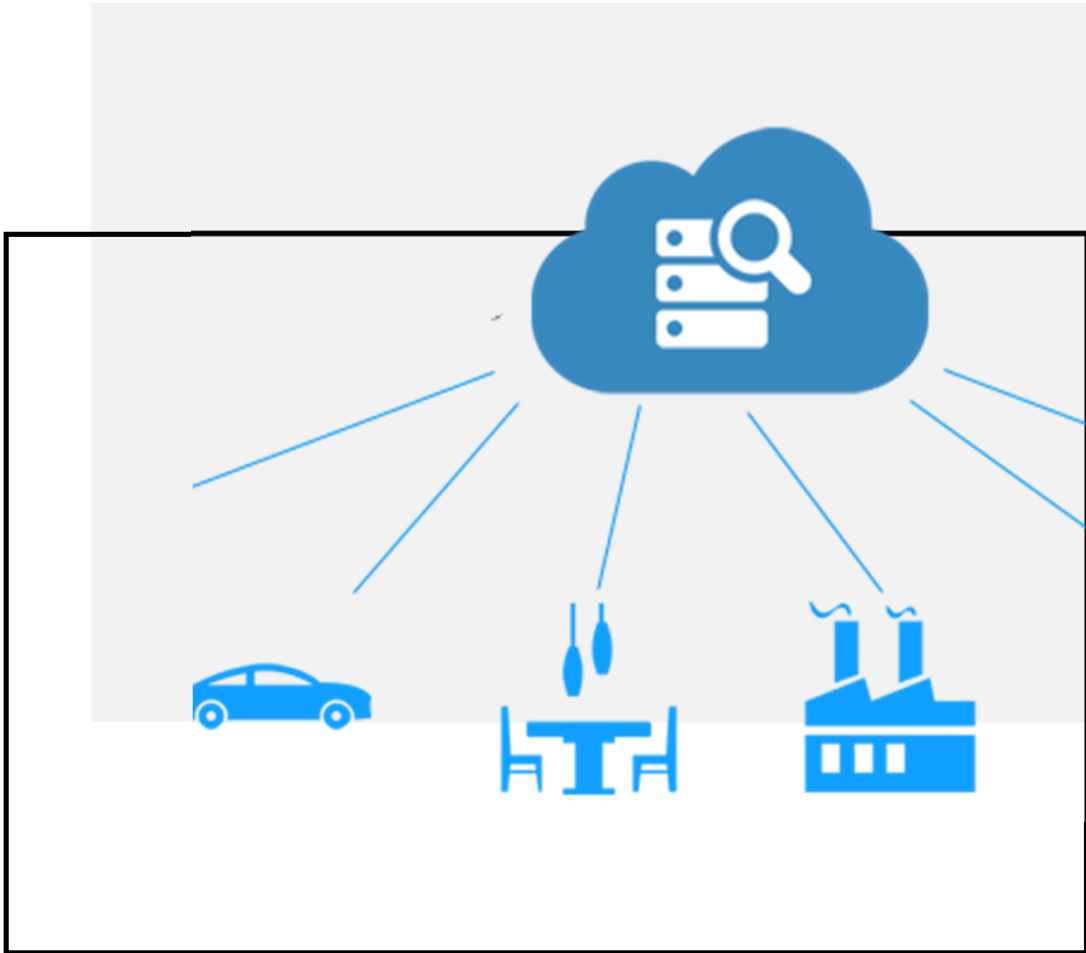
CONSTRUCCIÓN DE VALOR

Transferencia de Activos

Cualquier cosa que sea capaz de ser propiedad o controlado para producir valor es un activo

- Financiero. Ej, Bonos
- Intelectual. Ej, patentes
- Digital. Ej música

- El **Efectivo** también es un activo (Tiene propiedad de anonimato)



Tangibles e Intangibles.

Sistemas de Registro

Ledger o Libro

Es el sistema
de registro de
las compañías

Las compañías
tienen múltiples
libros o sistemas
de registro en la
medida que
participan en
diferentes
procesos de la
cadena de valor





Participantes, Tx. y Contratos

Participantes

Miembros de red de negocio ([Cliente](#), [Proveedor](#), [Gobierno](#), [Regulador](#))

Tiene identidades y roles específicos

Transacciones

Una transferencia de activos ([Juan le vende un carro a María](#))



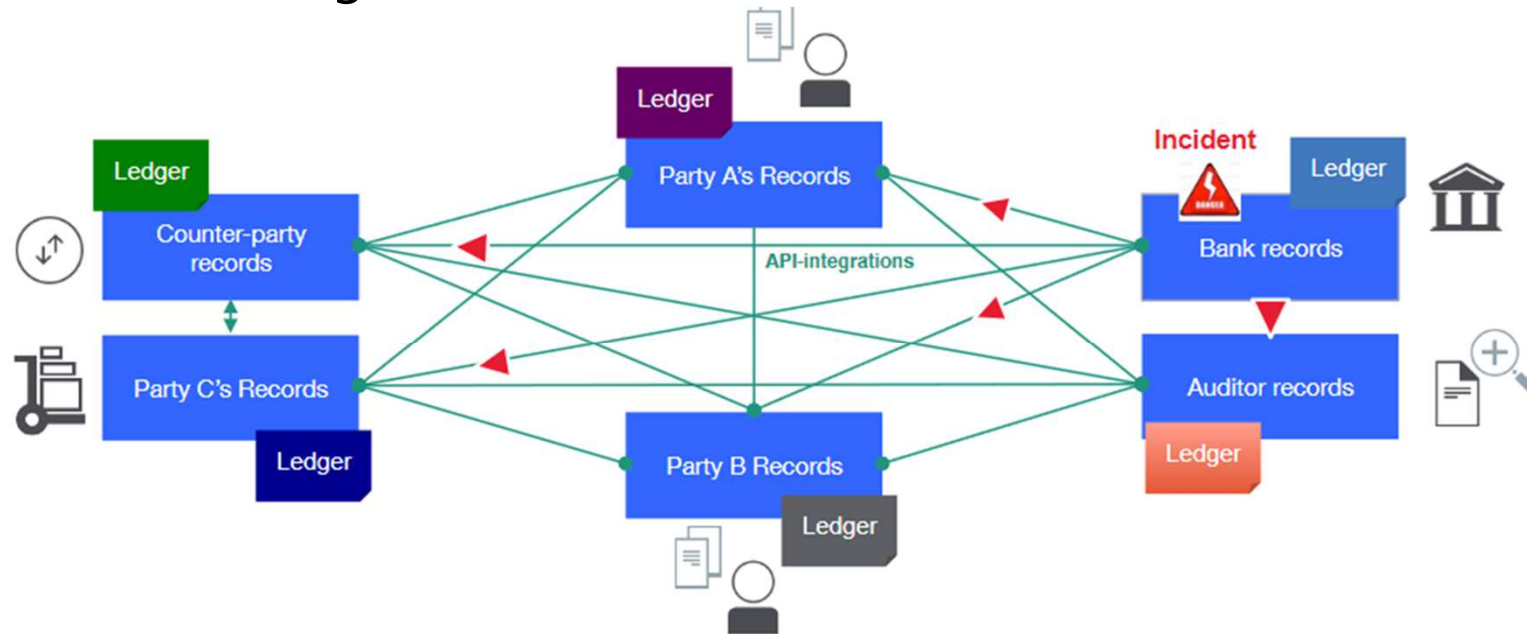
Contratos

Condiciones para que pase la transacción:

([Si María le paga a John, entonces pasa el auto. de Juan a María](#))

Problema

Difícil monitorear la propiedad de activos y transferencias en una red de negocios

