



# Maestría en Finanzas

FI-75301 Macrodatos y  
Fintech

M.Sc. Walter Jeremías López.

# Blockchain y criptomonedas.



# Maestría en Finanzas

FI-75301 Macrodatos y Fintech

M.Sc. Walter Jeremías López.

## Objetivos de aprendizaje:

- Comprender cómo las tecnologías DLT constituyen la arquitectura adyacente para los criptoactivos mediante la tecnología Blockchain
- Conocer las principales criptomonedas su funcionamiento y otras DApps.



# Maestría en Finanzas

FI-75301 Macrodatos y Fintech

M.Sc. Walter Jeremías López.

## Competencias a desarrollar:

- El alumno explica la manera en que blockchain funciona como la base para las criptomonedas.
- El alumno describe las principales criptomonedas y DApps del mercado en cuanto a características y funcionamiento.



# Maestría en Finanzas

FI-75301 Macrodatos y Fintech.

M.Sc. Walter Jeremías López.

## Agenda:

- Tecnologías DLT y Blockchain.
- Criptomonedas y otros criptoactivos.
- Aplicaciones descentralizadas DApps.
- Conclusiones.

# DLT: Distributed Ledger Technology

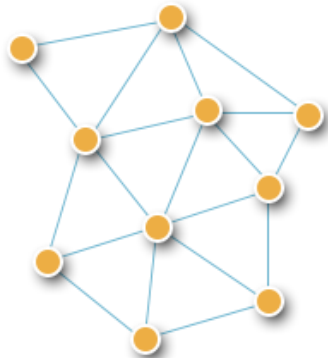
## Tipos de redes:



Centralizada

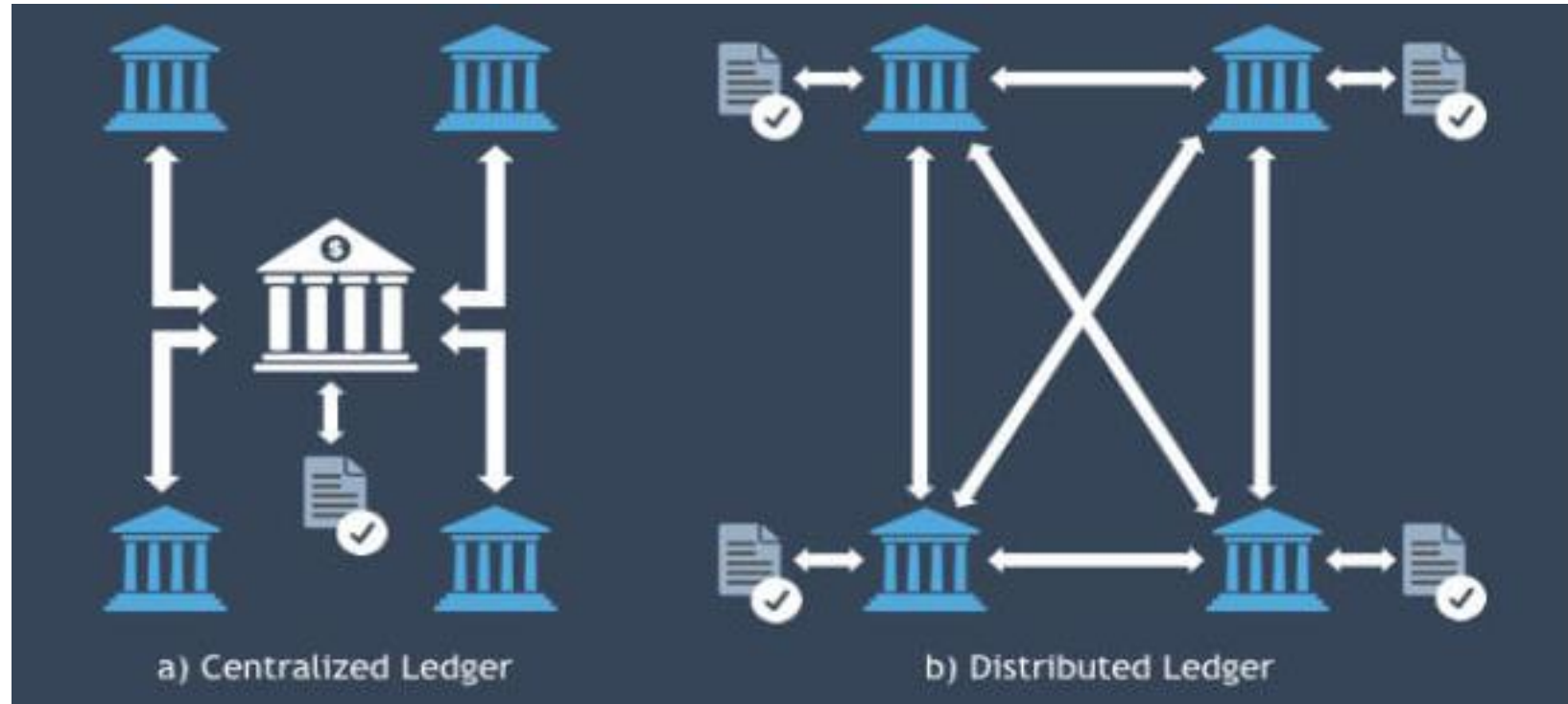


Descentralizada



Distribuida

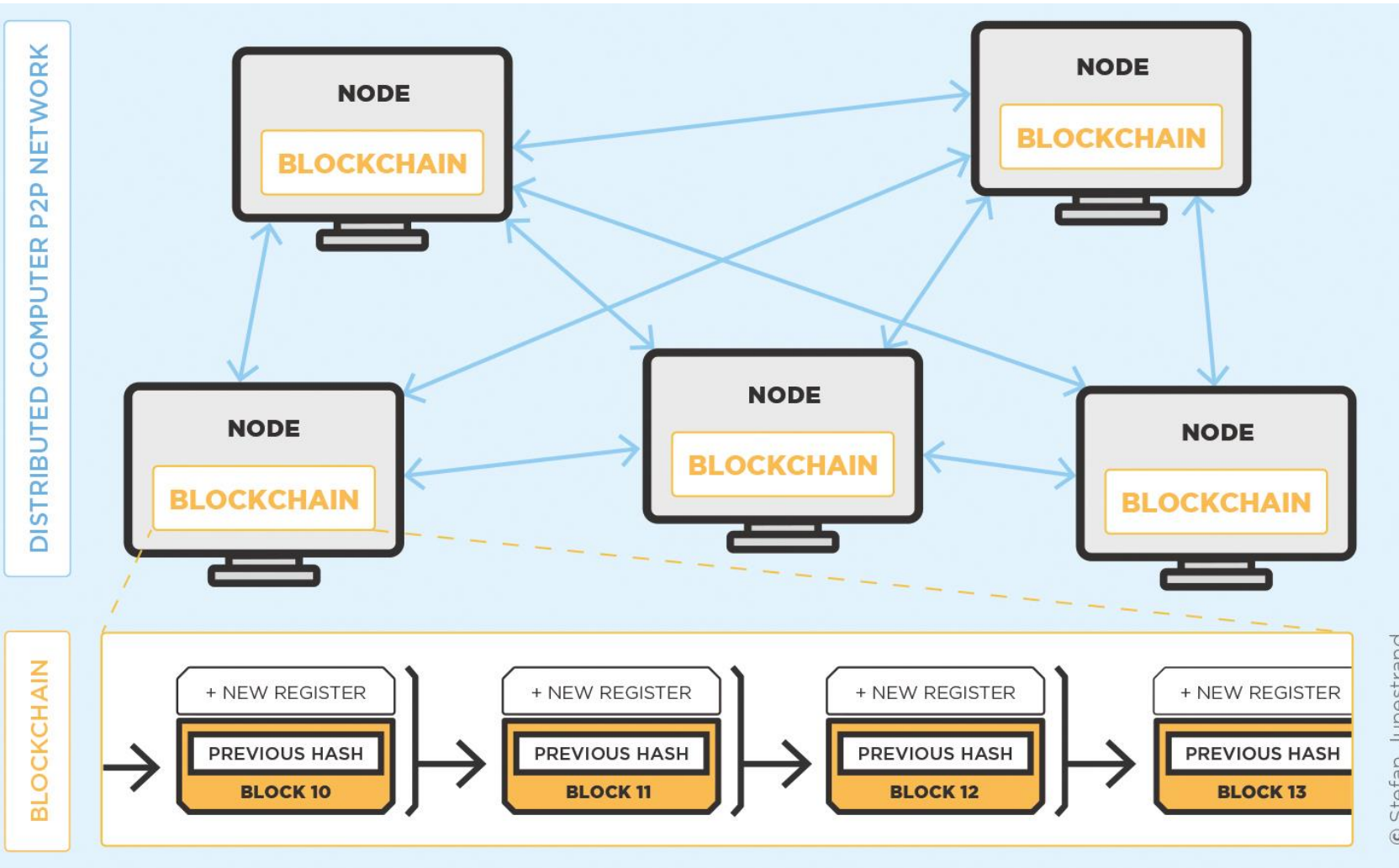
Comparación entre un sistema bancario centralizado y distribuido



