

Sistemas Operativos y Distribuidos

Iren Lorenzo Fonseca
iren.fonseca@.ua.es

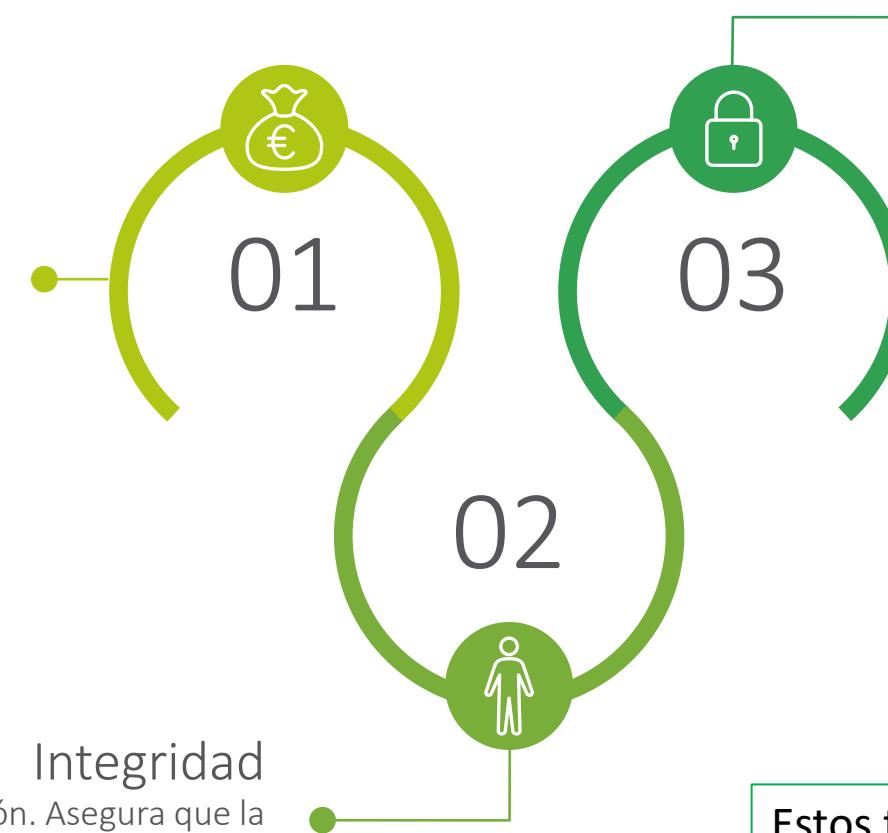


TEMA 3. Sistemas Distribuidos.

Seguridad en Sistemas
Distribuidos

Seguridad en Sistemas Distribuidos

Confidencialidad
Protección de la información contra accesos no autorizados. Es decir, solo las personas o entidades autorizadas deben poder acceder a la información.



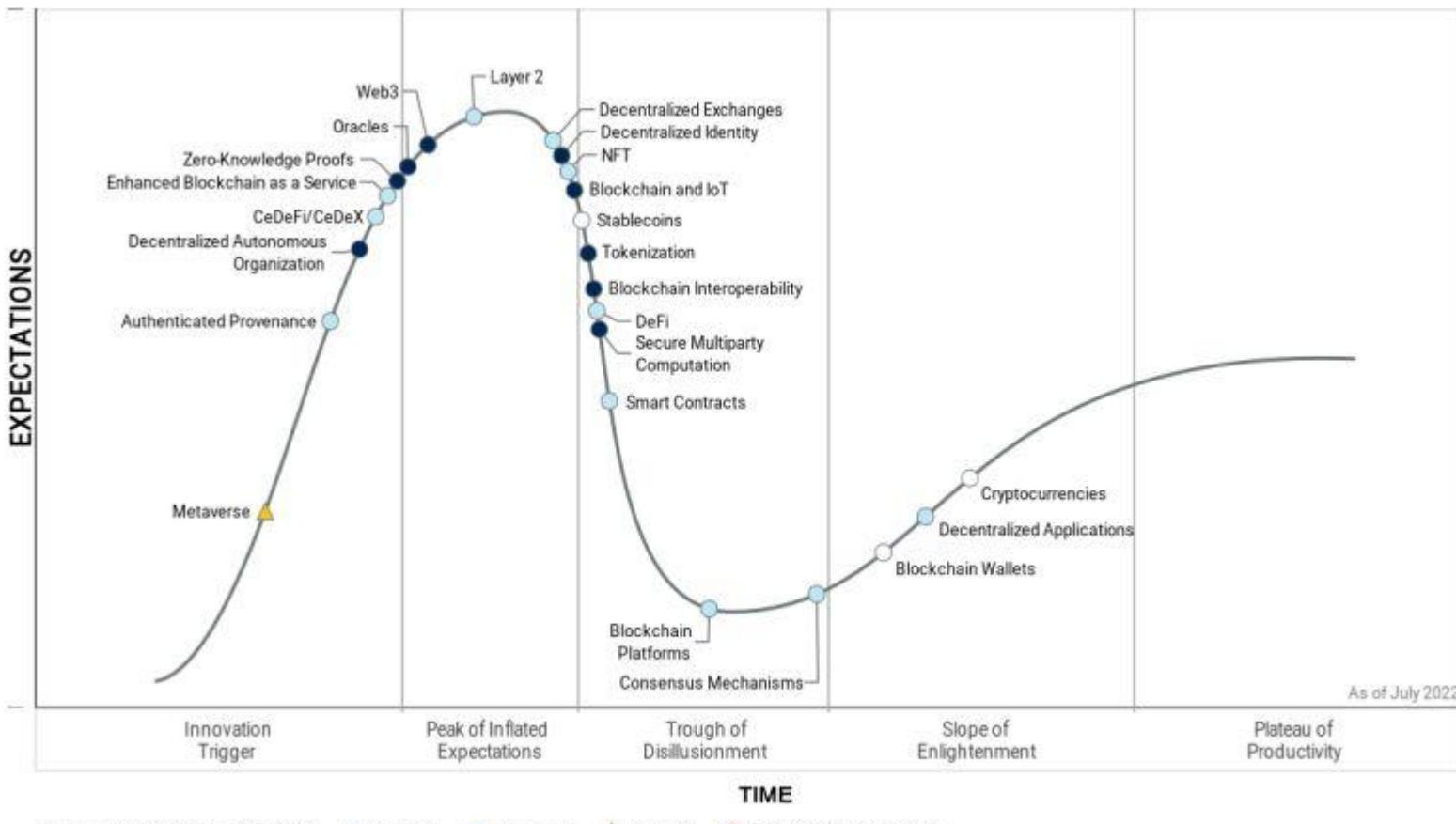
Integridad
Exactitud y completitud de la información. Asegura que la información no haya sido alterada de manera no autorizada y que cualquier modificación sea realizada solo por personas autorizadas.

Disponibilidad
Asegura que la información y los recursos están accesibles y utilizables por los usuarios autorizados cuando sea necesario

Estos tres principios están interrelacionados y son esenciales para un enfoque integral de la seguridad de la información. La falta de cualquiera de estos elementos puede comprometer la seguridad global del sistema

Seguridad en Sistemas Distribuidos

Gartner blockchain, web3 hype cycle 2022



Blockchain
La tecnología detrás del Bitcoin

Fuente: Gartner

Introducción

Requerimientos de Bitcoin

- | No depender de **terceros**
- | La moneda digital debe ser **única** y **no** debe poder **duplicarse**
- | Las **transacciones** realizadas con esta moneda y mediante este sistema **no** deben poder **alterarse**
- | Poseer un **mecanismo** para involucrar, **motivar** y compensar a la **comunidad** de forma que **proporcione** los **recursos** que precisa la red de blockchain
- | La moneda debe tener **valor**
- | Debe ser **sencillo** poder realizar **transacciones** comerciales con esta moneda y ser capaz de **adaptarse** al **entorno cambiante**
- | Las **transacciones** deben estar **libres de comisiones** o, al menos, que sean lo más **reducidas** posible

Definición de Bitcoin

El término hace referencia a dos elementos:

01 Una **divisa electrónica**, criptomoneda o moneda digital [**bitcoin**]

02 Un **sistema de pago electrónico** [**Bitcoin Core**]



Definición de la divisa electrónica

Bitcoin Core

Problema: se requiere que no se pueda falsificar: evitar el problema del “doble gasto”

Solución: la divisa se representa como un apunte de cada operación:
lista de transacciones