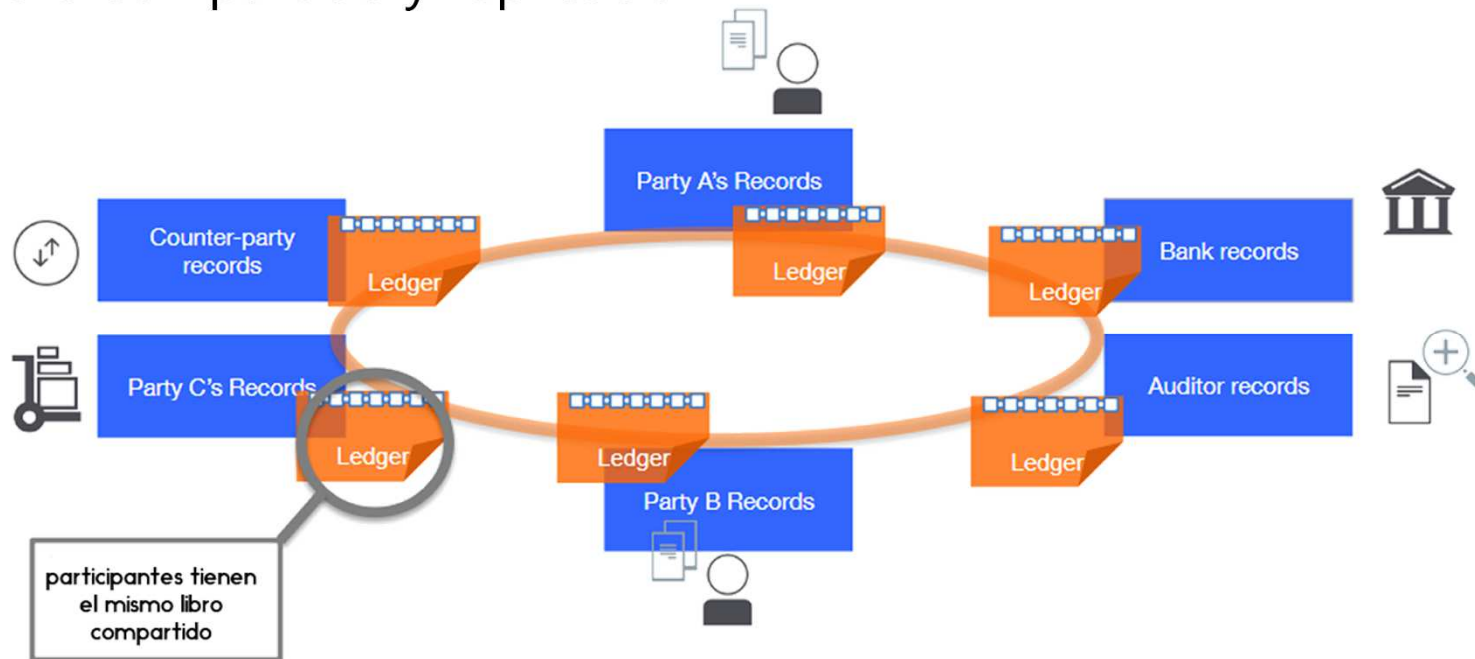


Ineficiente, Costoso, Vulnerable

Fuente: IBM

Solución

Libro compartido y replicado



Consenso, procedencia, inmutabilidad

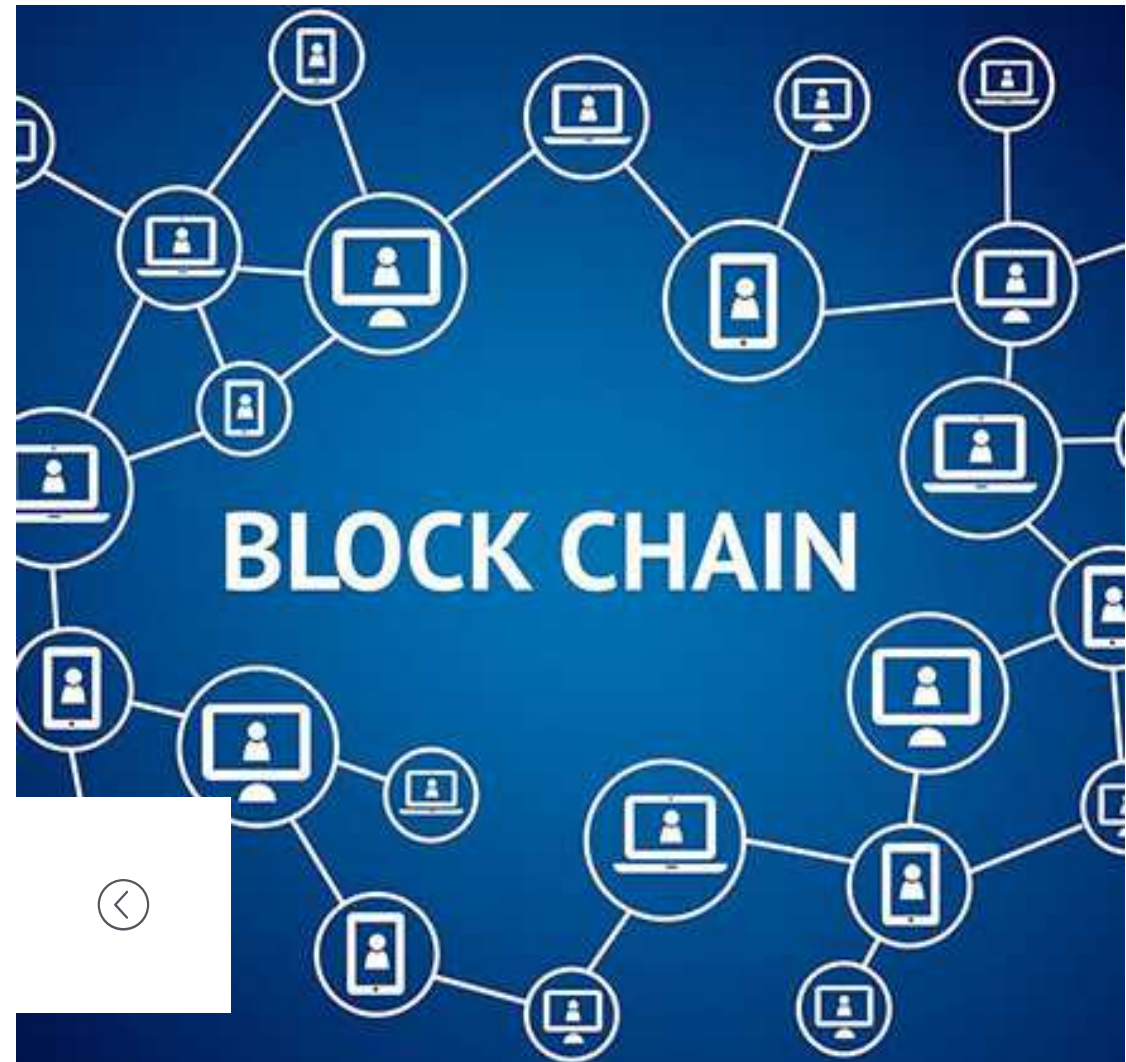
Fuente: IBM

BlockChai

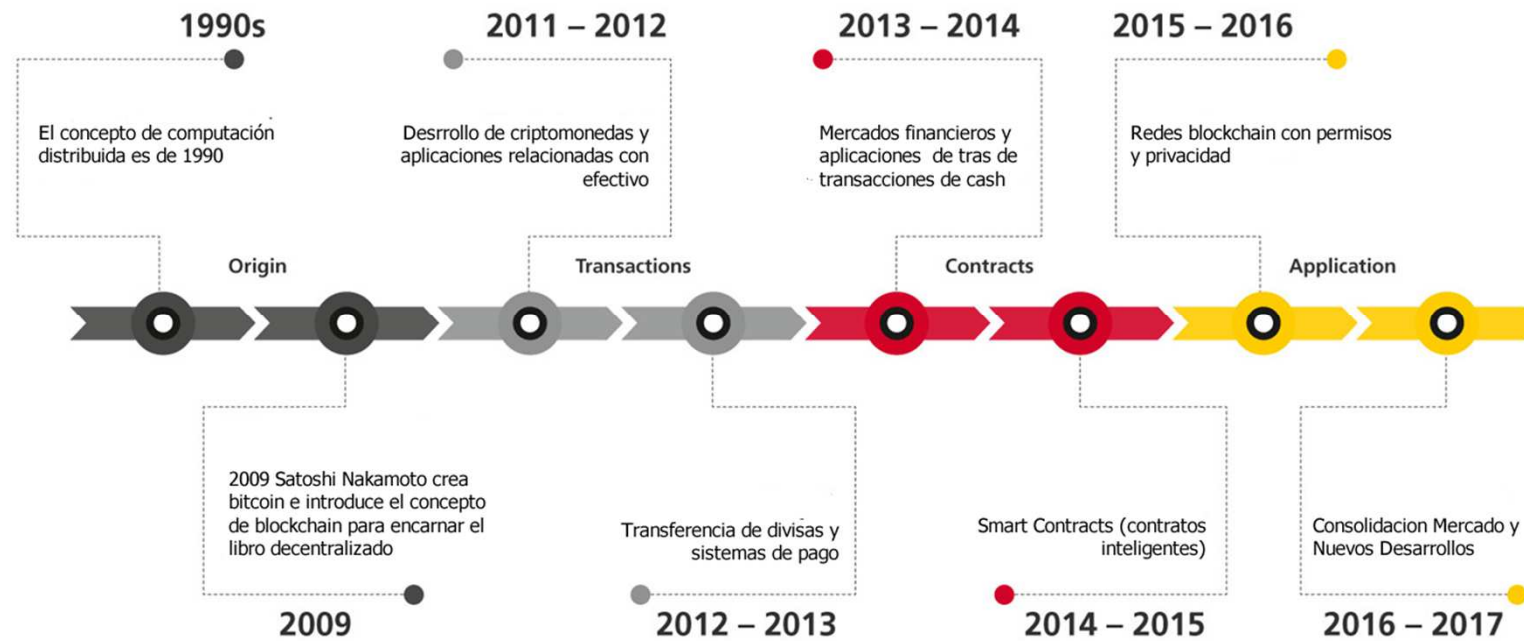
Cadenas de Bloques

Blockchain es un **libro distribuido P2P**

- Es criptográficamente **Seguro**,
- **inmutable** (extremadamente difícil de cambiar),