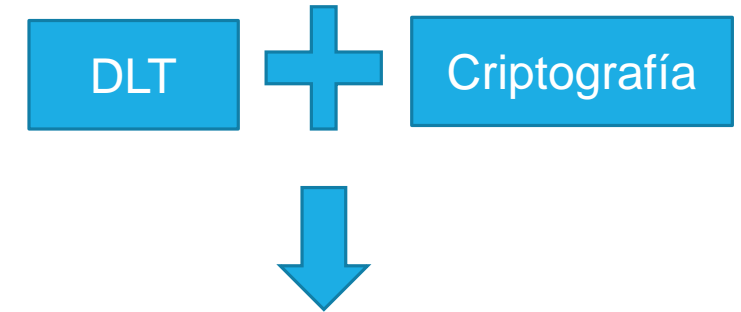
# Tipos de DLT y su funcionamiento



# Arquitectura de Blockchain



Combina dos tecnologías principales:

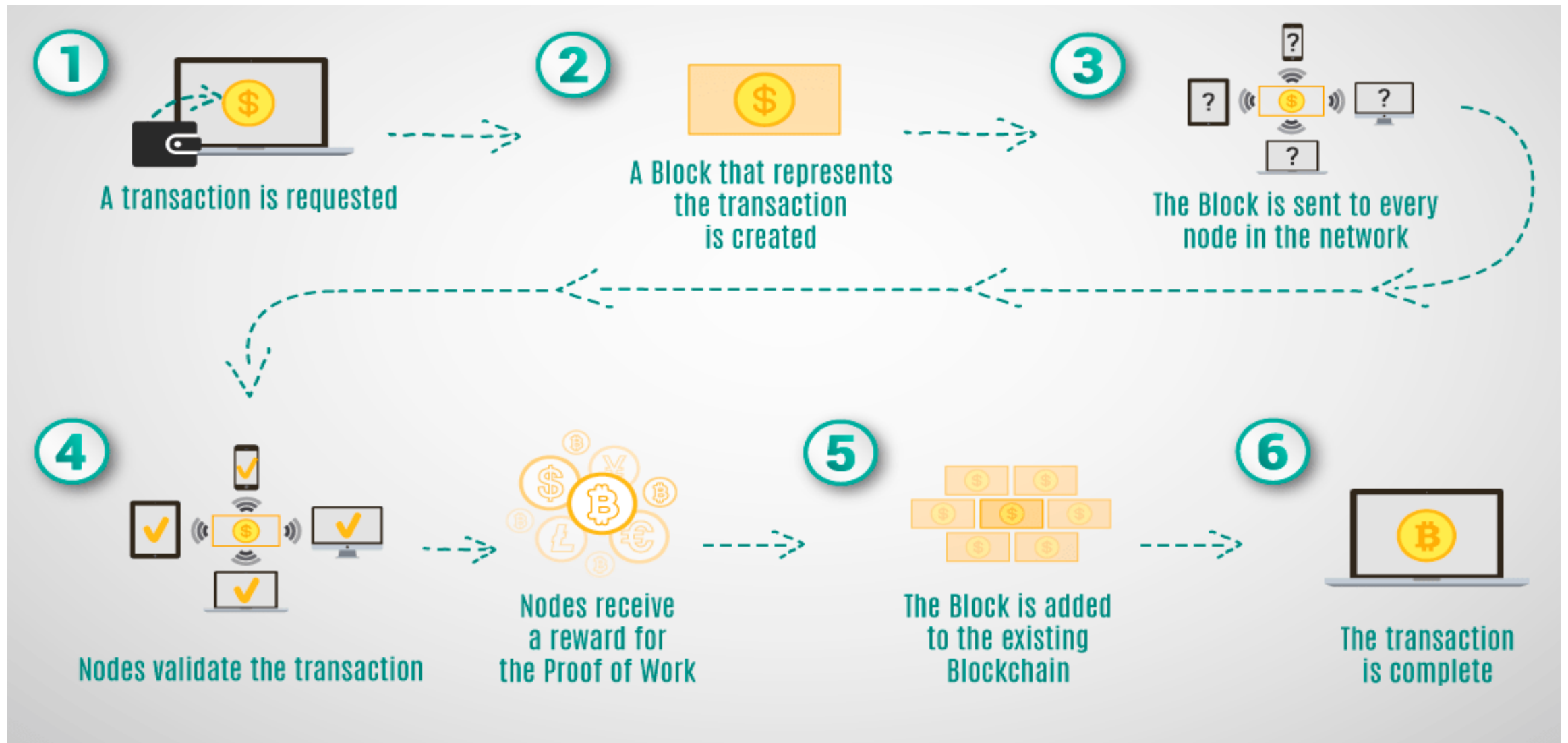


Para obtener Secure distributed ledgers, cuyas características son:

1. Seguridad.
2. Permanencia.
3. Transparencia.



# Funcionamiento de Blockchain





# Blockchain

## Versiones.

1.0

- Currency: 5 trx/min.

2.0

- Smart contracts: 25 trx/min.

