

A dark blue background featuring a network of white lines connecting various circular icons. The icons include a Bitcoin symbol (a large 'B' with two vertical bars), a globe, a robot, a stack of coins with a dollar sign, a chain link, a server rack, a lightbulb, a brain, a shield with a checkmark, a document with a checkmark, a person wearing a hat, a bar chart, a speech bubble, a binary code '00101' and '11001' with arrows, a grid of squares, a document with a checklist, a globe with a 'WWW' symbol, and a stack of papers. The word 'Blockchain' is written in large, white, sans-serif font across the center.

# Blockchain

BLOCKCHAIN

# Blockchain

- Definiciones básicas.
- Características de un sistemas distribuido.
- Origen de la Blockchain.
- Definición de Blockchain.

# Elementos Básicos

- Funcionamiento de la Blockchain.
- Características de la Blockchain
- Elementos que componen la Blockchain.

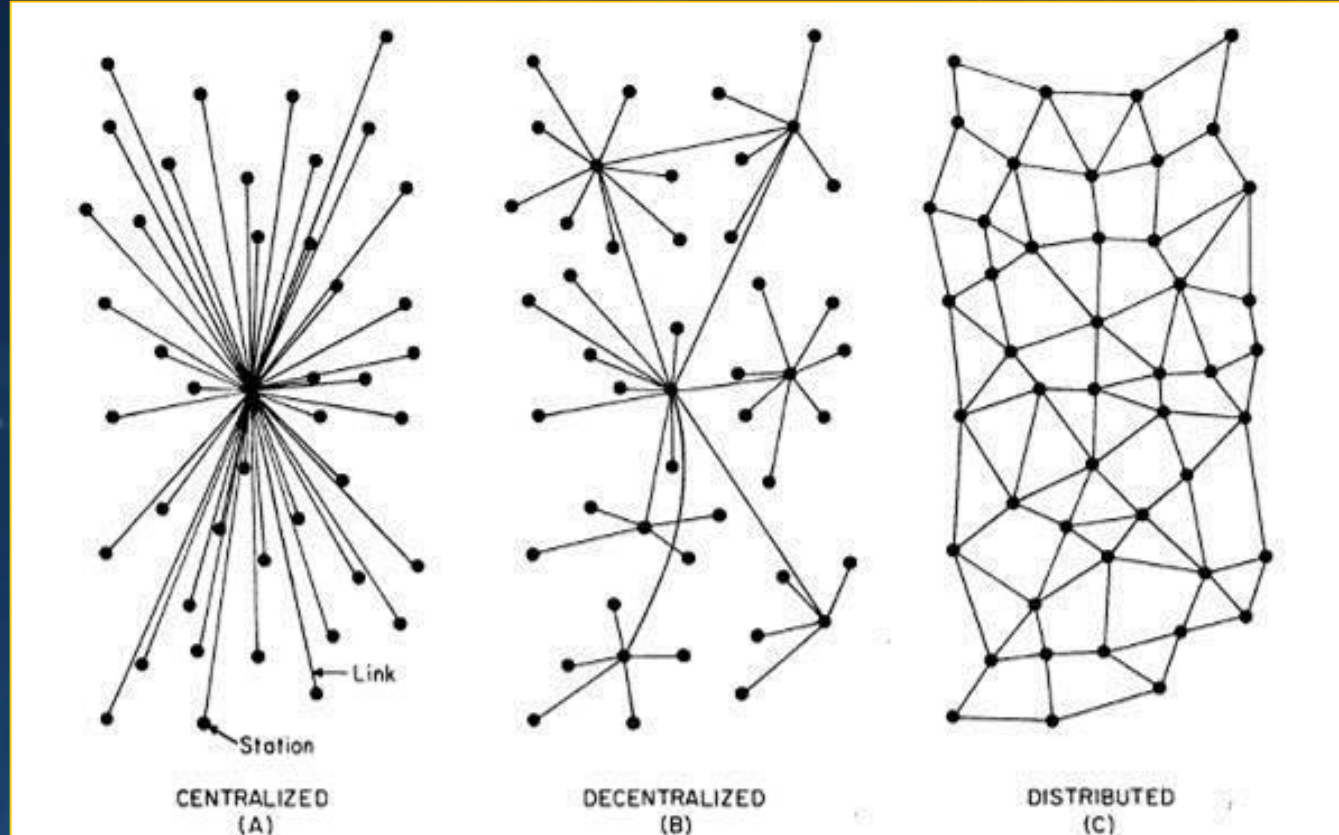


# Definiciones Básicas



# ¿Qué es una Red?

Se refiere al conjunto de equipos que están interconectados y que comparten diversos recursos.