- actualizable únicamente por vía **consenso** o acuerdo entre las partes



Historia de Blockchain

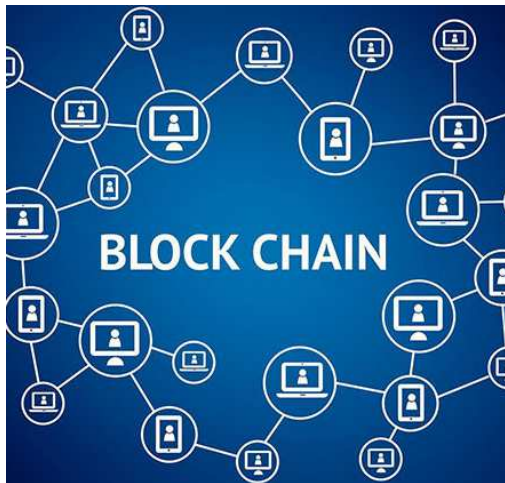


Cómo Funciona



BlockChain

Preguntas Clave



¿Cómo hacer para que se respeten el orden de los Bloques?

¿Como se protege la integridad de la cadena?

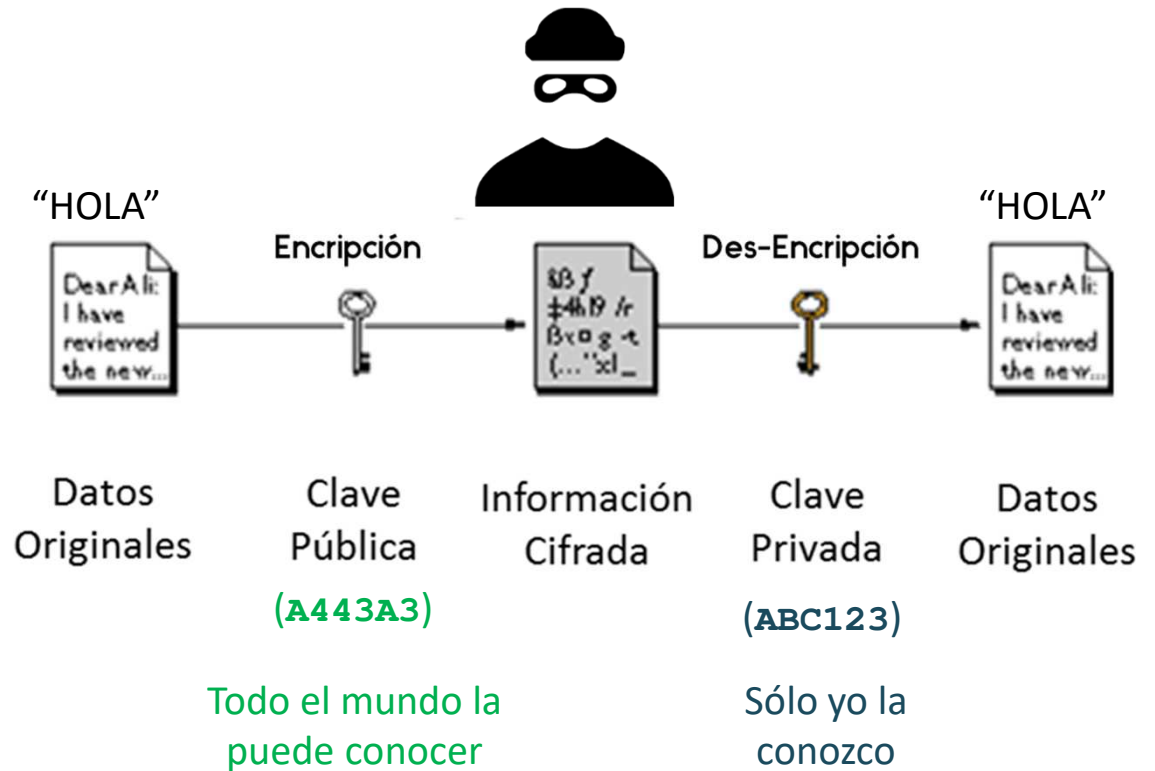
¿Cómo se evitan colisiones de escritura?

¿Qué incentivos tienen los mineros?

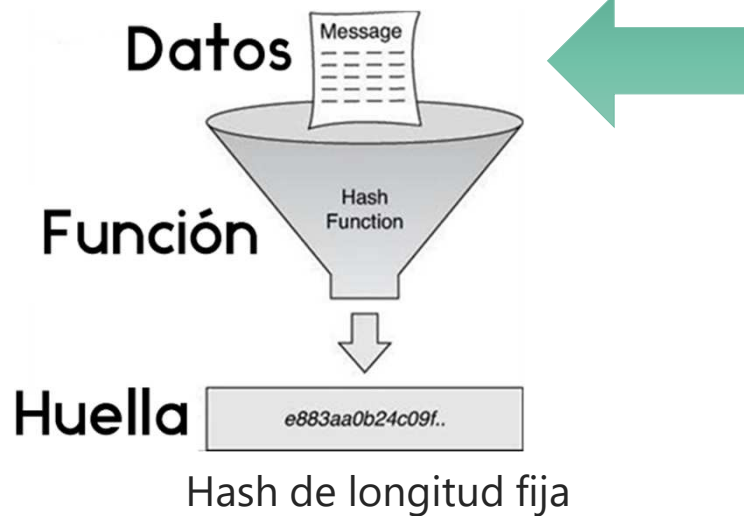
PKI

(Public Key Infrastructure)