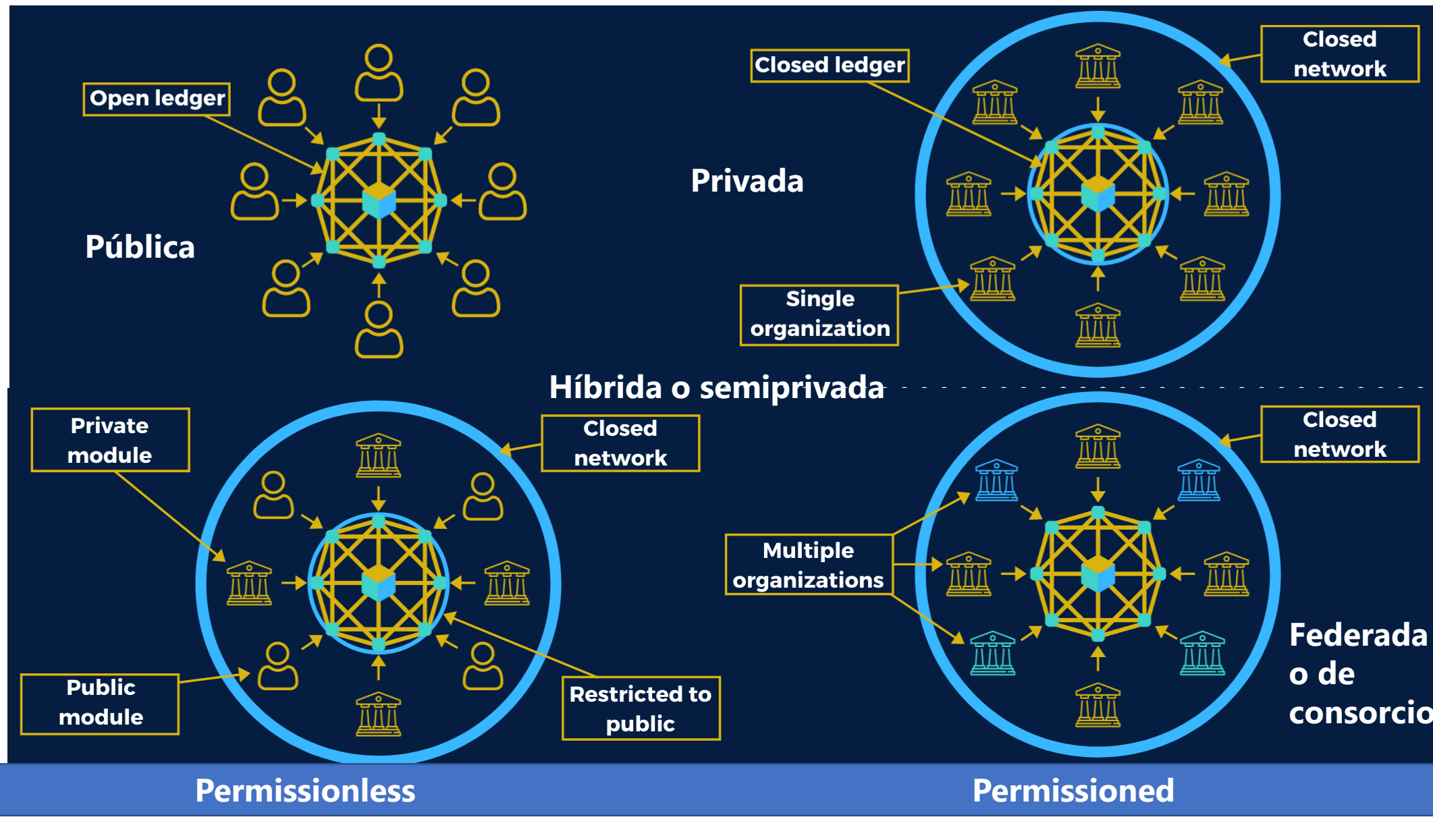
3.0

- Dapps: 2K a 4K trx/min.

4.0

- Usable en industria 4.0.

# Tipos de redes Blockchain



# Criptografía y cifrado

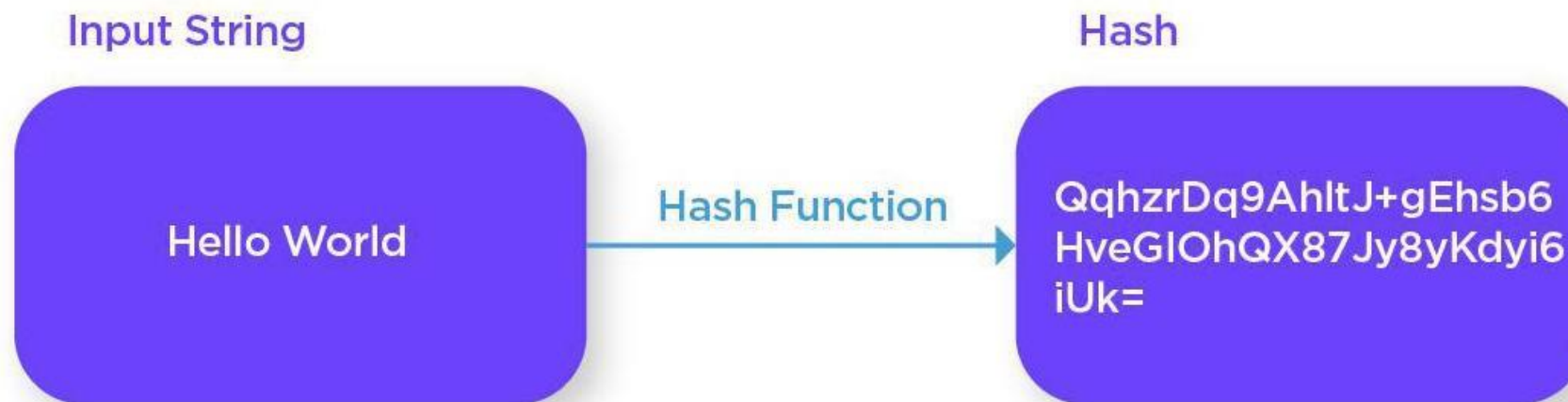
## 1. Simétrica

Es ocultar cualquier dato en un algoritmo, el receptor descifra el algoritmo a la inversa.

## 2. Asimétrica

Se crean dos llaves: privada y pública, la última la tiene cualquiera para enviar mensajes que solo pueden descifrarse con la privada.

# Funciones Hash.



- Generación de una huella digital de cualquier dato o información que lo vuelve único. También puede funcionar como sistema de autenticación. El algoritmo más utilizado es el SHA256 de la familia Secure Hash Algorithm desarrollado por la NSA considerados como los más seguros para cifrar información.

# Criptomonedas



Son activos digitales aplicando criptografía que sirven como medio de intercambio o para guardar valor. Su funcionamiento es típicamente descentralizado aunque ya algunos gobiernos han emitido sus propias.

# Bitcoin (bitcoin)



- Fue la primer criptomoneda del mercado basada en Blockchain.
- Se crea a partir del paper de Satoshi Nakamoto publicado en 2008.
- El bloque génesis se lanzó el 3/1/2009.
- En 2017 alcanzó el pico en su precio de \$19,783, siendo la criptomoneda de mayor uso, crecimiento y capitalización de mercado hasta el momento.

# Características de bitcoin

Usa Blockchain, es una moneda descentralizada y distribuida.

Es criptográfico, por lo que no permite el doble gasto.

Sin riesgo de terceros.

Costo bajo de uso.

Es un mecanismo veloz e internacional.

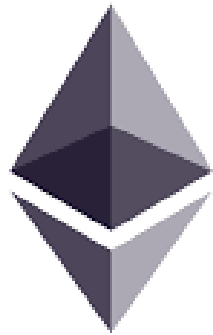
Sin derecho de admisión.

Sin confiscación posible.

Es limitado, solo se podrán minar 21 millones de bitcoins.



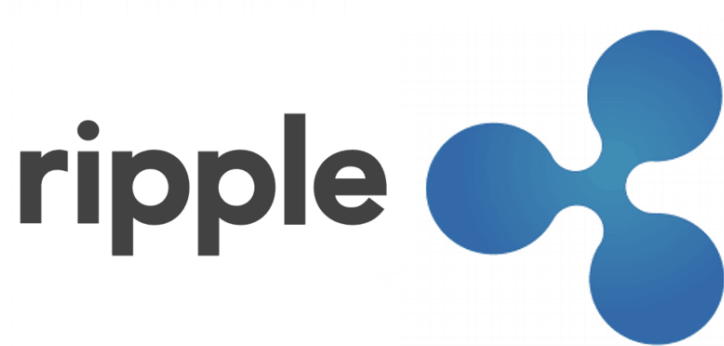
# Altcoins: Ethereum (Ether)



ethereum

- La segunda criptomoneda, al igual que en tamaño de mercado.
- Introduce el concepto de Smart contract.
- A raíz de un ataque se dividió en dos Blockchains: Ethereum (ETH) con el robo revertido y Ethereum Classic (ETC) con la cadena original.

# Altcoins: Ripple (XRP)



- Es la tercera red y criptomoneda más grande por capitalización de mercado.
- Pensada para facilitar pagos y transferencias transfronterizos de manera barata y rápida.
- No provee incentivos a los mineros y puede congeñar fondos arbitrariamente.

# Altcoins: Litecoin



- Técnicamente es casi idéntico a Bitcoin, pero Su principal objetivo es la rapidez en las transacciones.
- Busca reducir el tiempo de procesamiento de cada bloque, por lo que confirma las transacciones más rápido que Bitcoin.
- Usa un algoritmo criptográfico distinto al estándar SHA-256 llamado Scrypt, que es menos complejo.