**Red Centralizada:** Todos los nodos, menos uno, son periféricos y sólo pueden comunicarse a través del nodo central.

**Red Descentralizada:** no existe un único nodo central sino un centro colectivo de nodos centrales.

**Red Distribuida:** Todos los nodos se conectan entre sí sin que tengan que pasar necesariamente por uno o varios centros

# Definiciones Básicas

**Nodos:** son computadoras que se encargan de almacenar una copia exacta del libro contable y de hacer cumplir las reglas de la red, estos son guardianes de la red.



Los **sistemas distribuidos** son un paradigma informático, mediante el cual, dos o más nodos trabajan manera coordinada.



con el fin de lograr un **resultado común.**

# Sistemas Distribuidos

## CARACTERÍSTICAS DE LOS SISTEMAS DISTRIBUIDOS

### Consistencia

garantiza que todos los nodos tengan una única copia de datos más reciente.

### Disponibilidad:

permite que el sistema esté activo, accesible para su uso, acepte solicitudes entrantes, y responda sin ningún error como y cuando necesario.

### Tolerancia a las fallas

garantiza que si un grupo de nodos falla, el sistema distribuido todavía continuará funcionando correctamente.

# Origen de la Blockchain

Primeras aproximaciones a los Sistemas Distribuidos:

Ingeniero Paul  
Baran

“Sobre redes de comunicaciones distribuidas”

1962

Leslie Lamport

“Trivia sobre el consenso entre nodos”

1982

Castro y Liskov

“Algoritmo de tolerancia a fallas bizantinas (PBFT)”

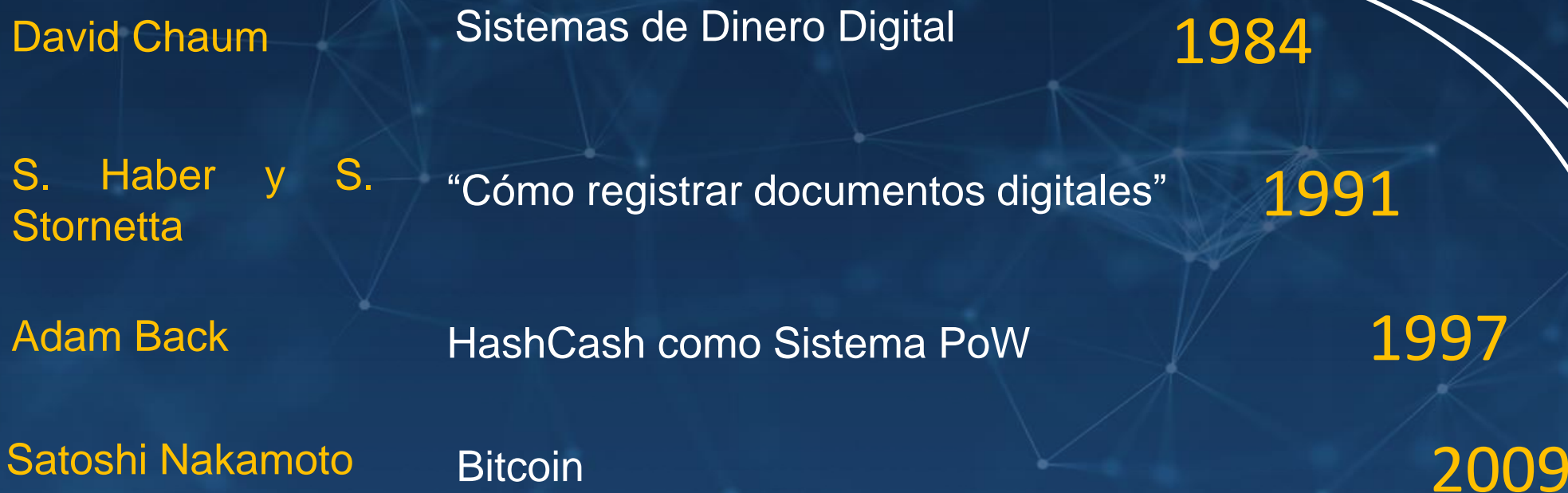
1999





# Origen de la Blockchain

Primeras aproximaciones al Dinero Digital:



# Origen de la Blockchain

Bitcoin

Blockchain

Esquemas de  
Dinero  
Digital

Sistemas  
Distribuidos



# Blockchain

# Blockchain



Esta tecnología permite la realización confiable y **segura** de cualquier tipo de transacción entre dos o más personas sin la necesidad de intermediarios, a través de Internet.