Infraestructura de Clave Pública



HASH



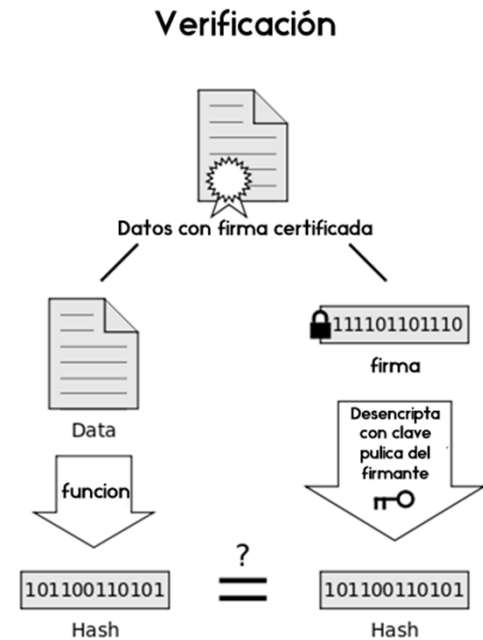
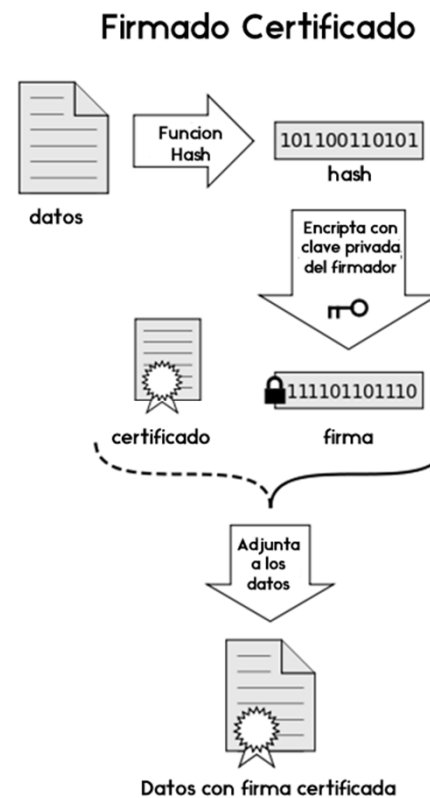
Texto	“Hola Mundo”
Hash	BE2E2578EB03870291F98B4ED05944FD6E5ECF4F

Texto	abc
Hash	A9993E364706816ABA3E25717850C26C9CD0D89D

Nota: SHA 256 es un ejemplo de algoritmo hash muy usado en Blockchain

Verificación de Firma Criptográfica

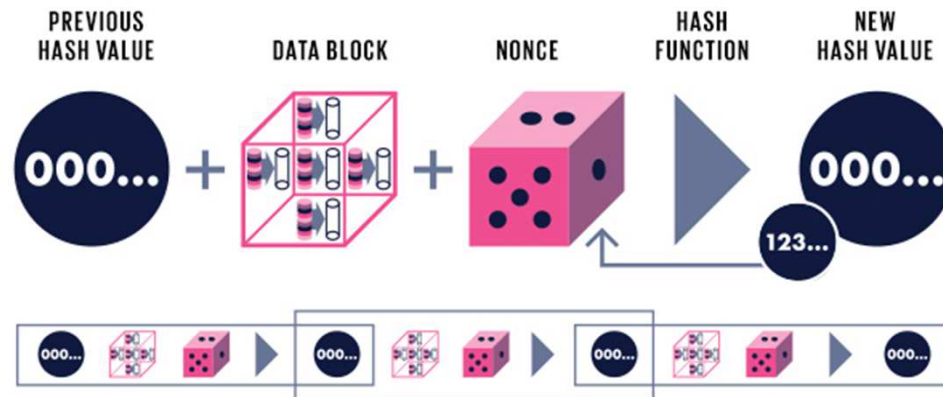
El proceso de firmado se hace con la clave privada del firmante y permite **verificar el hash** que se envía adjunto.



Si el hash es el mismo la información está verificada

Prueba de Trabajo (PoW)

La prueba de trabajo implica el escaneo de un valor **nonce** que, cuyo hash combinado con todas las transacciones en un bloque, el hash resultante comienza con un número de bits cero:

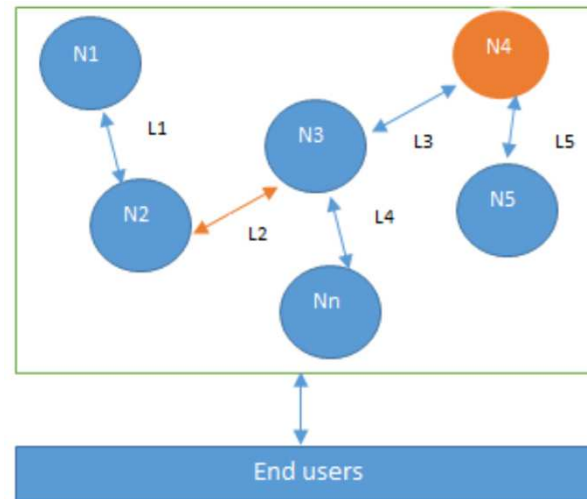


Sistemas Distribuidos

Más de un nodo con un propósito común

Todos los nodos son capaces de enviar y recibir mensajes entre sí. Los nodos pueden ser honestos, defectuosos o maliciosos.

Los nodos tienen su propia memoria y procesador





| Ejercicio Práctico |

Blockchain Humano

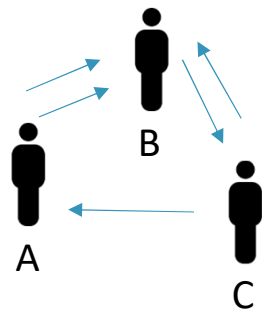
Ejercicio Práctico

Blockchain "social"

Bloques



$s \rightarrow a$ $a \rightarrow b$ $b \rightarrow c$ $c \rightarrow a$???
5BTC **3**BTC **2**BTC **1**BTC

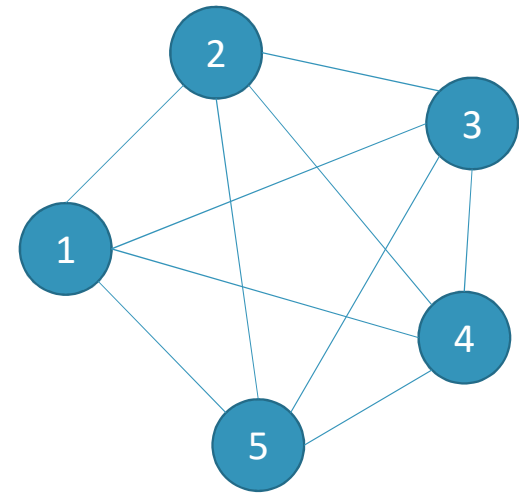


Cuentas

$A \rightarrow B$
1BTC

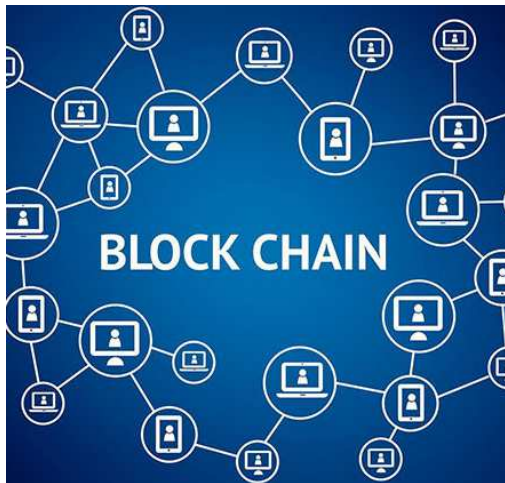
$C \rightarrow B$
1BTC

Mineros



BlockChain

Preguntas Clave




¿Cómo hacer para que se respeten el orden de los Bloques?

¿Como se protege la integridad de la cadena?

¿Cómo se evitan colisiones de escritura?

¿Qué incentivos tienen los mineros?



Blockchain no es solo BitCoin

Otras Redes

- Ethereum
- Quorum

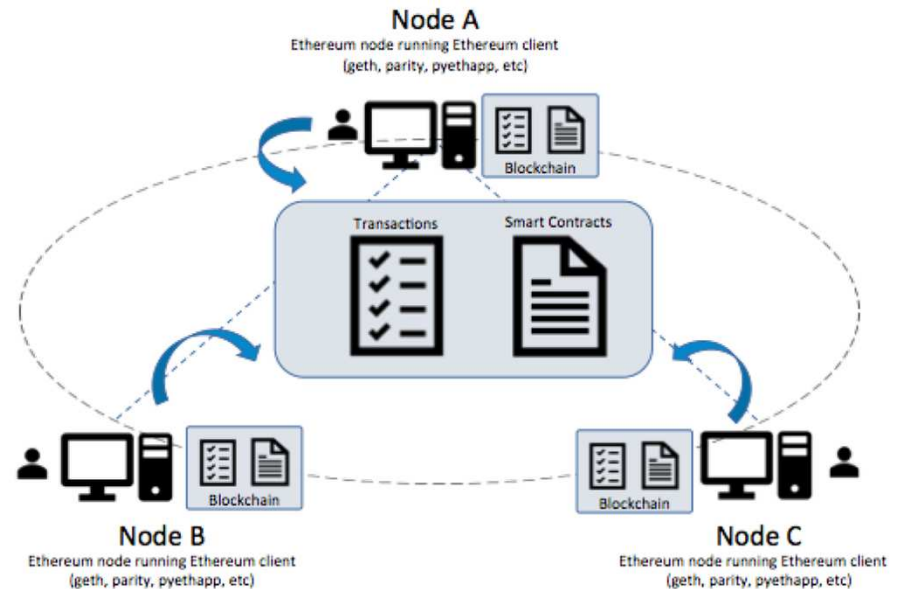
Red Ethereum



Ethereum es una plataforma open-source, **descentralizada** que permite la creación de acuerdos de **contratos inteligentes** entre pares, basada en el modelo blockchain.