# Altcoins: Bitcoin Cash



- Se desprende de Bitcoin, al igual que Litecoin buscaban mejorar la rapidez de las transacciones.
- La diferencia es que para lograrlo aumentaron en 8 MB el tamaño de los bloques de la cadena.
- Sin embargo, conlleva un riesgo de seguridad potencial al aumentar la velocidad de verificación de los bloques.

# Stablecoins

Son criptomonedas con mecanismos de estabilización de precios.

## Funciones del dinero

Medio de intercambio.

Atesorar valor.

Unidad de contabilidad.

Estándar de pagos diferidos.

El problema de las criptomonedas para cumplir con las funciones del dinero es su alta volatilidad.

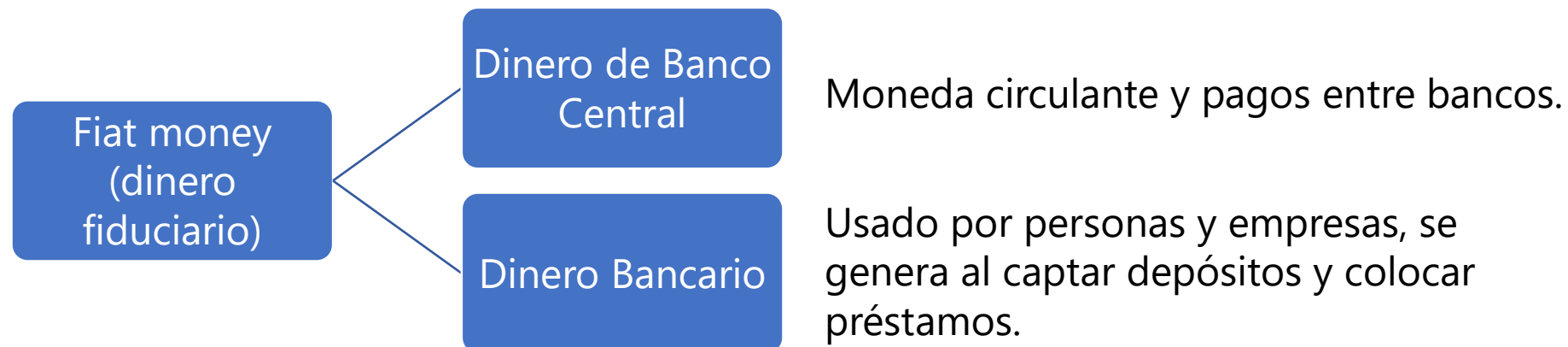
La solución requiere política monetaria, por lo que surgen las stablecoins.

# Stablecoins: Tether



- Es un ejemplo de una stablecoin respaldada por la compañía Tether Limited.
- Su precio es estable y está siempre a la par del Dólar Estadounidense.
- Para mantener el precio la empresa debe tener reservas equivalentes en dólares que respalden los Tether en circulación.

# Categorías de stablecoins



## Fiat-collateralized (Fiduciario-Garantizado)

Garantías en instituciones financieras convencionales.

Tasa de cambio fija.

Arbitraje entre precio de mercado y tasa de cambio.

No descentralizada.

## Crypto-Collateralized (Cripto-Garantizado)

Colateral retenido en un contrato inteligente.

Tasa de cambio dinámica.

Protegida la disminución de valor, pero a un costo.

Potencialmente descentralizada.