La Blockchain es una **base de datos distribuida** que también puede ser entendida como un libro de contabilidad compartido, este libro mantiene una lista del registro de **información** (Transacciones, documentos, archivos, cualquier tipo de información digitalizada) protegida criptográficamente de alteraciones.



Blockchain es una articulación de diferentes tecnologías como lo son las wallets, los nodos y los mineros.



# Definiciones Básicas

## Wallets



Las Wallets o “carteras digitales”, son interfaces gráficas para interactuar con la red blockchain que permiten a los usuarios poseer fondos en criptoactivos, realizar transacciones y manejar sus identidades digitales.

## Mineros

Los mineros son computadoras que se encargan de autorizar la adición de los bloques de transacciones que realizan las carteras digitales a la cadena de bloques, al resolver el acertijo matemático del protocolo de consenso, recibiendo a cambio recompensas en la moneda digital propia de la red blockchain.



# Blockchain

El libro mayor se crea utilizando una cadena de bloques vinculados, donde cada bloque contiene una cierta cantidad de transacciones que fueron validadas por la red en un período de tiempo determinado.

Este 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, cada libro de contabilidad distribuido, contiene un registro certero y verificable de todas las transacciones que se han hecho sin necesidad de que exista confianza entre los miembros que la conforman.



# Blockchain

La Blockchain es la solución al viejo problema humano de la confianza en terceros y al doble gasto.



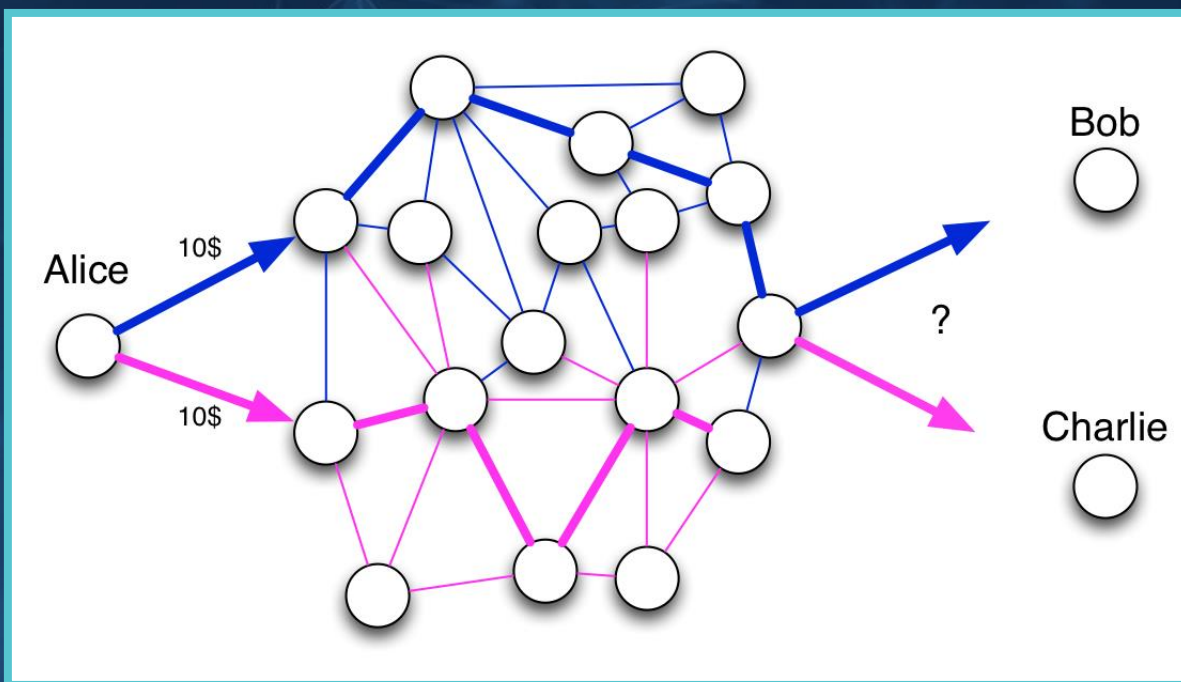
El problema de la confianza en terceros nos obliga a confiar en intermediarios que cobran por sus servicios



Dentro de la Blockchain al no haber intermediarios, los costos por transacción son menores.