Ordenante	Beneficiario	Cantidad
Juan	José	10 ₿
José	María	6 ₿
María	Ana	2 ₿

* **No precisa un TOKEN especial**

→ No puede duplicarse. El saldo se calcula sobre todas las operaciones



Definición de la divisa electrónica

Bitcoin

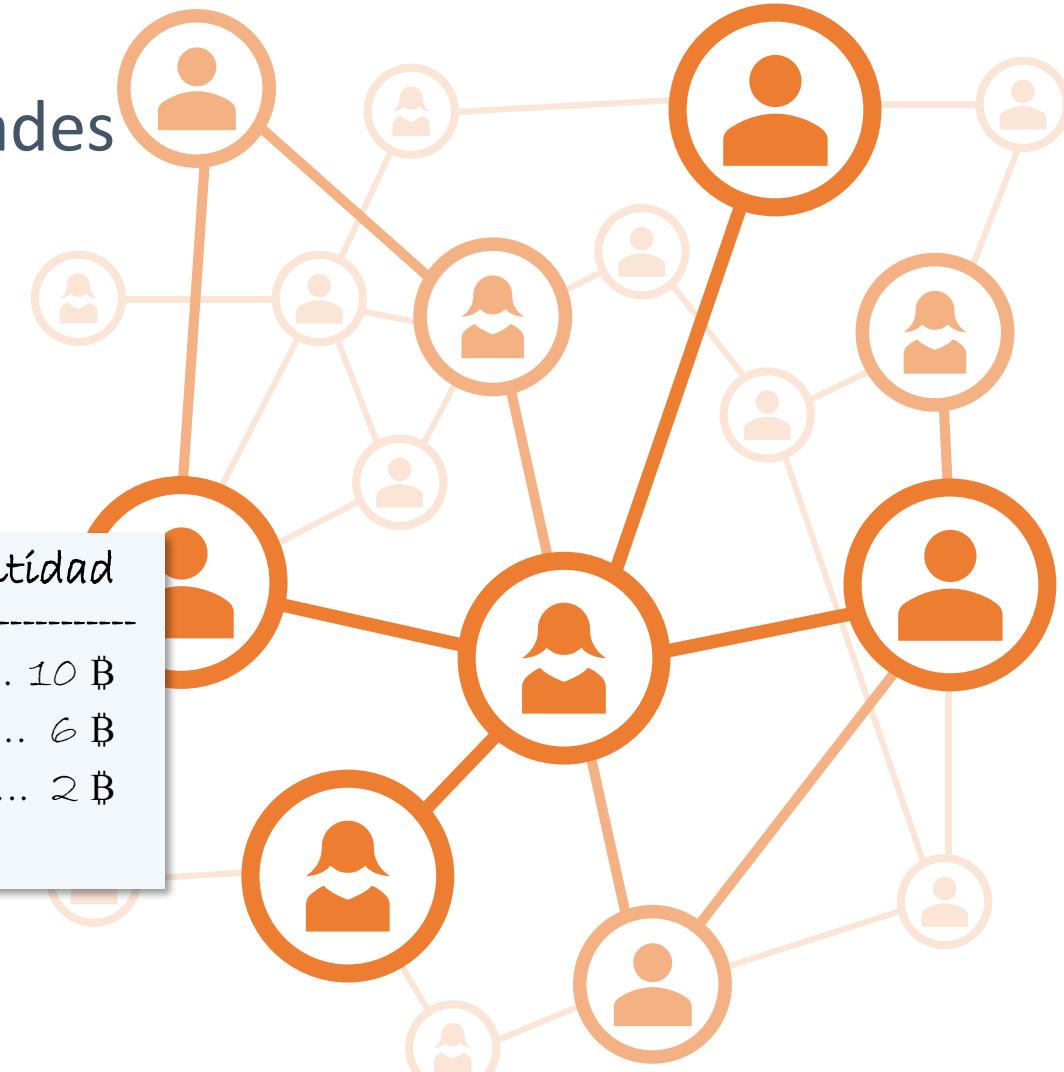
Problema: se requiere que no exista dependencia de terceros (bancos, entidades financieras, sistemas de pago, ...)

Solución:

- 01 Que exista un único registro de transacciones
- 02 Que este registro lo tengan todos los participantes

Red
Peer

Ordenante	Beneficiario	Cantidad
Juan	José	10 ₿
José	María	6 ₿
María	Ana	2 ₿



Red P2P



Red P2P



Red P2P



Red P2P



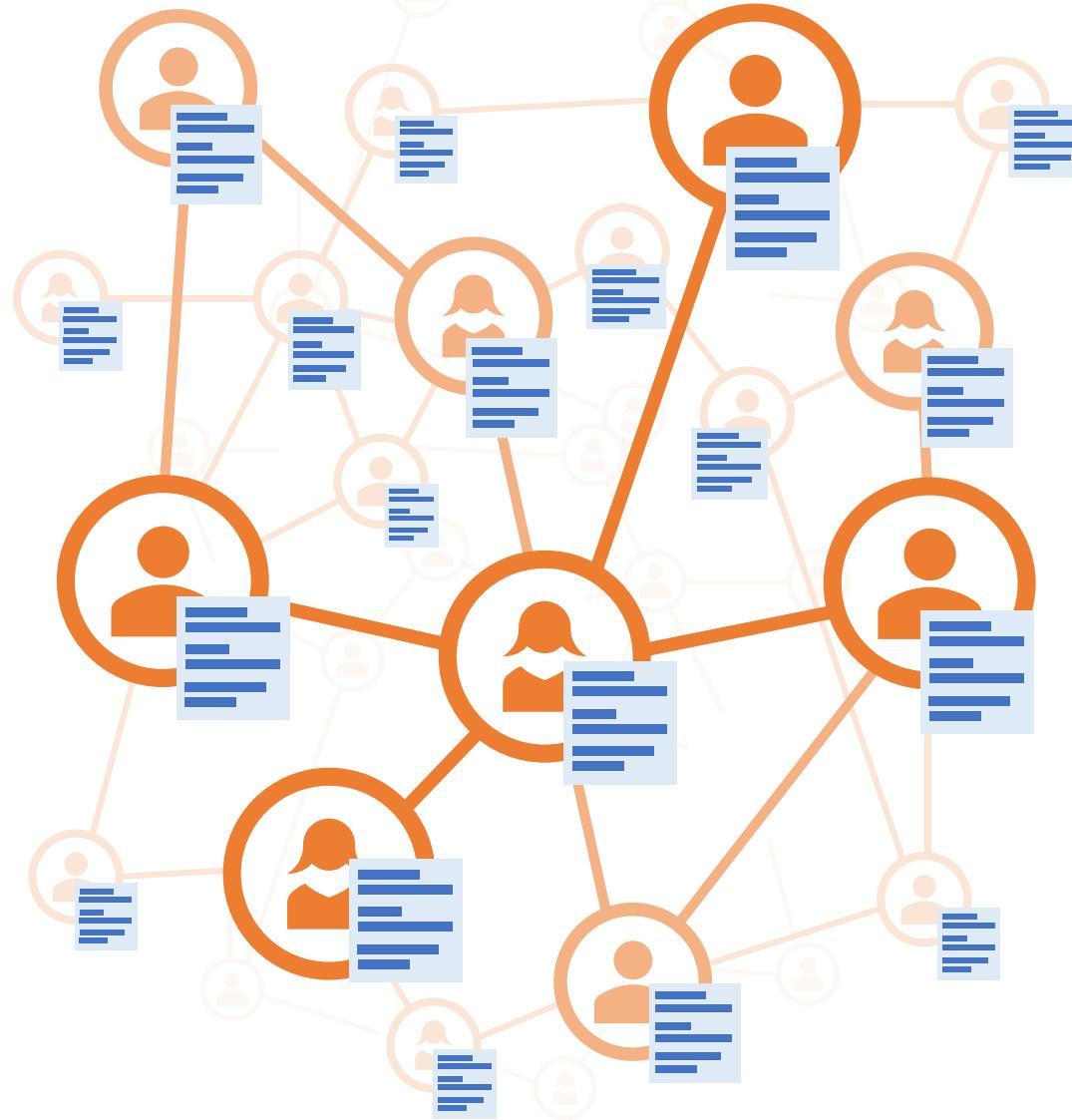
Red P2P



Red P2P



Red P2P



Cadena de Bloques (Blockchain)