## Uncollateralized (Sin garantía)

**Pegged (vinculado).**

**Unpegged (desvinculado).**



# Crypto Exchanges

Mercado Primario



Proyectos ↔ Inversionistas

Mercado Secundario

Activos y monedas digitales



Traders ↔ Traders

# Tipos de Exchanges.

Centralizados

Autoridad central

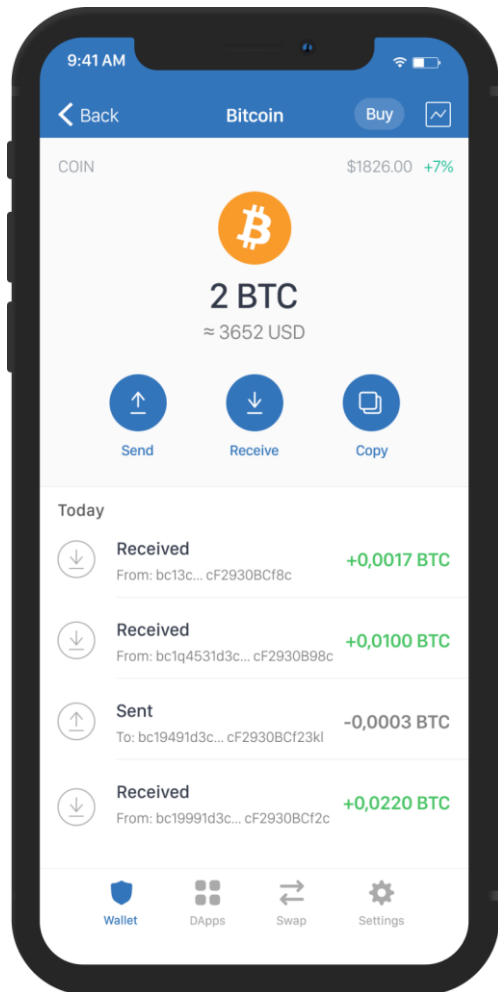


Descentralizados

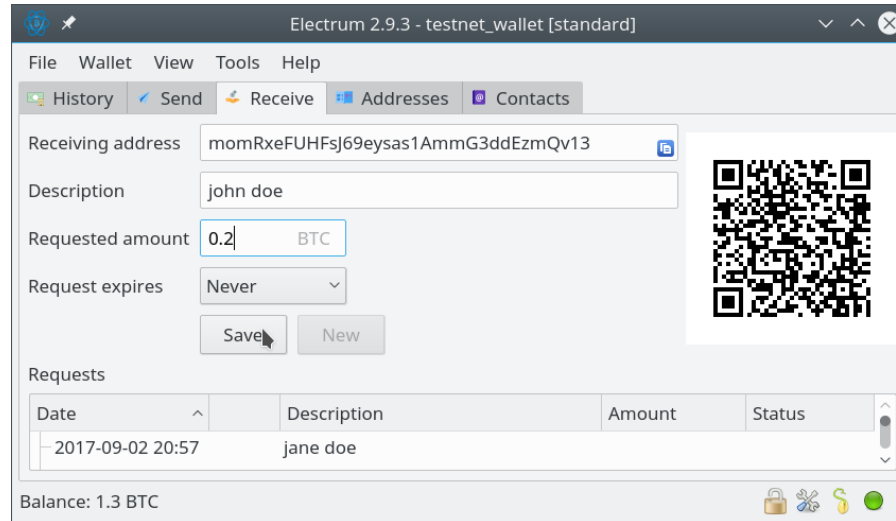
P2P



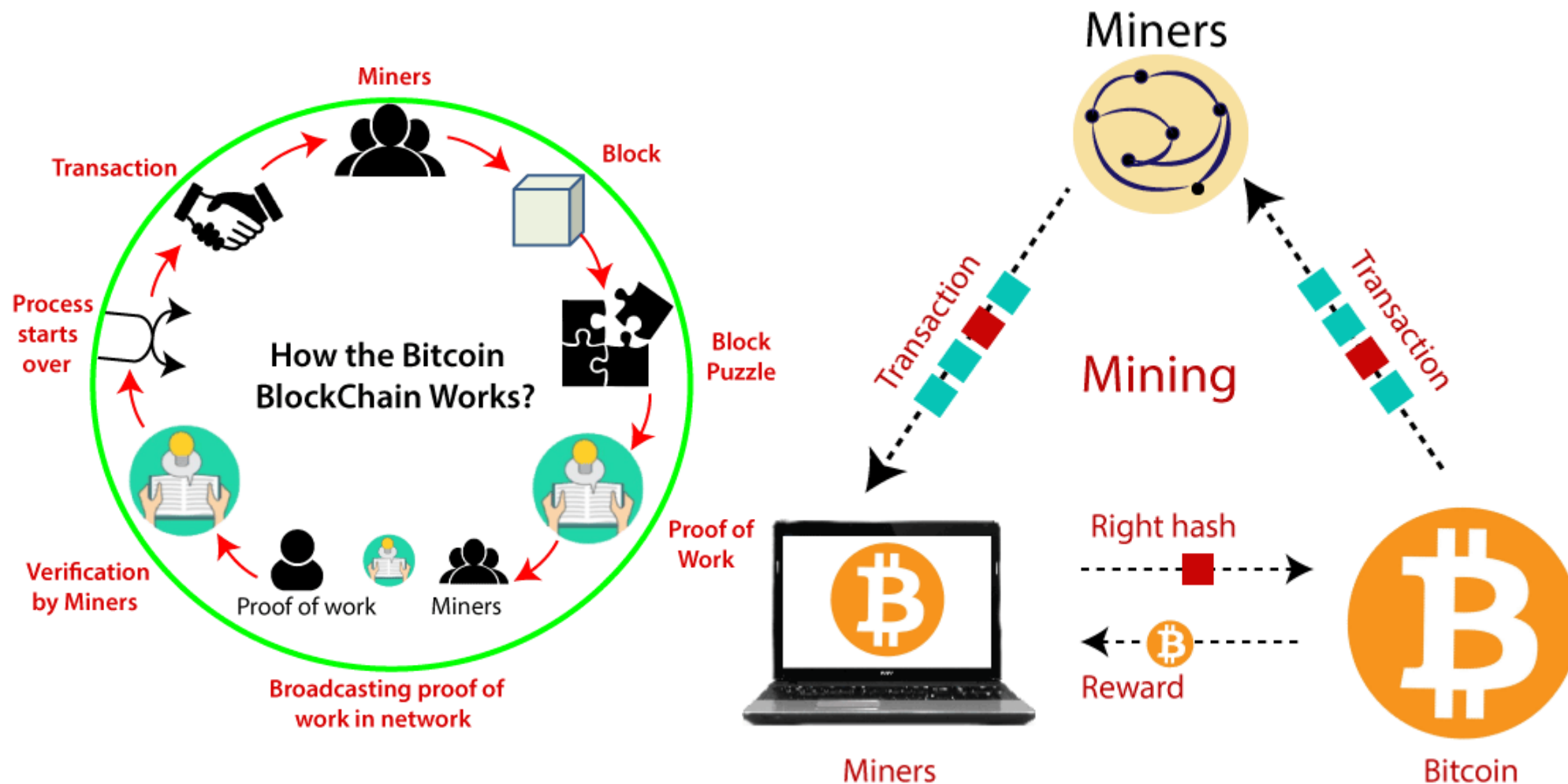
# Crypto Wallets



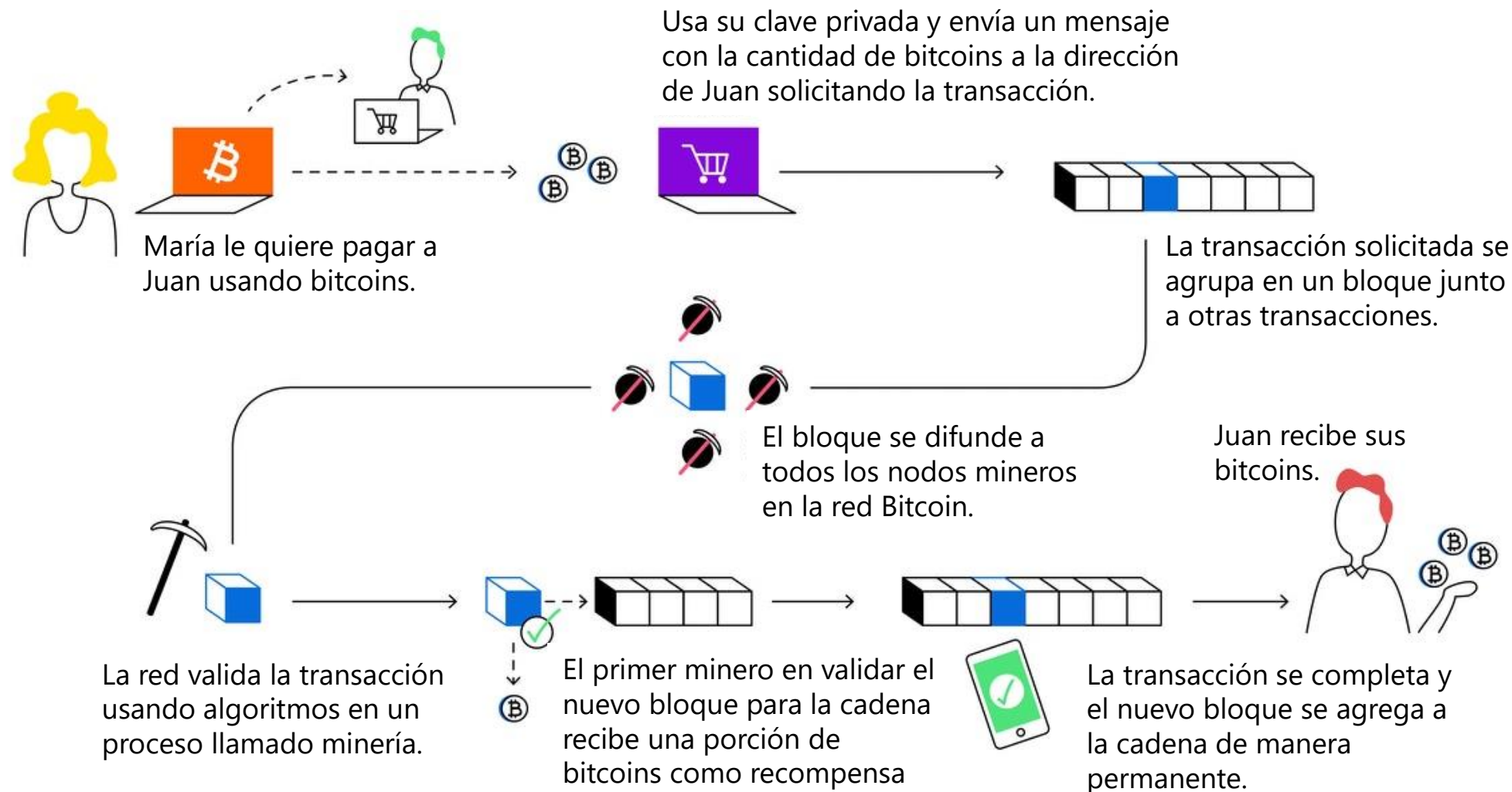
- Pueden ser de software o hardware.
- Sirven para guardar, enviar y recibir criptomonedas y tokens.
- Si el usuario olvida su clave privada o sus doce palabras su dinero quedaría atrapado.