Cualquier desarrollador puede crear y publicar aplicaciones distribuidas que realicen **contratos inteligentes**.

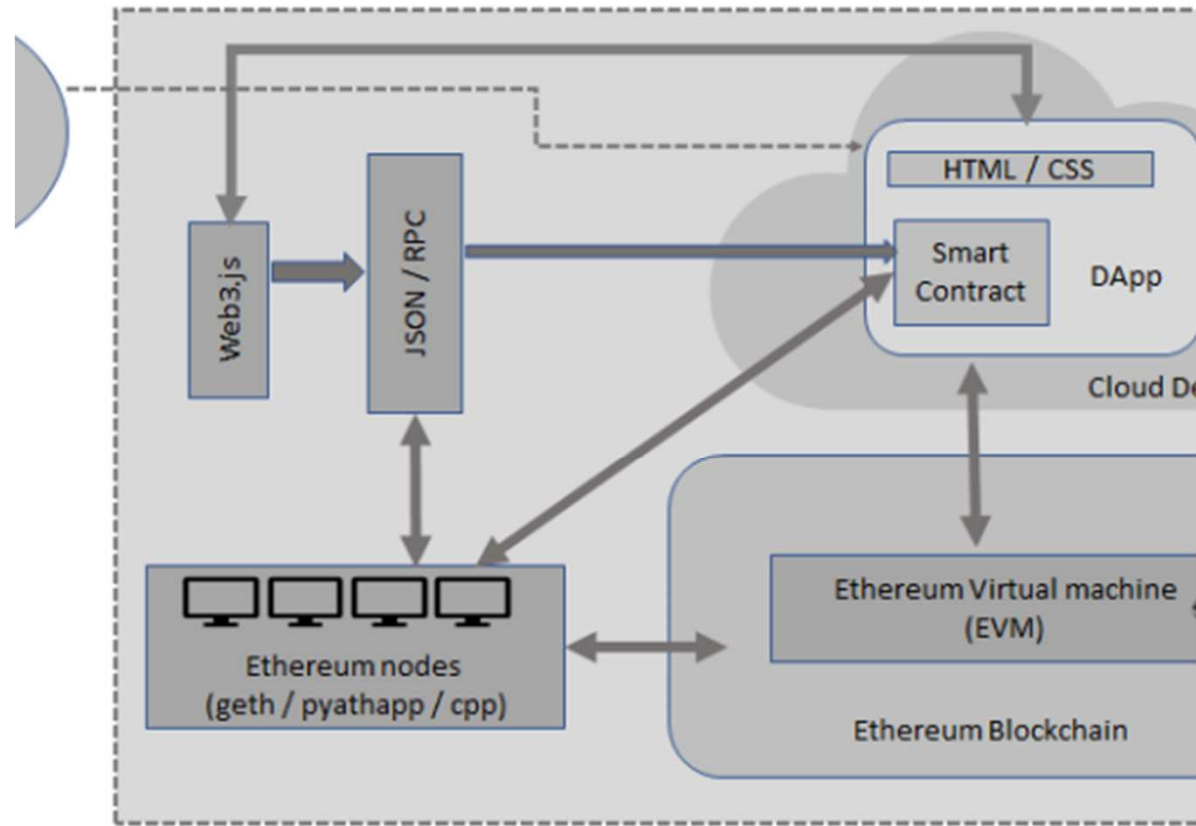
Se puede intercambiar **ether** entre cuentas diferentes y también para compensar los nodos participantes por los cálculos realizados.



La Máquina Virtual (EVM)



- La máquina virtual (**EVM**) aísla e independiza la ejecución de los smart contracts de la máquina residente.
- Hay dos tipos de cuentas en ethereum: externas (controladas por los pares de claves pública-privada) y las cuentas de "contratos" almacenadas con las cuentas.
- **EVM** soporta transacciones entre cuentas (de contrato o externas).
- Cada transacción ejecutada en la EVM consume **Gas**.