Registro único de transacciones

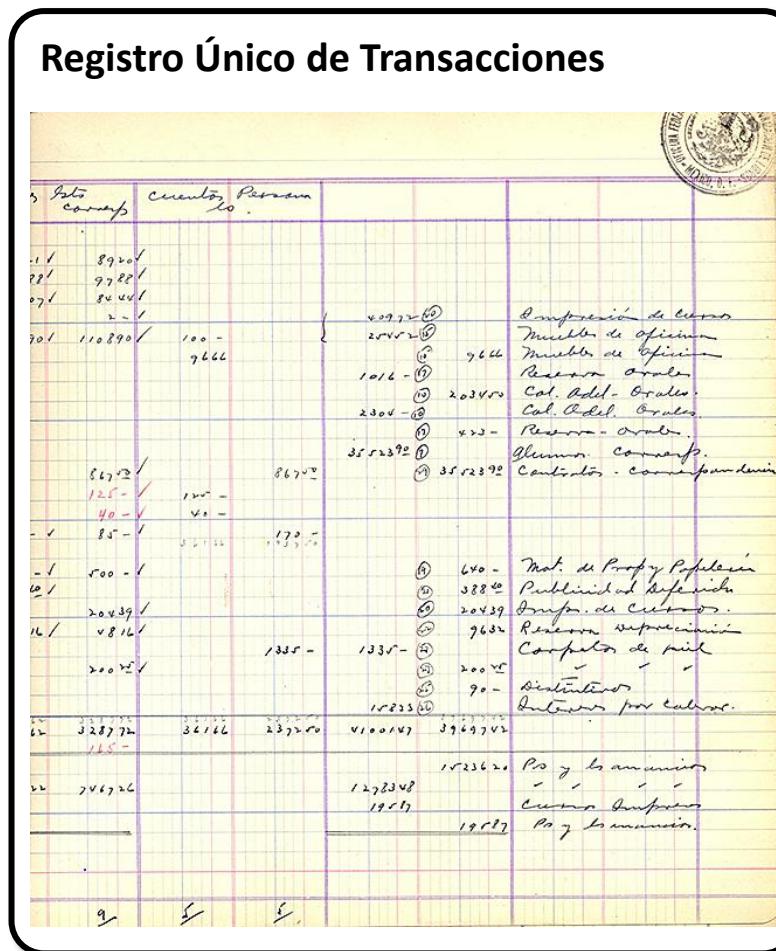
Libro Diario Contable

Dato corriente		Cuentas	Pasadas	
1/	89207			
2/	77887			
3/	70447			
4/	2 -			
5/	1108907	100 -	4297267	Comisión de leyes
		9666	2034520	Muebles de oficina
			9644	Muebles de oficina
			1016 -	Reserva - orales
			2304 -	Cal. Adel. - orales.
			3552392	Cal. Adel. - orales.
			3552392	Reserva - orales.
			3552392	Gastos corrientes.
			3552392	Contáctos - corriente
	86747		86747	
	125 -	100 -	600 -	
	40 -	40 -	38840	Mati. de Propy. y Pelecin.
	85 -	85 -	20439	Publicidad Referencia
	500 -	500 -	9638	Difus. de Cursos.
	20439		10233	Reserva depreciación
	8816		600 -	Cartelería de public.
	20027	1335 -	1335 -	
			90 -	Sindicatos
			10233	Interven. por tributos.
	328772	32166	237250	
	115 -		4100187	Ps y tramitaciones
	786726		1278348	
			19517	
			19517	Cuenta Comisión
			19517	Ps y tramitaciones.

Blockchain

Cadena de Bloques (Blockchain)

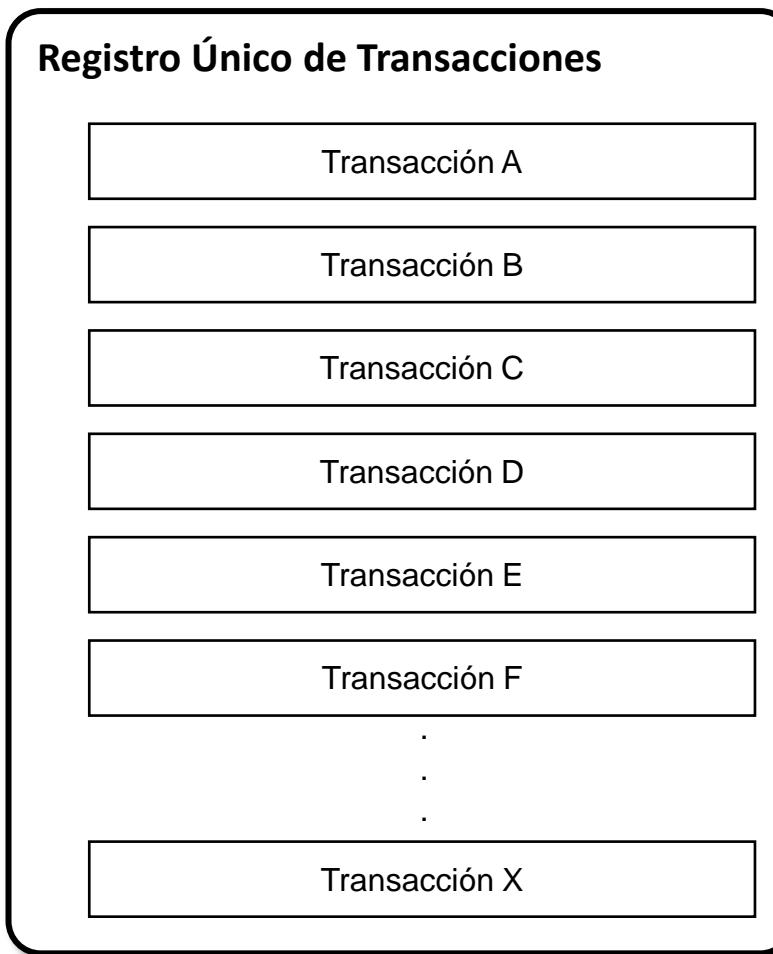
Registro único de transacciones



Blockchain

Cadena de Bloques (Blockchain)

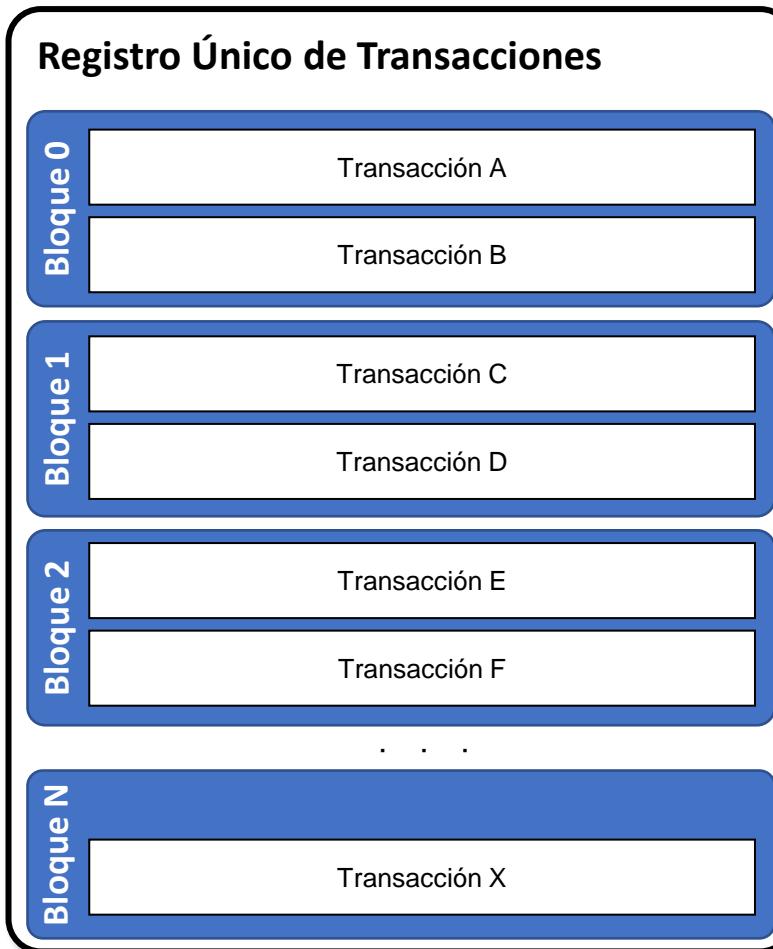
Registro único de transacciones



Blockchain

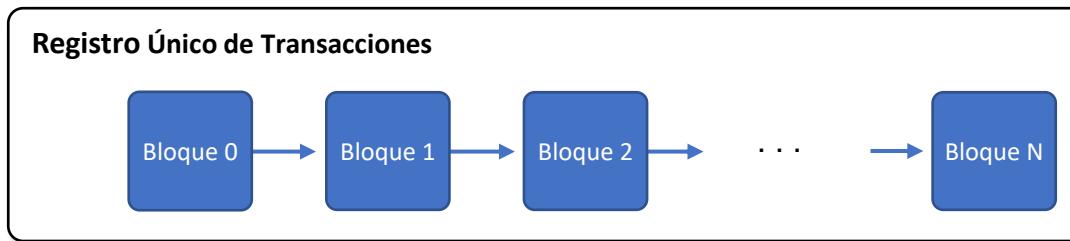
Cadena de Bloques (Blockchain)