# Minería y mecanismos de consenso.



# Proceso de minería.





# Pools de minería



Halving de bitcoin

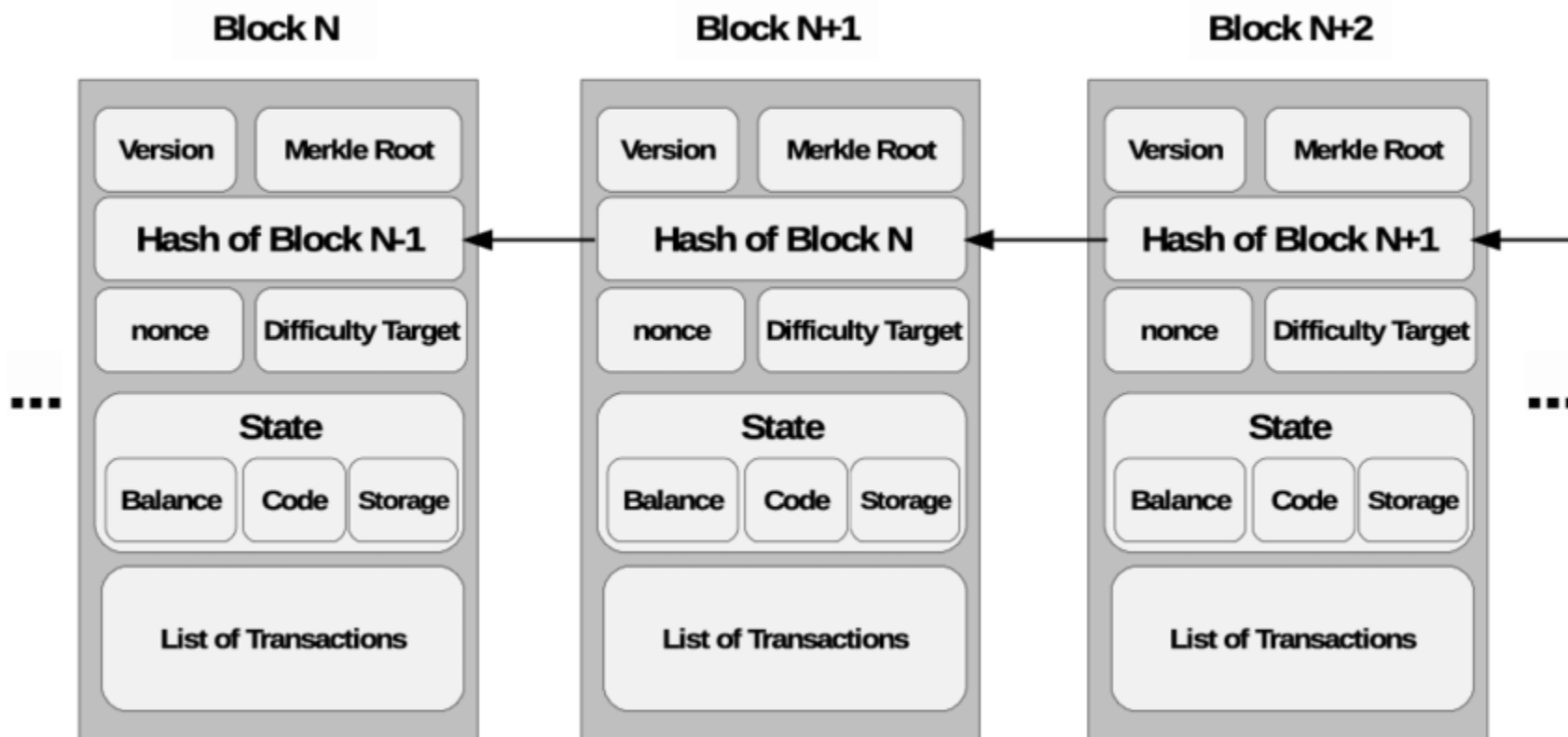


Granja de minería



# PoW (Proof of Work)

Consiste en la dificultad para permitir agregar el siguiente bloque de la cadena encontrando un hash con ciertas características, por lo que el cálculo matemático se vuelve más complejo.





# PoS (Proof of Stake)

## PROOF OF WORK



La probabilidad de minar un bloque es determinada por el poder computacional del minero



Se da una recompensa al primer minero que resuelva el rompecabezas criptográfico de cada bloque



Los mineros compiten entre sí usando poder de cómputo, por lo que las comunidades de mineros tienen a ser más centralizadas.

## PROOF OF STAKE



La probabilidad de validar un nuevo bloque es determinada por el número de monedas que posee.



Los validadores no reciben una recompensa por cada bloques, sino una comisión.



Los sistemas PoS pueden ser mucho menos costosos y más eficientes que los PoW, pero son menos probados.

# Otros protocolos de consenso:



Reduce el alto consumo de energía de PoW.



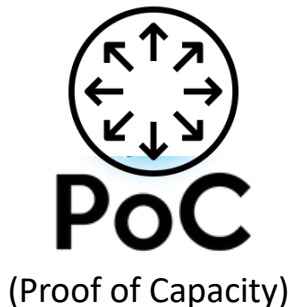
Prototipo para demostrar la viabilidad práctica de un proyecto de Blockchain.



Basado en la reputación según historial de transacciones



Otorga a un número pequeño y designado de autores el poder de validación.

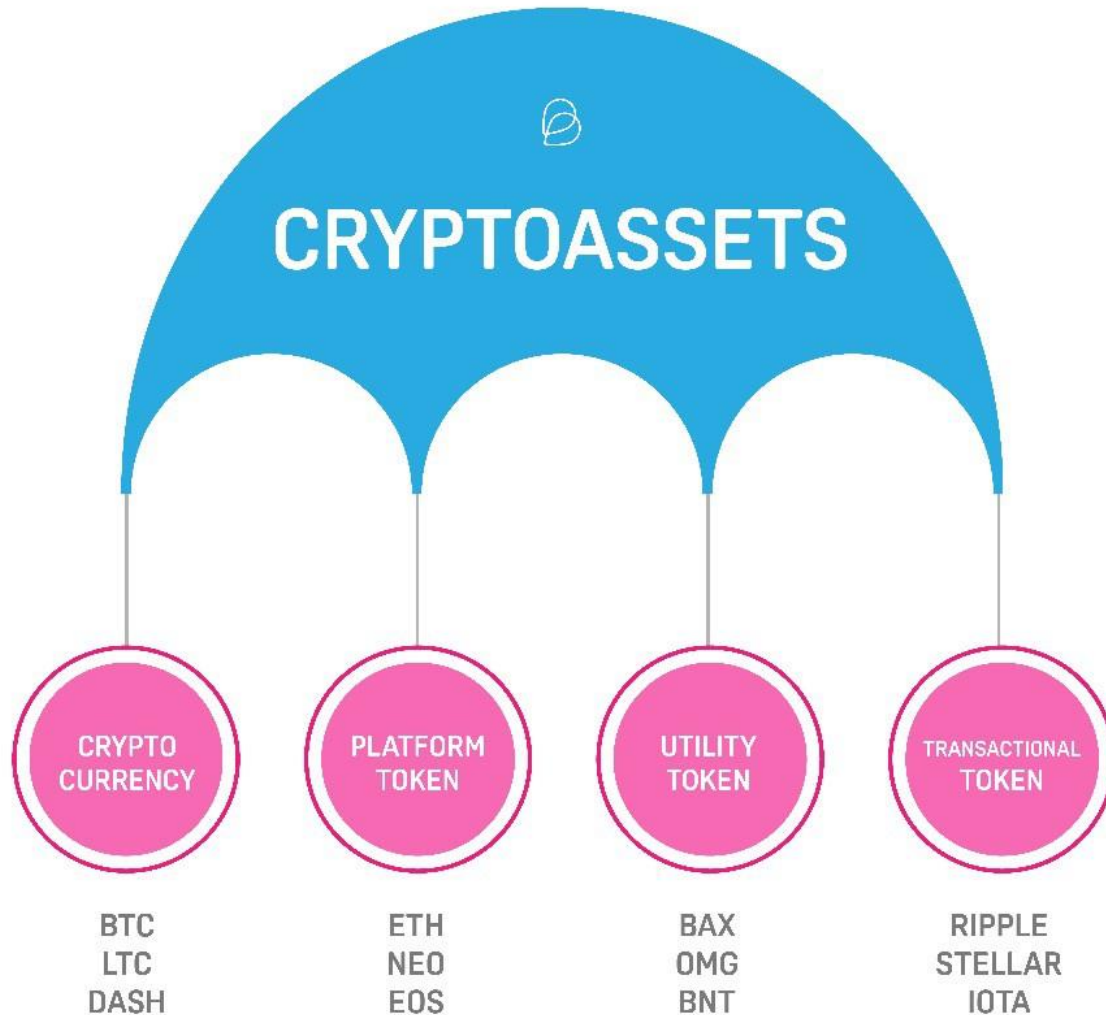


Permite a los mineros utilizar el espacio vacío en su disco duro para minar.