Smart Contracts

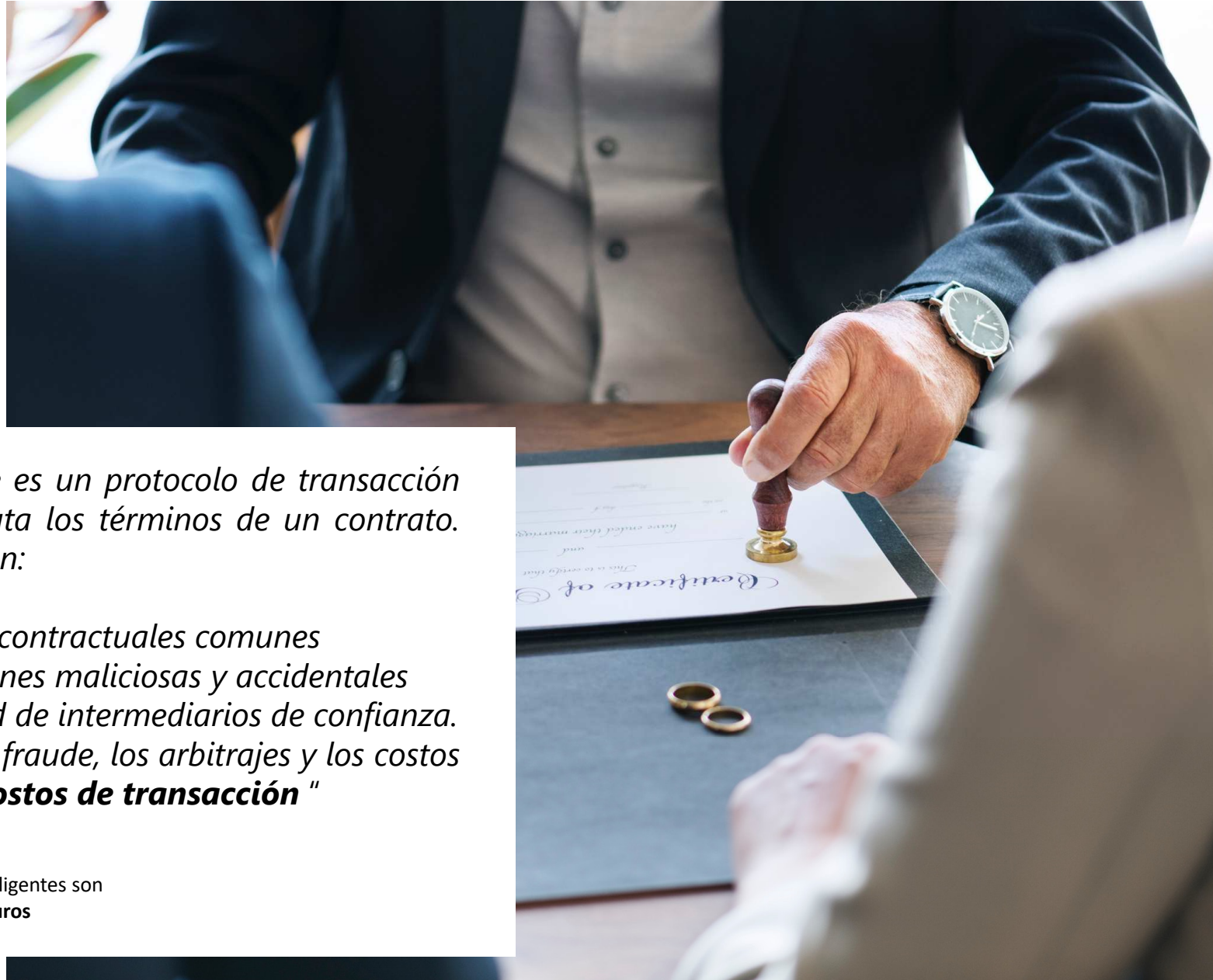


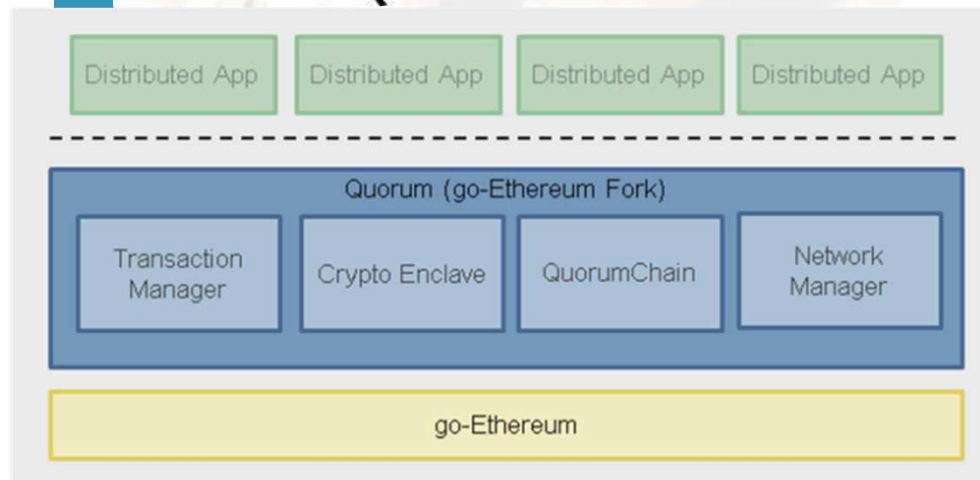
Un **contrato inteligente** es un protocolo de transacción computarizado que ejecuta los términos de un contrato. Los objetivos generales son:

- Satisfacer condiciones contractuales comunes
- Minimizar las excepciones maliciosas y accidentales
- Minimizar la necesidad de intermediarios de confianza.
- Reducir la pérdida por fraude, los arbitrajes y los costos de ejecución, y otros **costos de transacción** "



Los contratos inteligentes son **imparables** y **seguros**





INTRODUCCIÓN

Red Quorum

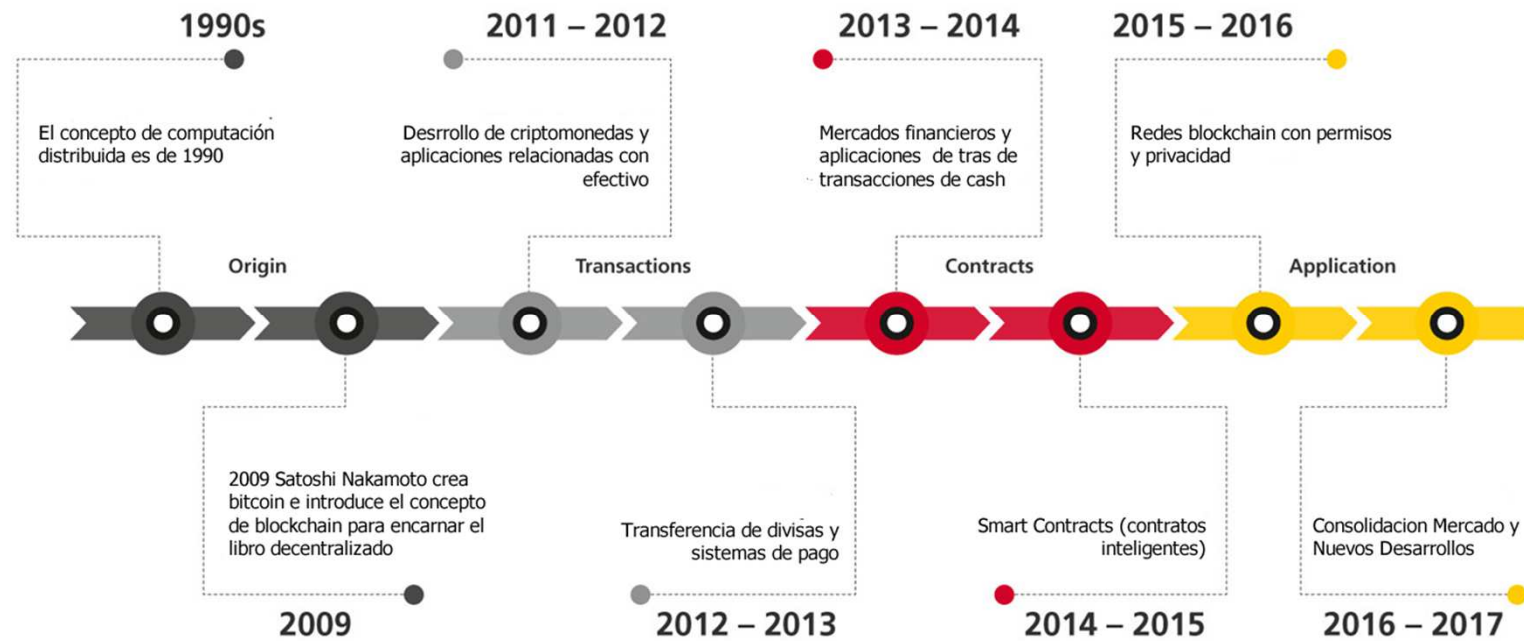
Quorum se construye a partir de Go Ethereum, el código base para la cadena de bloques Ethereum.

Funciona de manera muy similar a Ethereum y adiciona:

- administración de permisos de red y de pares,
- mayor privacidad de las transacciones y los contratos,
- mecanismos de consenso basados en la votación
- mayor rendimiento.



Historia de Blockchain



BLOCKCHAIN

Mitos y Realidades

Blockchain es Bitcoin

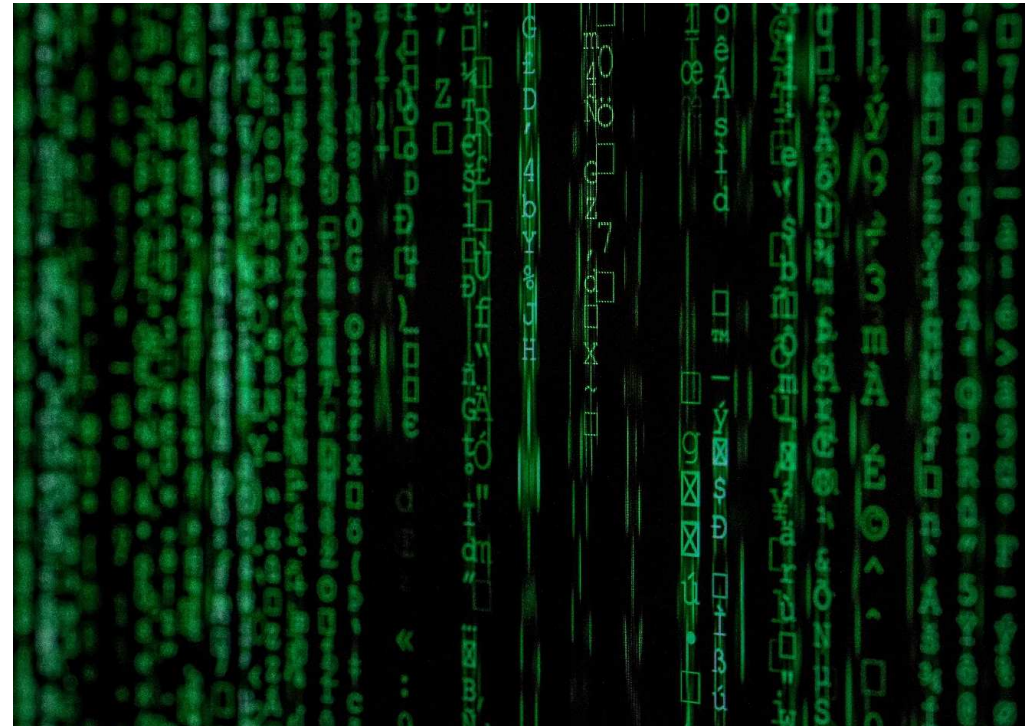


- Sin Blockchain, no habría Bitcoin.
- Pero sin Bitcoin, podría haber Blockchain, de hecho se está masificando su uso.
- El bitcoin no es la única aplicación que tiene el Blockchain.