Lista de bloques



Cadena de Bloques (Blockchain)

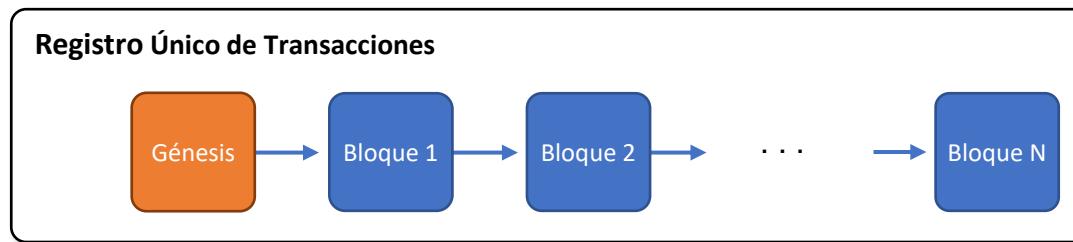
Lista de bloques



Blockchain

Cadena de Bloques (Blockchain)

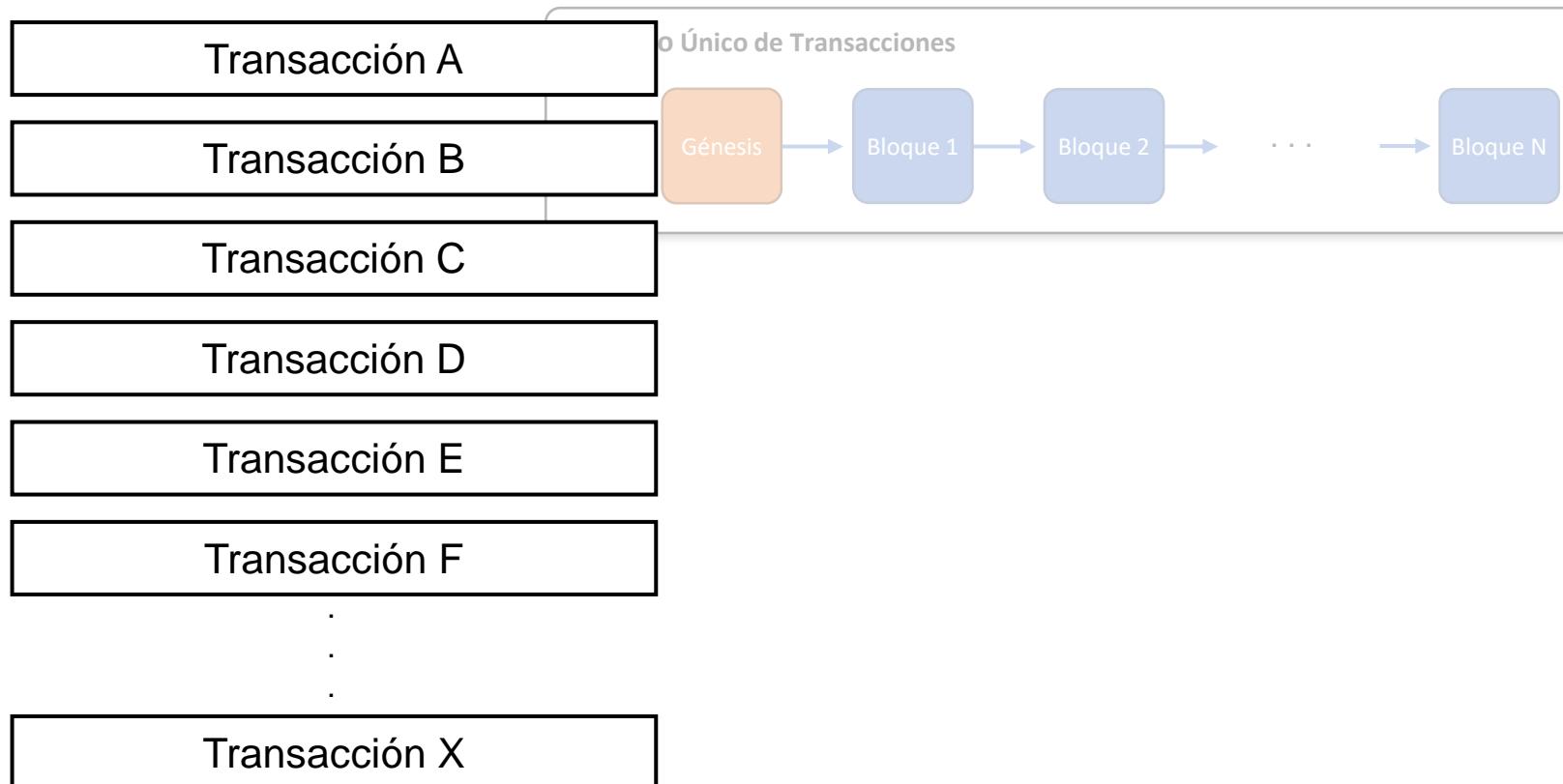
Bloque génesis



Ordenante	Beneficiario	Cantidad
<hr/>		
	Juan	50 ₩
Juan	José	10 ₩
José	María	6 ₩
María	Ana	2 ₩

Cadena de Bloques (Blockchain)

Nuevo bloque ($n+1$)

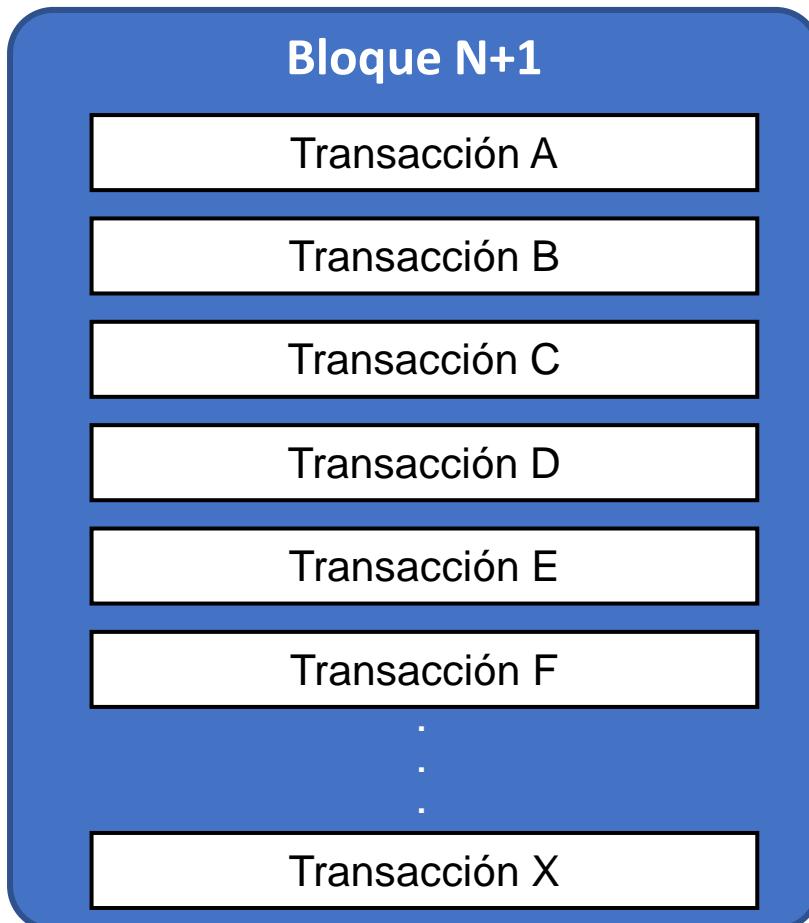


Blockchain



Cadena de Bloques (Blockchain)

Nuevo bloque (n+1)



co de Transacciones

esis

Bloque
Bloque 1 → ... → Bloque N

01

01 Bloque Bitcoin de transacciones

- 1.56 MB de tamaño máximo
- Entre 1.000 y 6.200 transacciones x bloque
- Cada minero va montando bloques a partir de las transacciones pendientes
- Cada transacción debe verificarse previamente