Es un protocolo híbrido que combina lo mejor de los mecanismos PoW y PoS

# Criptoactivos



- Se les denomina criptoactivos tanto al conjunto de criptomonedas o criptodivisas existentes en el mercado como a otras formas de bienes que utilizan la criptografía para funcionar.
- Cualquier activo puede ser digitalizado en un token.

# Diferencias entre criptomonedas y tokens

## Criptomonedas

Tienen una función específica como moneda.

Tiene su propia Blockchain.

Tiene su propio sistema de minería o consenso.

## Token

Es cualquier activo digitalizado.

Es un Smart contract sobre una blockchain ya existente.

No se puede minar.

# Tipos de tokens



Security tokens

Utility tokens

Payment tokens



Platform tokens

Governance tokens

# Categorías de Criptoactivos

- Pensadas como monedas.

Currency

- Enfocadas en resguardar privacidad y anonimato.

Private currency

- Pensadas para remuneración en redes sociales.

Social

- Apps que funcionan sobre Blockchain.

DApps

- Formas de almacenamiento en Blockchain.

Almacenamiento

- Facilitan transacciones entre dispositivos IoT.

IoT

# Lanzamiento de criptoactivos



## ICO

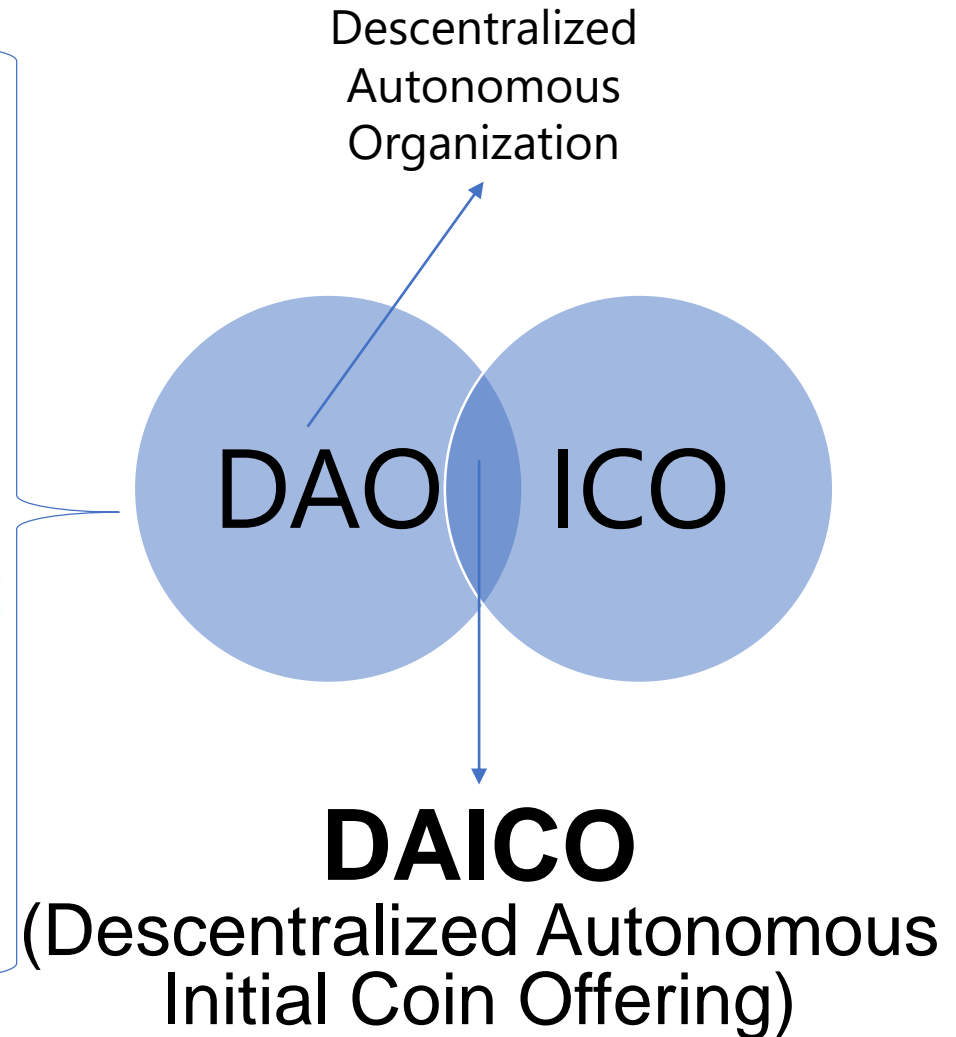
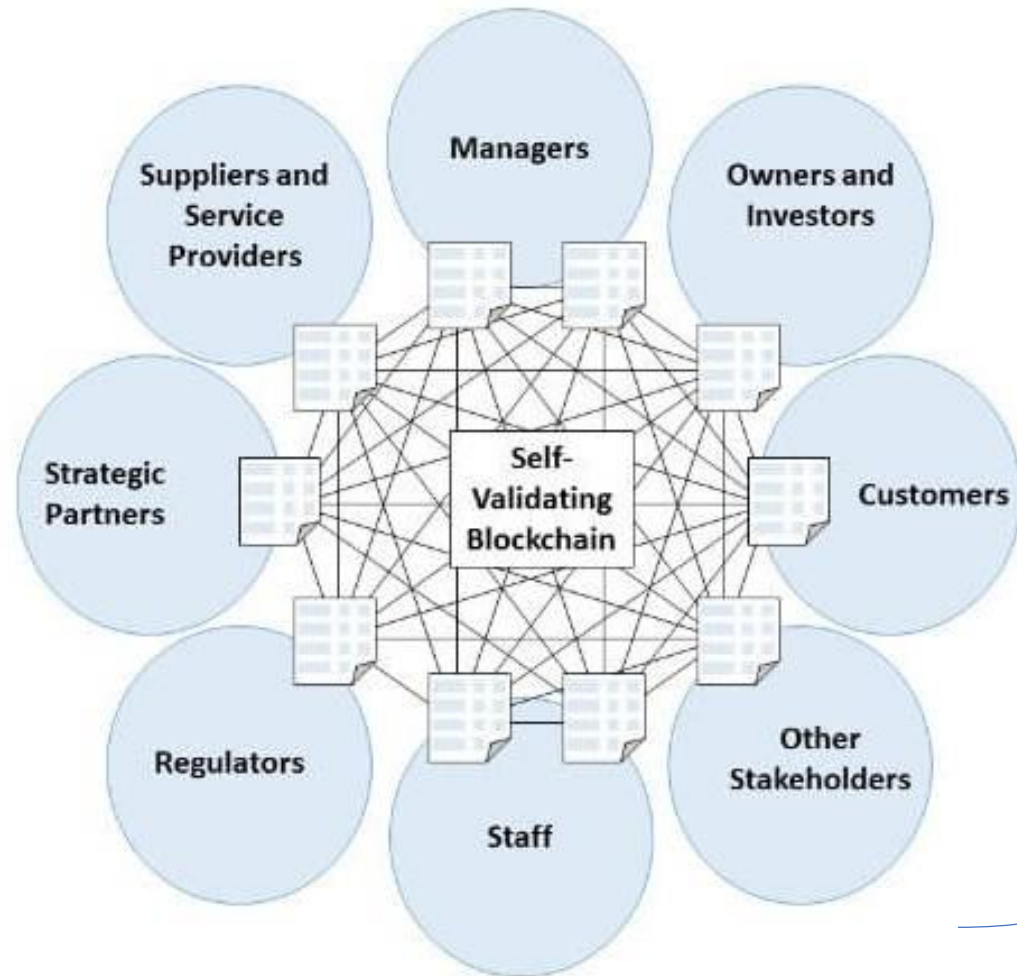
(Initial Coin Offering)

## ITO

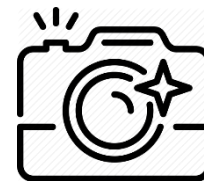
(Initial Token Offering)



# DAO y DAICO



# Bifurcaciones (forks)



Snapshot

## Hardfork

- Se crea otra moneda o token no compatible con la anterior, es otra Blockchain distinta.