# Blockchain

La Blockchain es la solución al doble gasto y al viejo problema humano de la confianza en terceros.



El **doble gasto** es un defecto potencial del dinero digital por el que una misma moneda digital puede gastarse más de una vez.



# Blockchain

Cada participante de la red guarda una copia de la cadena de bloques completa

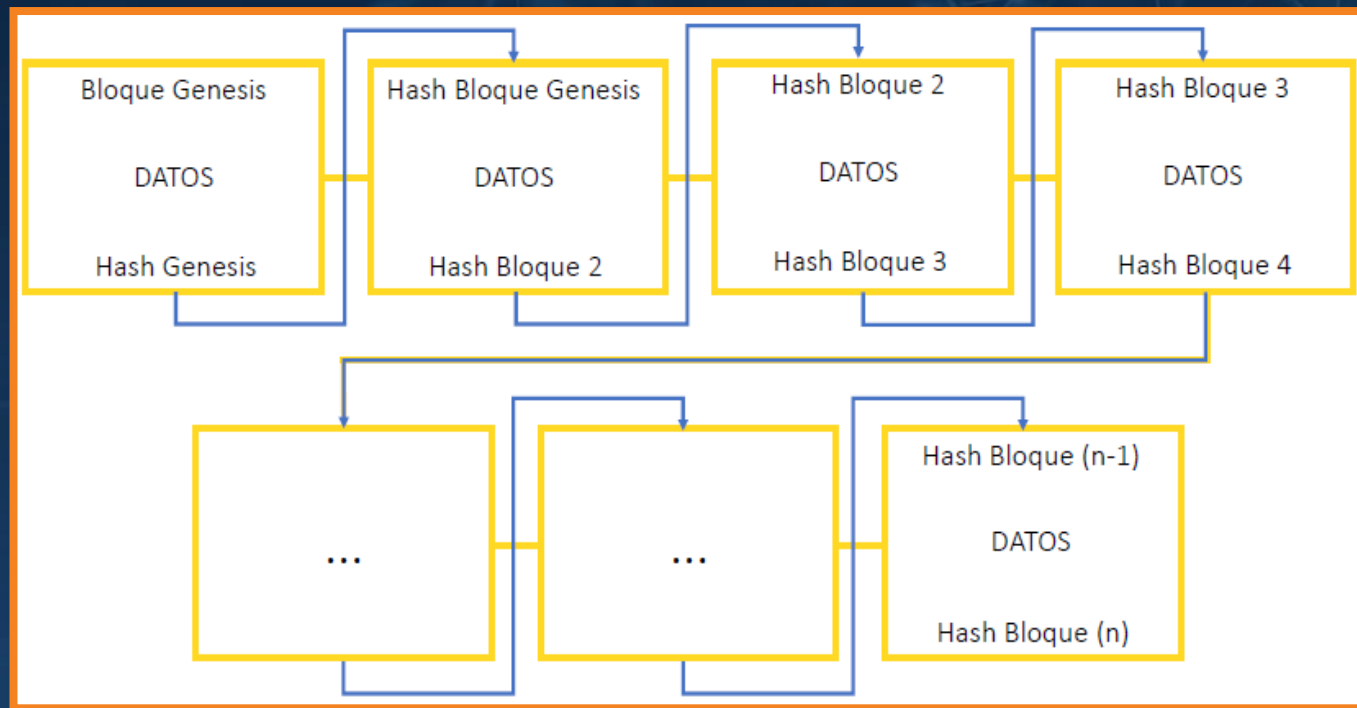
Si una parte maliciosa realiza cambios no autorizados en su copia de la blockchain en una computadora, otros miembros de la red rechazarán la transacción.



Para manipular los datos en la blockchain, se tendría que manipular datos en la mayoría de la red.