Cadena de Bloques (Blockchain)

Nuevo bloque (n+1)



Cadena de Transacciones

esis

Bloque 1 → Bloque 2 → ... → Bloque N

02

Transacción Coinbase

| Recompensa por minar + comisiones

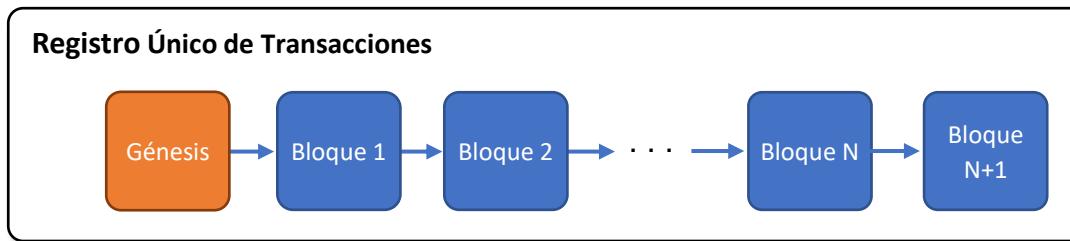
| Inicialmente 50 BTC (actualmente 3,125 BTC)

| Halving: reducción a la mitad cada 210.000 bloques (cada 4 años aproximadamente)

| Sobre 2140 se minará el último BTC de un total de 21 millones BTC

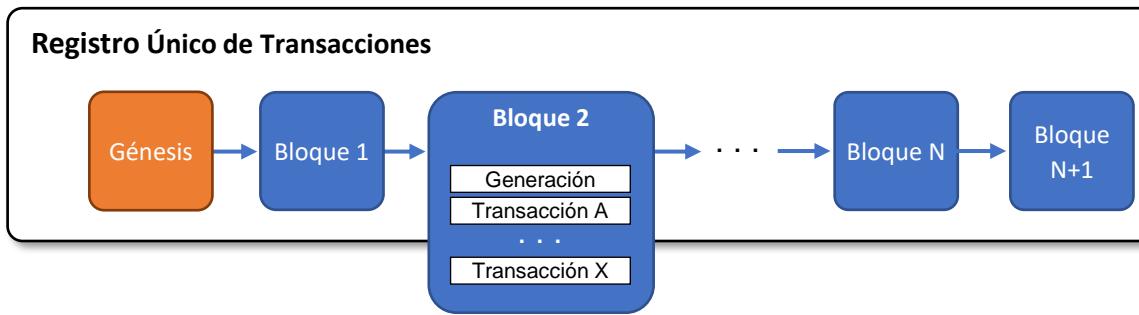
Cadena de Bloques (Blockchain)

Nuevo bloque (n+1)



Cadena de Bloques (Blockchain)

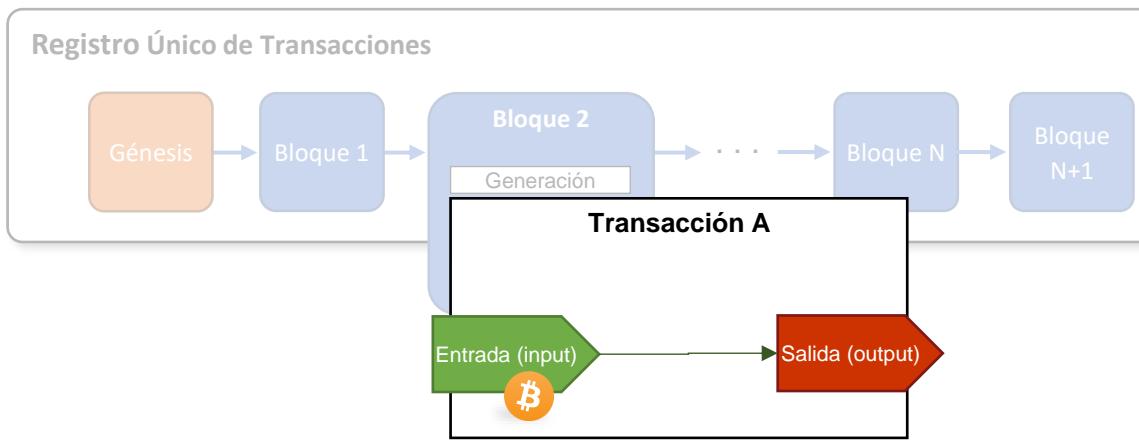
Transacciones Tx



Blockchain

Cadena de Bloques (Blockchain)

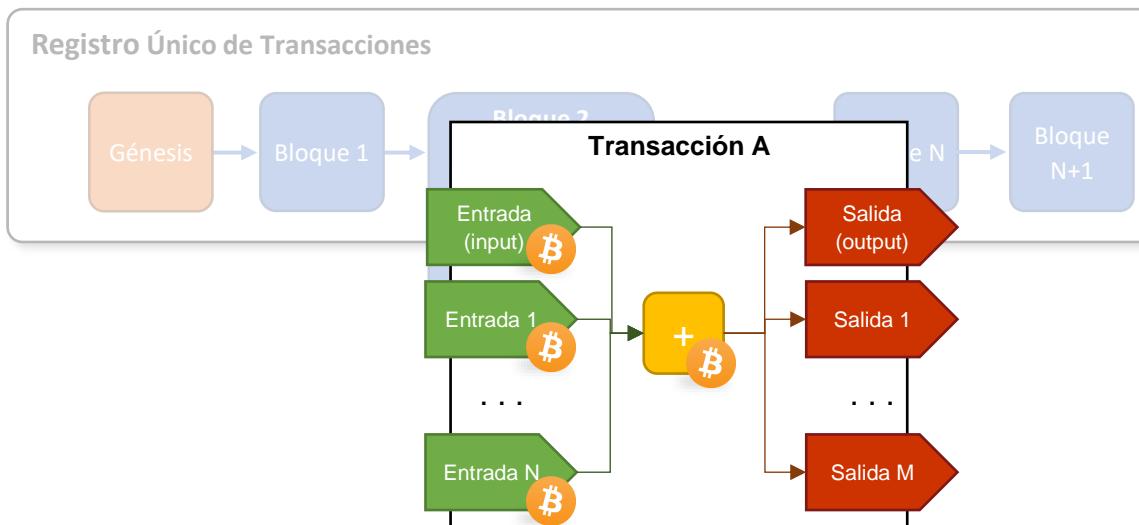
Transacciones Tx



$1 \text{ BTC} (\text{bitcoin}) == 100.000.000 \text{ satoshi}$
 $1 \text{ satoshi} = 1/100.000.000 \text{ BTC} = 0,00000001 \text{ BTC}$

Cadena de Bloques (Blockchain)

Transacciones Tx

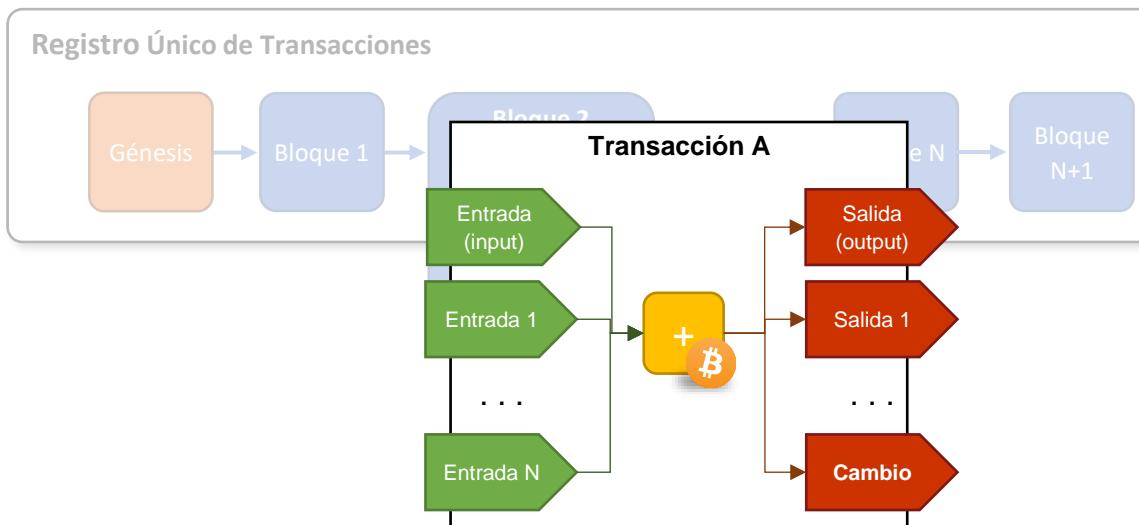


$$\sum_{i=0}^N Input_i$$

Blockchain

Cadena de Bloques (Blockchain)