## Softfork

- Cuando una red Blockchain recibe una actualización y sigue siendo compatible con la versión anterior, no se crea otro token.

Ver y buscar historial de forks: <https://forks.net/list>

# Mecanismos de publicidad:



- Pequeñas cantidades de tokens que se regalan por ser tenedor de otra

Airdrops

- Son recompensas en redes sociales o votar por una criptomoneda en un Exchange, etc..

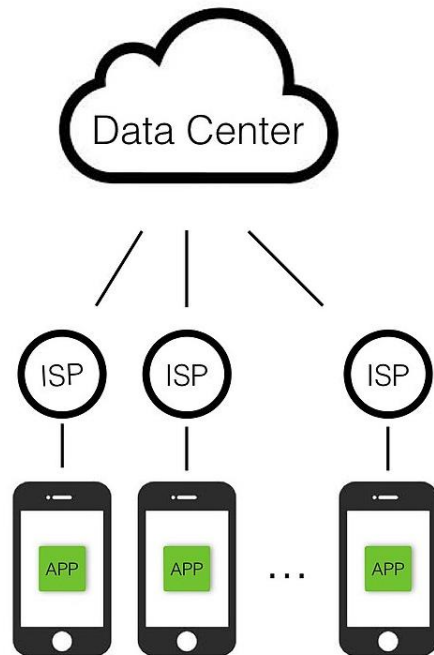
Bounties

# Otros modelos de lanzamiento

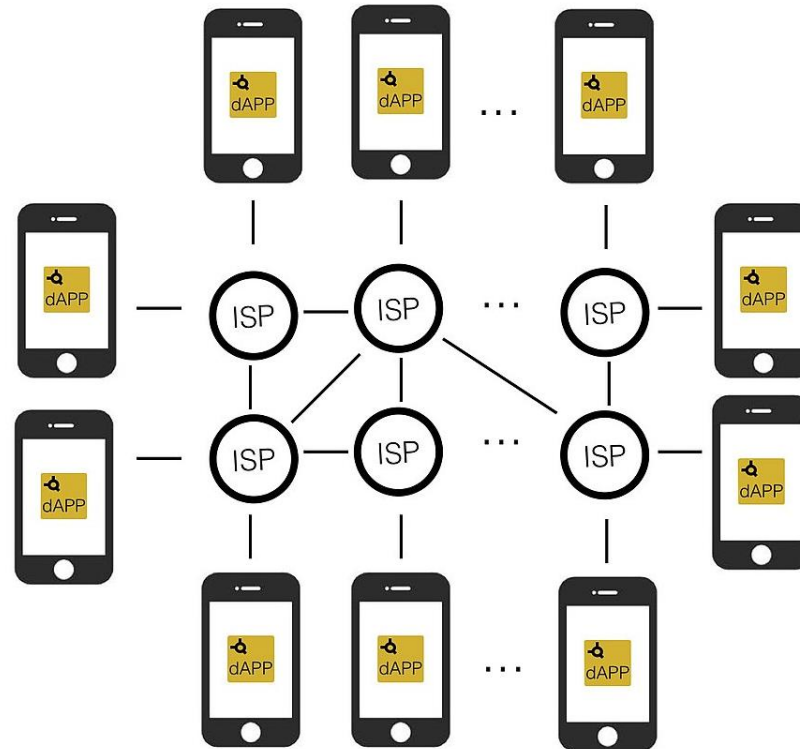


# Aplicaciones descentralizadas











Apps



DApps



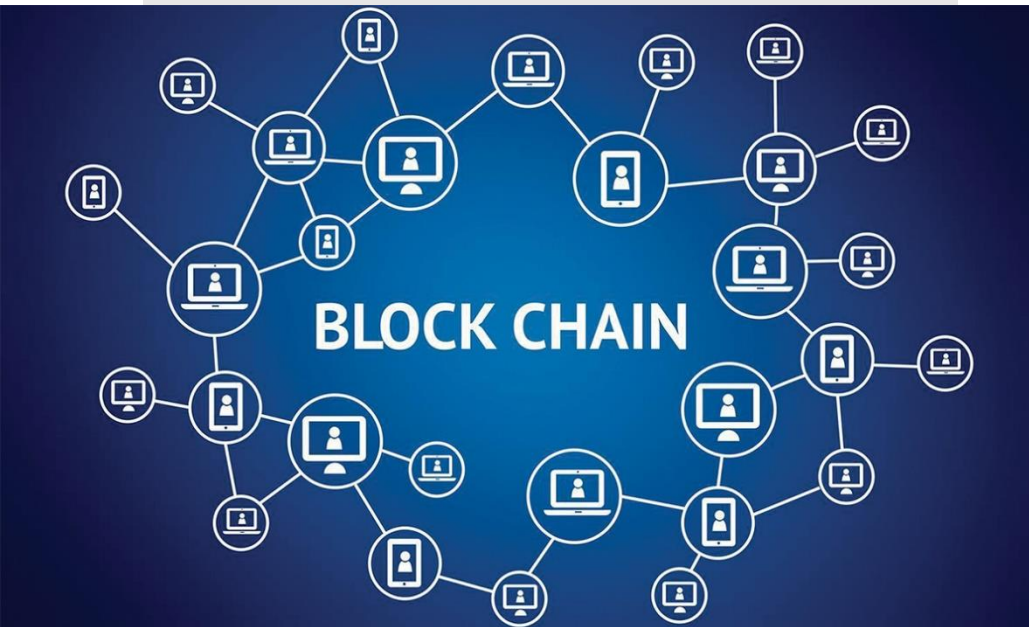
# Valuación de criptoactivos

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	
1	 Bitcoin	\$62,951,331,549	\$3,598.21	\$5,182,112,369	17,495,162 BTC	0.49%		...
2	 XRP	\$13,118,159,857	\$0.319640	\$416,488,201	41,040,405,095 XRP *	-0.30%		...
3	 Ethereum	\$12,387,007,103	\$118.53	\$2,517,774,485	104,509,311 ETH	0.78%		...
4	 EOS	\$2,179,159,673	\$2.40	\$658,759,966	906,245,118 EOS *	1.98%		...
5	 Bitcoin Cash	\$2,174,985,340	\$123.72	\$208,066,110	17,580,300 BCH	0.65%		...

*Capitalización de mercado = monedas en circulación × precio actual de mercado*

$$MVRV = \frac{\text{Capitalización de mercado}}{\text{Capitalización realizada}}$$

# Conclusiones.



- Blockchain es un tipo de tecnología DLT que combina criptografía para crear un libro mayor distribuido seguro, confiable y transparente, que puede tener muchas aplicaciones siendo la arquitectura adyacentes de las criptomonedas su uso más conocido.

# Conclusiones.



1. Bitcoin es la primer y principal criptomoneda, también están Ether, XRP, Litecoin, Bitcoin Cash conocidas como altcoins.
2. Para solucionar la volatilidad en los precios surgen los modelos de stablecoins.
3. Para tranzar con ellas se necesita usar los Exchanges y tener una crypto wallet.
4. El proceso de minería permite crearlas y validar las transacciones realizadas mediante métodos de consenso como PoW y PoS, entre otros.



# Conclusiones.



1. Un criptoactivo es cualquier token digital que funciona mediante criptografía para representar un activo del mundo real.
2. Existen tokens de pagos, seguridad, plataforma, utilidad y gobernanza.
3. Los principales mecanismos para su lanzamiento son ICO, ITO y DAICO.



# Maestría en Finanzas

FI-75301 Macrodatos y Fintech.

M.Sc. Walter Jeremías López.



# ¡Gracias por su atención!

¿Preguntas o comentarios?