# Funcionamiento de la Blockchain

# ¿Cómo funciona?



Dentro de la cadena de bloques se le denomina **bloque génesis** al primer bloque creado y verificado de la blockchain de un criptoactivo.

# ¿Cómo funciona?

**1** La Blockchain tiene una configuración inicial que permite el almacenamiento de los datos en bloques, que son codificados mediante algoritmos de encriptación (funciones Hash).

**2** Ese hash es utilizado para conectar cada bloque de información con el bloque siguiente.

**3** Cada nuevo hash creado es el producto de los datos del bloque más el hash del bloque anterior.

**4** A esta vinculación entre bloques se le conoce como encadenamiento



# ¿Cómo se realiza una transacción?



Una transacción común en blockchain comienza con el envío de un activo digital de una cartera digital a otra.

Esta transacción es escuchada por diversos nodos y agrupada con otras transacciones.

# ¿Cómo se realiza una transacción?

Los mineros toman el trabajo, y compiten entre si por resolver un acertijo matemático que autoriza al minero que lo encuentra a proponer su bloque, con las transacciones en él para ser agregado a la cadena.



Este grupo de transacciones es luego enviado a los mineros como un trabajo a resolver, y el ganador agrega el nuevo bloque a la red.



# Características de la Blockchain

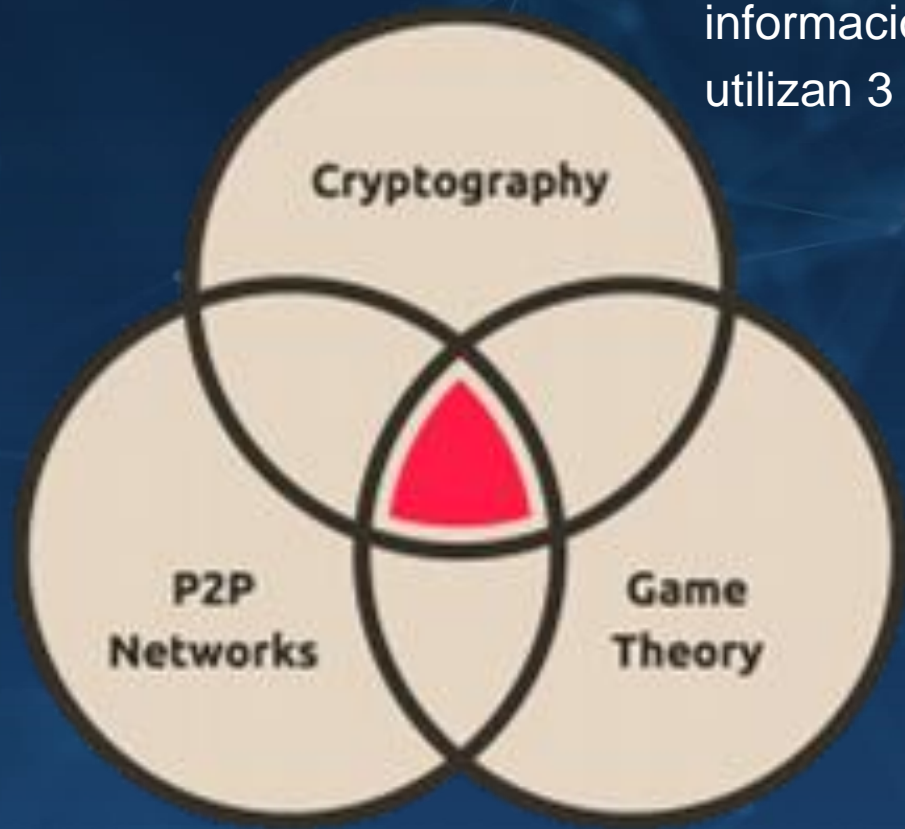
1. Es un libro distribuido
2. Todo el contenido está en formato digital.
3. La Red se actualiza en tiempo real.
4. La red es cronológica y con marca de tiempo.
5. La información está sellada criptográficamente.
6. Una vez dentro de la plataforma esta información es irreversible y auditable.
7. Funciona "sin confianza"
8. Elimina intermediarios





# Elementos de la Blockchain

La tecnología **Blockchain** plantea una forma distinta de almacenar la información en internet, en la que se prioriza la seguridad y para lograrlo se utilizan 3 elementos:

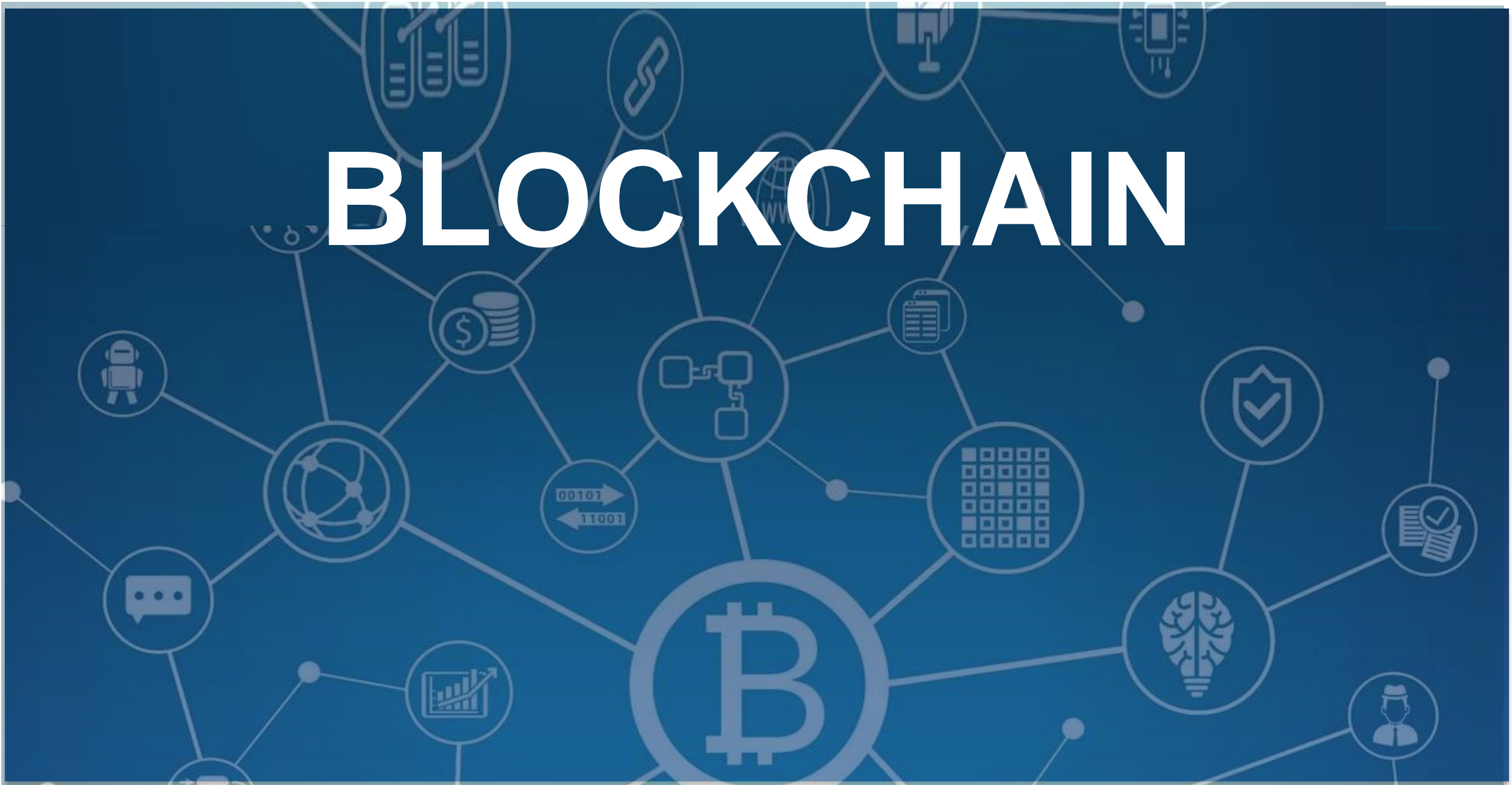


**1. Criptografía:** aporta la capa de seguridad a la información que se almacena para protegerla de modificación y alteraciones

**2. Redes P2P:** posibilita el almacenamiento distribuido y replicado de la Blockchain

**3. Teoría de Juegos:** se utiliza ya que los nodos de la red validan transacciones por consenso, siguiendo un mecanismo que contiene incentivos económicos





# BLOCKCHAIN