Transacciones Tx



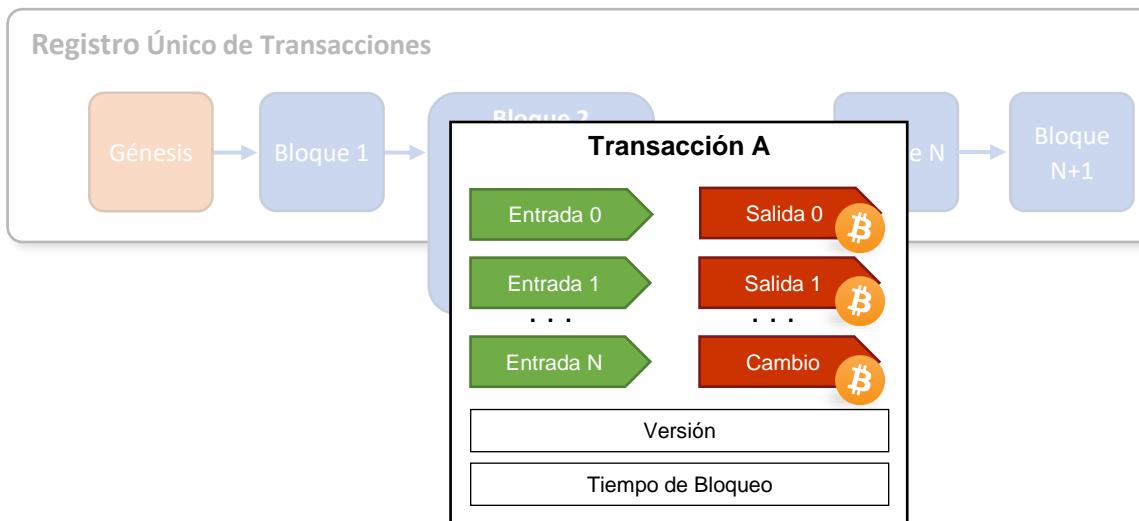
$$\sum_{i=0}^N Input_i \geq \sum_{j=0}^M Output_j$$

$$\sum_{i=0}^N Input_i - \sum_{j=0}^M Output_j = \text{Comisión}$$

Blockchain

Cadena de Bloques (Blockchain)

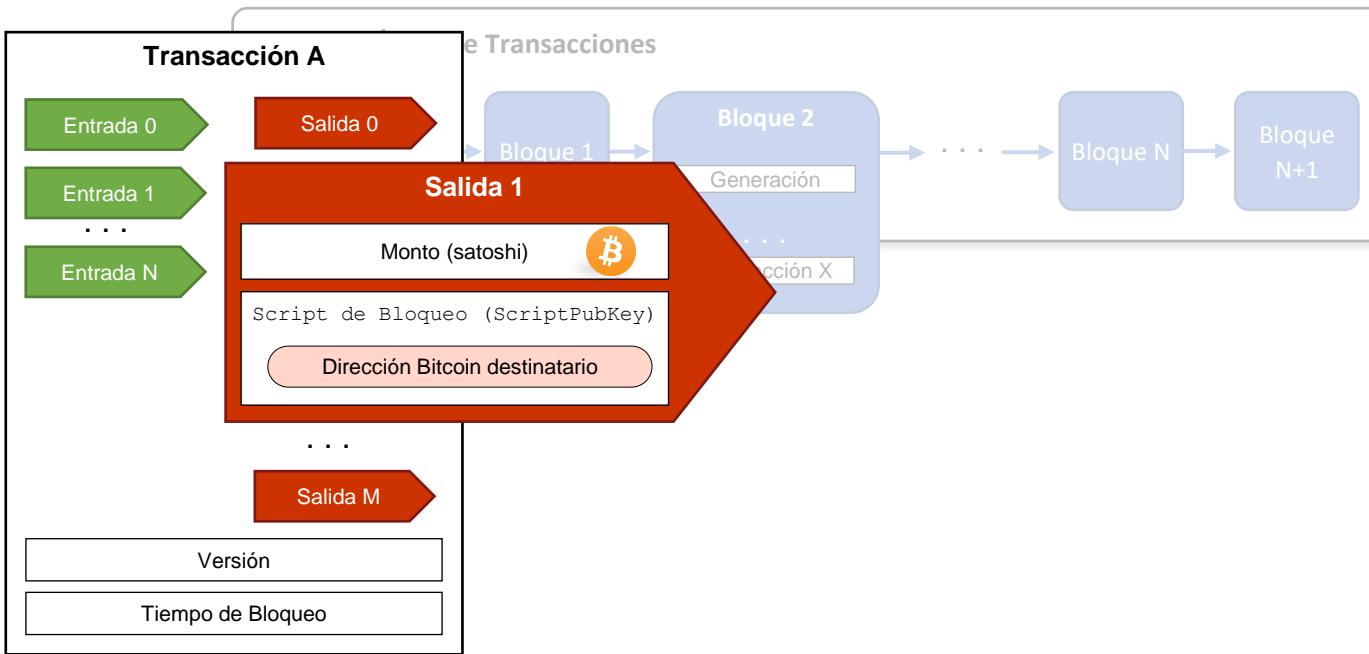
Transacciones Tx



Blockchain

Cadena de Bloques (Blockchain)

Transacciones Tx



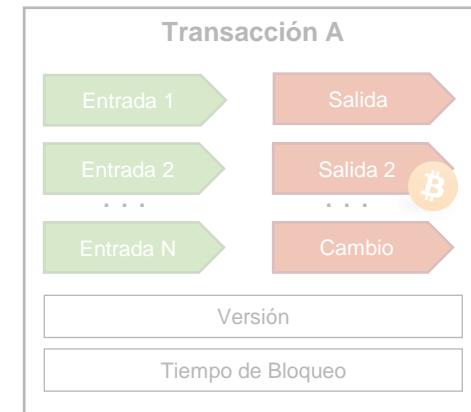
Blockchain

Criptografía básica para blockchain

01 Función Hash

02 Función Hash Criptográfica

03 Criptografía Asimétrica



Criptografía básica para blockchain

Función Hash y Hash Criptográfica

01 Función Hash

Comprime una cadena de entrada en otra de tamaño fijo

Texto entrada (p.ej.: Transacciones):	Juan	José	10 ₿
	José	María	6 ₿
	María	Ana	2 ₿

Texto salida (Hash): 

02 Función Hash Criptográfica (SHA-256 y RIPEMD-160)

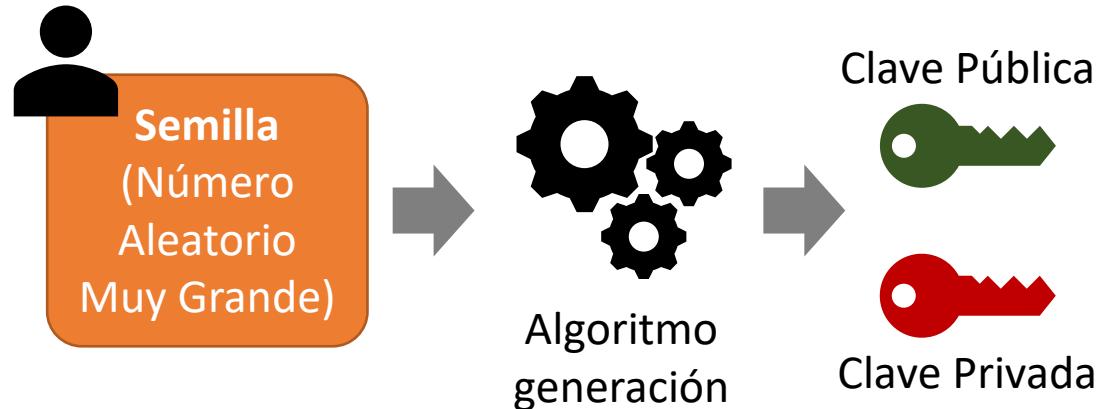
Hash útiles para criptografía → fácil calcular hash, muy difícil deducir la fuente

Criptografía básica para blockchain

Criptografía Asimétrica

03 Criptografía Asimétrica

Utiliza un par de claves para encriptar y desencriptar una información



Principalmente lo utilizamos para :
03A Cifrado de clave pública

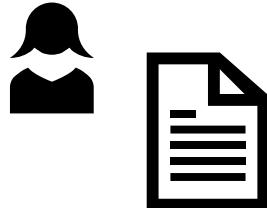
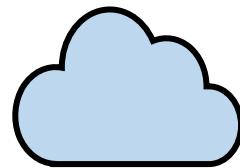
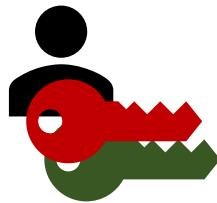
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