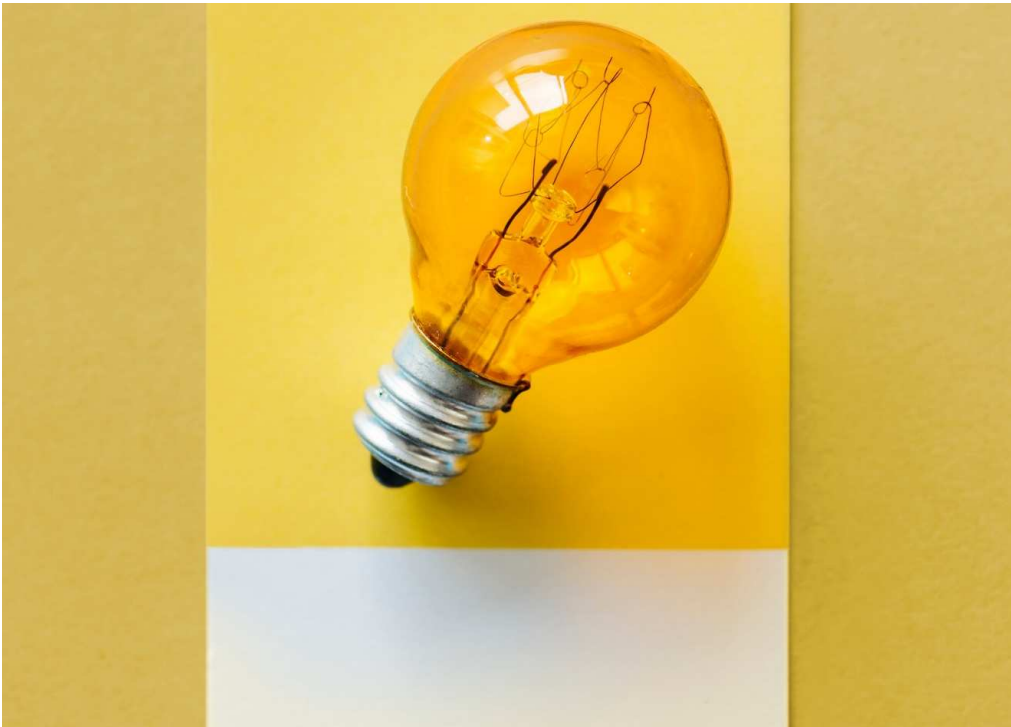
¿Usarla es riesgosa o ilegal?

Utilizar esta tecnología no trae riesgos; tampoco es ilegal, su diseño trata de resolver algunos problemas de las bases de datos convencionales

“La confusión parte al vincular el Blockchain como mecanismo habilitador de las criptomonedas, ya que estas no son legales en Colombia”



¿Permite la Innovación de las Empresas?



Esta herramienta es considerada una de las tecnologías disruptivas que cambiarán el mundo tal como hoy lo conocemos.

Su uso significa la eliminación de **terceros de confianza** para validar una transacción entre dos o más implicados.

Cada industria debe pensar cómo aprovechar esta tecnología para facilitar, agilizar y hacer más transparentes y seguros sus procesos.

¿Acaba con el Sistema Financiero?

El sector financiero es uno de los pioneros en el entendimiento y aplicación de la tecnología, en la prevención de fraudes y en la gestión casi en tiempo real de operaciones de transferencias monetarias basadas en consenso por cumplimiento de contratos

“La confusión parte al vincular el Blockchain como mecanismo habilitador de las criptomonedas, ya que estas no son legales en Colombia”



¿Solo sirve para transferir dinero?



En cualquier industria en que se necesite un consenso entre partes para realizar una operación, hay la necesidad de un ente mediador que actúe como garante, es ahí donde el Blockchain tendrá el protagonismo.

Existen ya usos ampliamente descritos en **salud, defensa, educación y gobierno**, en los que la herramienta elimina la necesidad de un ente centralizado para garantizar la legalidad o consenso de una operación.

¿Sirve para todo?

Blockchain **no puede resolver todos los problemas**. Algunos problemas ya tienen una buena solución y otros necesitarán otra tecnología que quizás no exista todavía.

En algunas redes las transacciones en están tomando más de 10 minutos. No lo hace viable para operaciones de micro pagos





BLOCKCHAIN

CASOS DE USO



Sector Salud

Los pacientes, los proveedores o las organizaciones de salud pueden colaborar utilizando Blockchain.

- Interoperabilidad nacional
- Accesibilidad a los registros médicos
- Contratos inteligentes
- Identidades digitales del paciente
- Investigación clínica
- Ciberseguridad



GemOs Health
PHILIPS

Pokitdok


HealthCombix
S. Medicos
decentralizados.

Bl. Healt Co
Pacientes e
Investigadores.

PointNurse
Asistentes
Virtuales.

Sector Industrial



A nivel industrial cualquier compañía puede beneficiarse de las distintas aplicaciones del blockchain ya que este sistema hace posible la trazabilidad total de un producto, desde que se fabrica hasta que lo compra un consumidor final.

- Trading Energético
- Farmacéutico
- Cadena de Suministro
- Logística



Sector Financiero

Finanzas, microseguros y demás actividades financieras con las siguientes ventajas:

- Disminución de Papel
- Transferencias transfronterizas
- Interacciones con empresas
- Identidad Digital



ViDChain
Identdad Digital

 **ripple**

 **ALASTRIA**

 
 **gasNatural**



BLOCKCHAIN

SECTOR PÚBLICO

Singapur:



El gobierno está buscando con blockchain detener **fraudes** bancarios de los comerciantes.

Esto ha llevado al gobierno de Singapur a desarrollar un sistema con bancos locales enfocados en prevenir el fraude de facturas usando **Blockchain para crear un hash criptográfico único** (una huella digital única) para cada factura.

E-Government Estonia

"Somos, en teoría, el primer país del mundo que puede funcionar sin un territorio físico. Todos los procesos gubernamentales pueden permanecer operativos incluso en circunstancias críticas. Podríamos votar, pagar impuestos, tomar decisiones. Estamos creando una nación digital en la nube"

Marten Kaevats

Asesor de estrategias digitales

Gobierno de Estonia



Voto Electrónico

**Registros
Médicos**

Impuestos

**Tramites
Digitales**

BitNation



Bitnation es la primera nación voluntaria descentralizada sin fronteras del mundo (DBVN). Bitnation comenzó en julio de 2014 y acogió el primer matrimonio Blockchain del mundo, certificado de nacimiento, identificación de emergencia de refugiados, ciudadanía mundial, constitución DBVN y más

DECODE

El proyecto **DECODE** surge como respuesta a la preocupación por la creciente cantidad de datos personales que se almacenan de forma centralizada y sin control por parte del usuario en Internet.

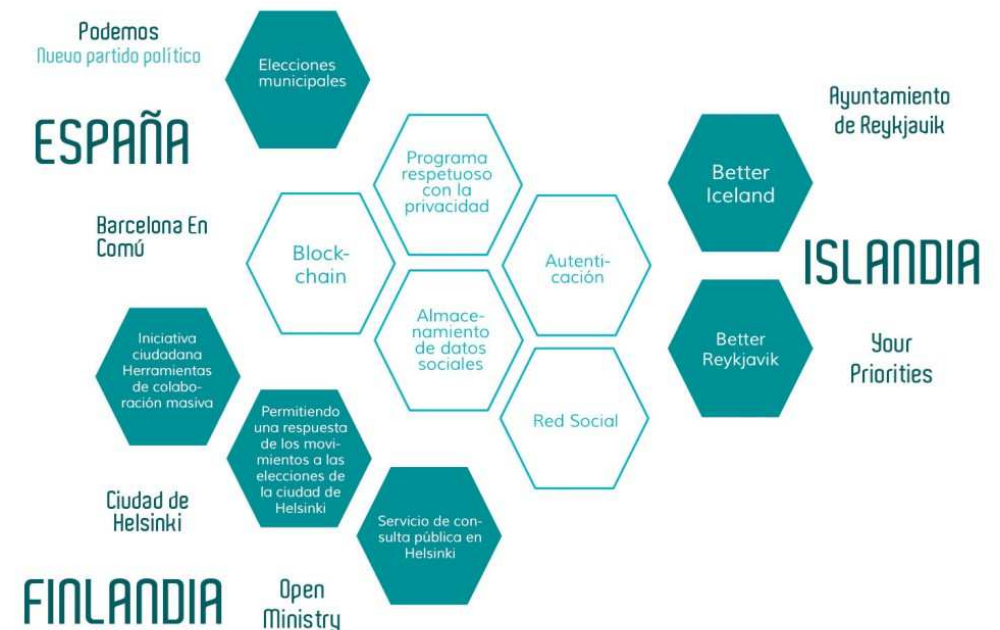


D-CENT

D-CENT permite debatir y compartir contenidos, participar en deliberaciones a gran escala, elaborar políticas colaborativas y votar.