Juan tiene una clave privada y su correspondiente clave pública

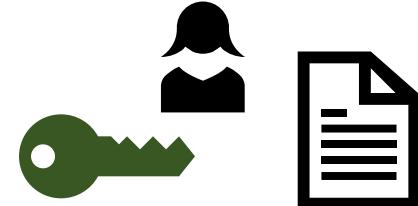
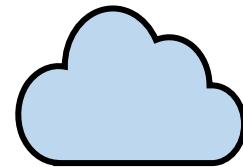
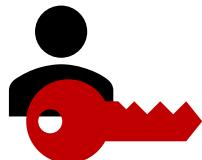
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



Juan envía su clave pública a María

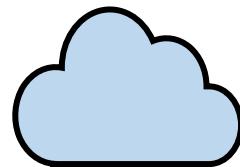
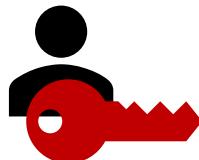
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



... es como enviar un sobre abierto, con cerradura

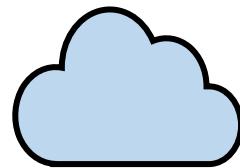
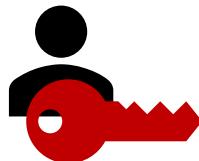
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



María mete el mensaje o el archivo (o los datos en general) dentro del sobre abierto

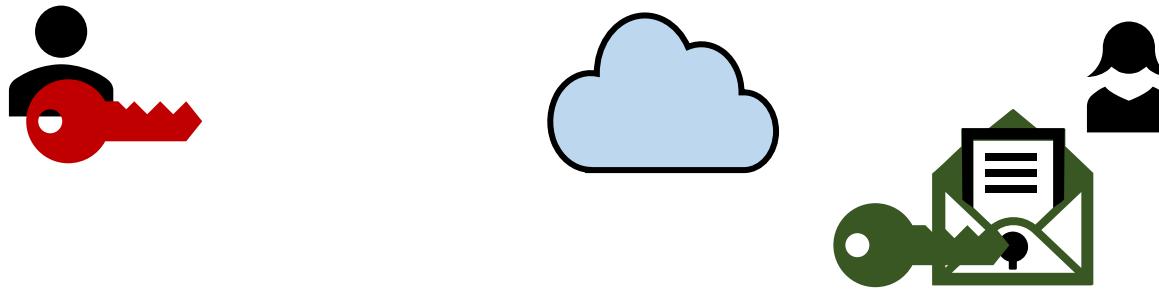
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



María cierra (**encripta**) el sobre con la clave pública de Juan

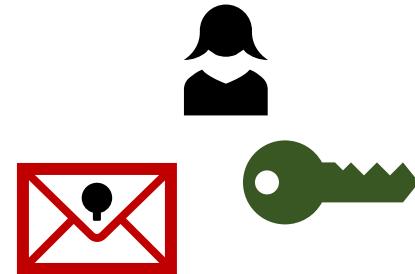
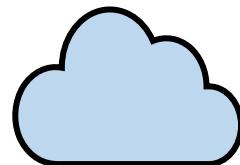
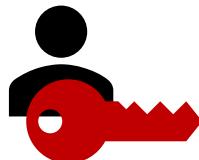
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



María ya no podrá abrir (**desencriptar**) nuevamente el sobre !!!

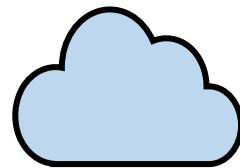
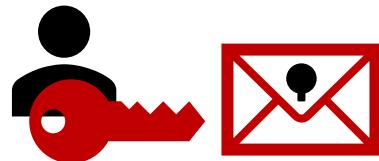
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



María envía la información encriptada y Juan recibe el sobre cerrado

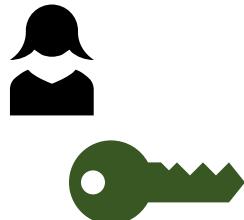
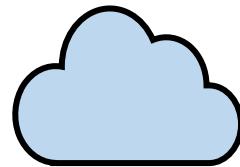
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



Juan puede abrir (**desencriptar**) el sobre porque tiene la clave privada

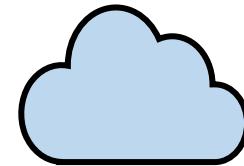
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



El sobre solo pudo abrirse (**desencriptarse**) con la clave privada asociada
a la clave pública con la que se cerró (**encriptó**)

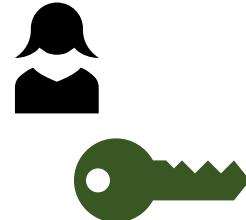
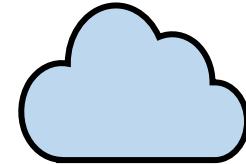
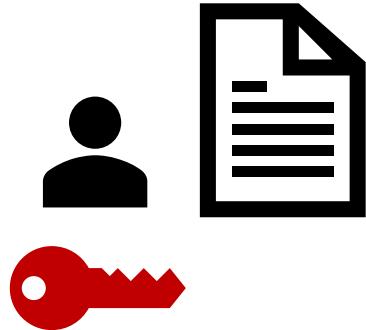
Criptografía básica para blockchain

Criptografía Asimétrica

03ACifrado de clave pública

Utiliza la clave pública para cifrar un mensaje:

María desea enviar un archivo que sólo pueda ver Juan.



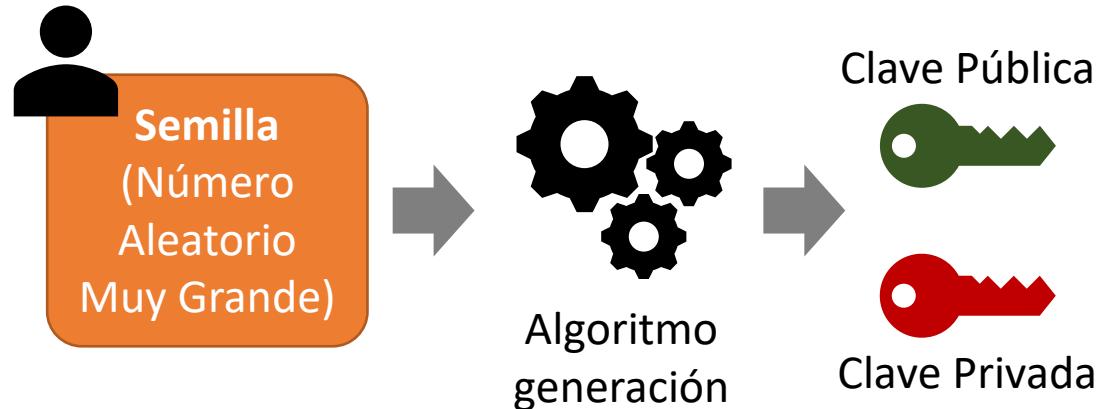
Juan puede acceder al mensaje cifrado

Criptografía básica para blockchain

Criptografía Asimétrica

03 Criptografía Asimétrica

Utiliza un par de claves para encriptar y desencriptar una información



Principalmente lo utilizamos para :

03A Cifrado de clave pública

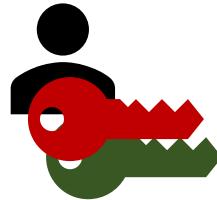
03B Firma digital

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- | Utiliza la clave privada para firmar un hash del mensaje



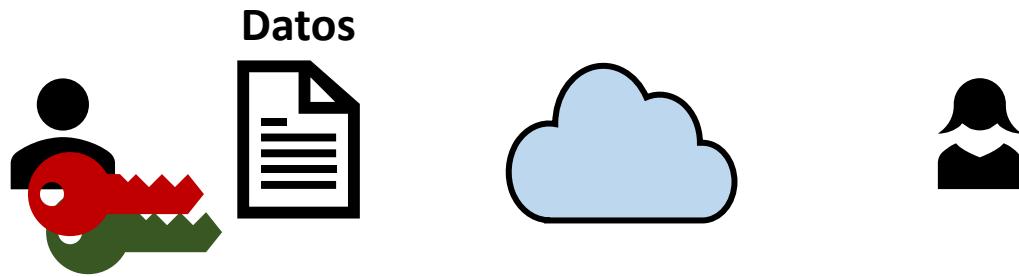
Juan posee una clave privada y su correspondiente clave pública