La plataforma modular incluye herramientas para la democracia en red:

deliberaciones a gran escala, debates, votaciones, elaboración de políticas colaborativas y algoritmos de filtrado colectivos.





BLOCKCHAIN

BLOCKCHAIN

CASO COLOMBIA



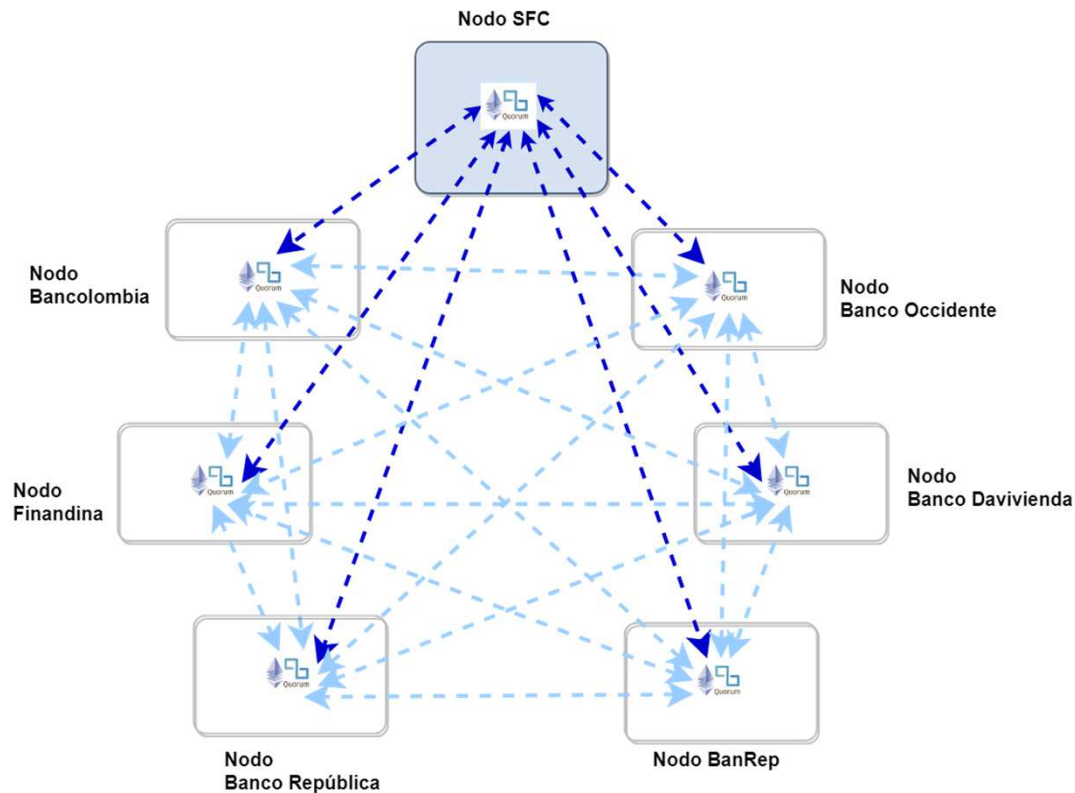
Superintendencia Financiera



Piloto BlockChain interbancario en Colombia

Libro descentralizado de movimientos de dinero entre entidades financieras.

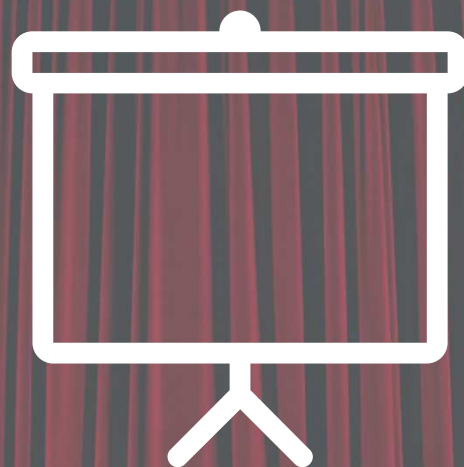
Integra actores institucionales, bancos, regulador y personas.



Privacidad

Oportunidad

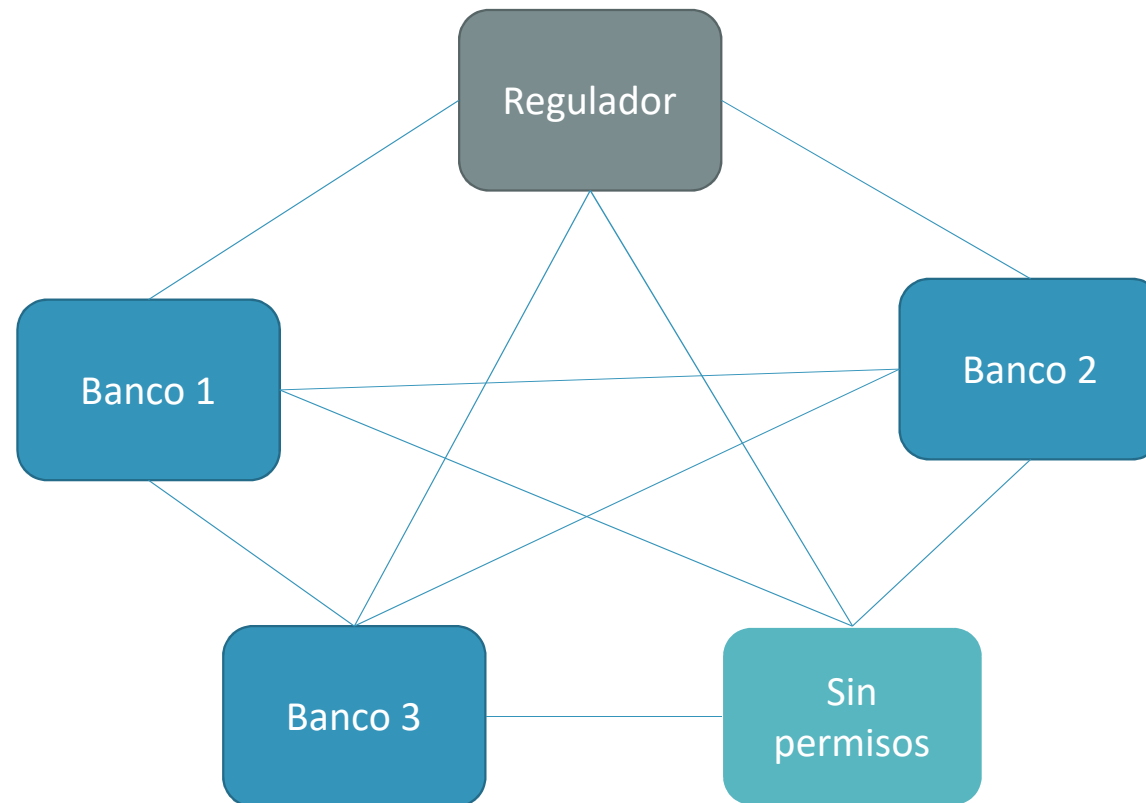
Descentralización



| Demo |

Blockchain en Acción

Liquidación Bruta Interbancaria





¿Preguntas?

aws



Hightech
Software

Gracias!



Andrés Barrantes Bernal

@abarrantesb

abarrantes@htsoft.co

CEO HighTech

www.htsoft.co

aws partner
network

Standard
Consulting
Partner