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- | Utiliza la clave privada para firmar un hash del mensaje



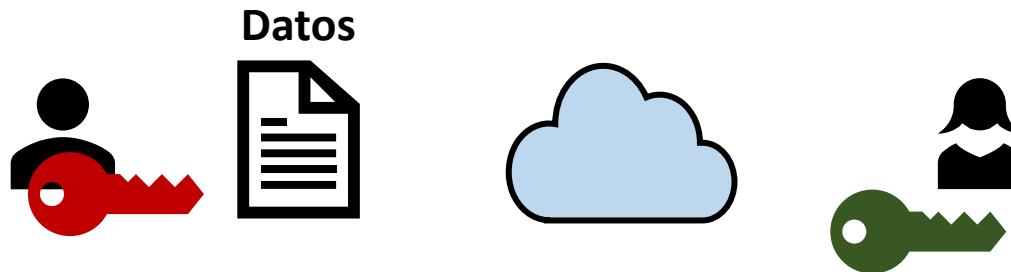
Juan desea enviar un mensaje a María de forma que ella pueda saber si lo envió él

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- | Utiliza la clave privada para firmar un hash del mensaje



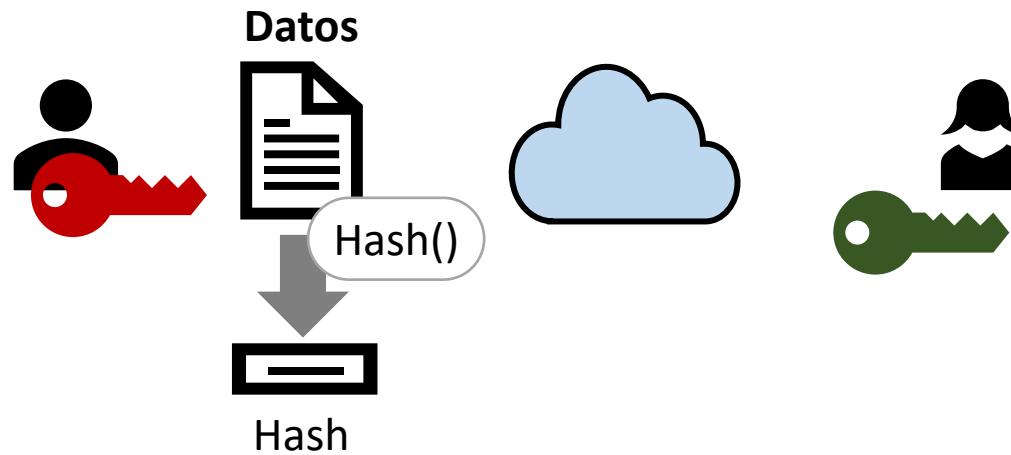
Para que María se asegure de que el emisor es Juan, este le envía su clave pública

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- Utiliza la clave privada para firmar un hash del mensaje



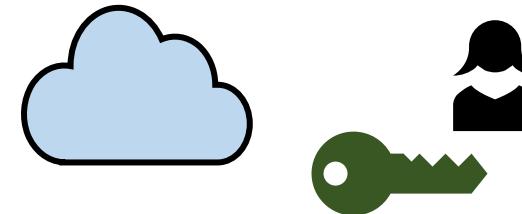
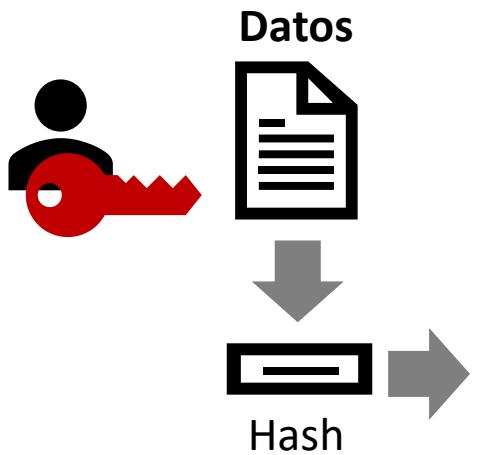
Juan calcula un hash de su mensaje

Criptografía básica para blockchain

Criptografía Asimétrica

03BFirma digital

- Utiliza la clave privada para firmar un hash del mensaje



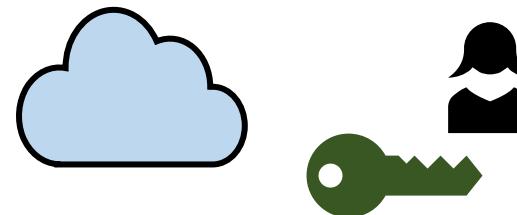
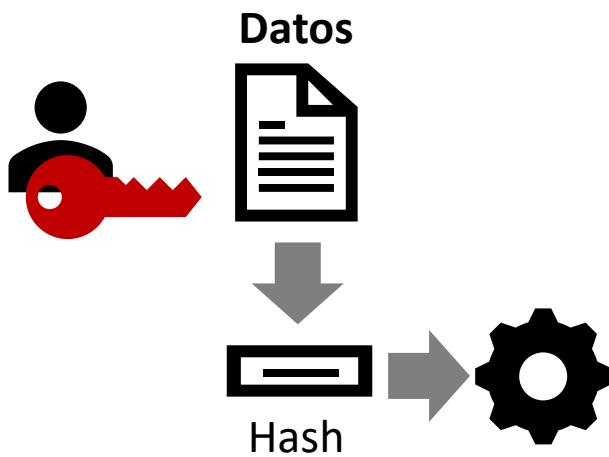
Juan calcula un hash de su mensaje

Criptografía básica para blockchain

Criptografía Asimétrica

03BFirma digital

- | Utiliza la clave privada para firmar un hash del mensaje



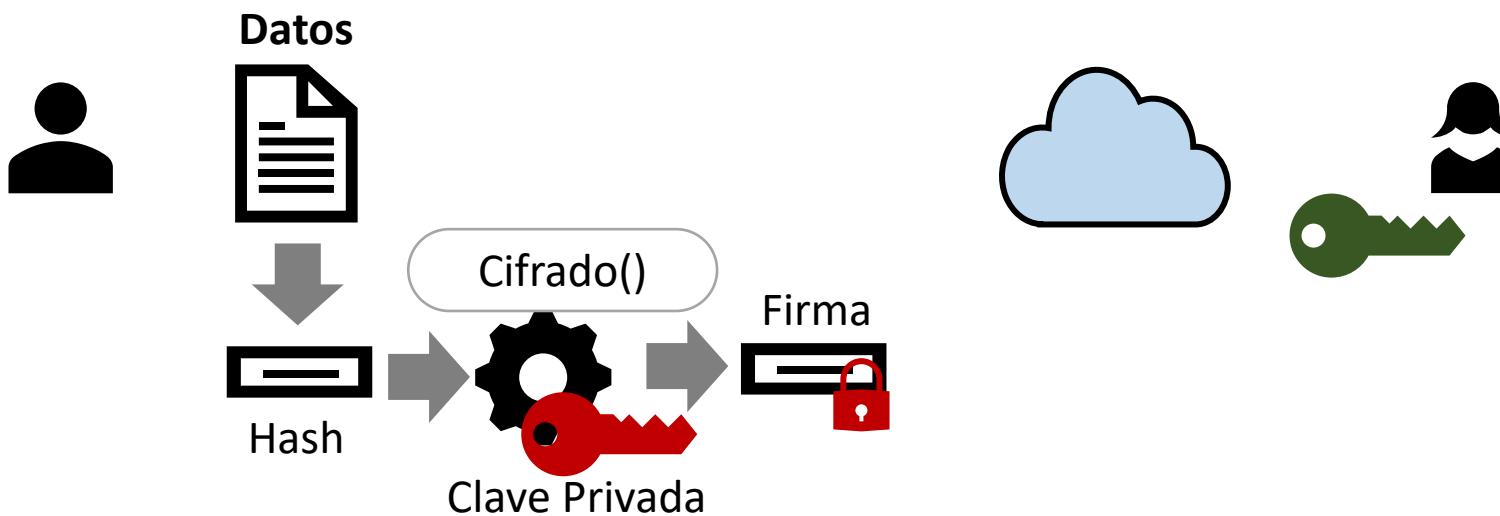
Y utiliza su clave privada para cifrarlo

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

| Utiliza la clave privada para firmar un hash del mensaje



Obteniendo una firma digital mediante su clave privada

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- | Utiliza la clave privada para firmar un hash del mensaje



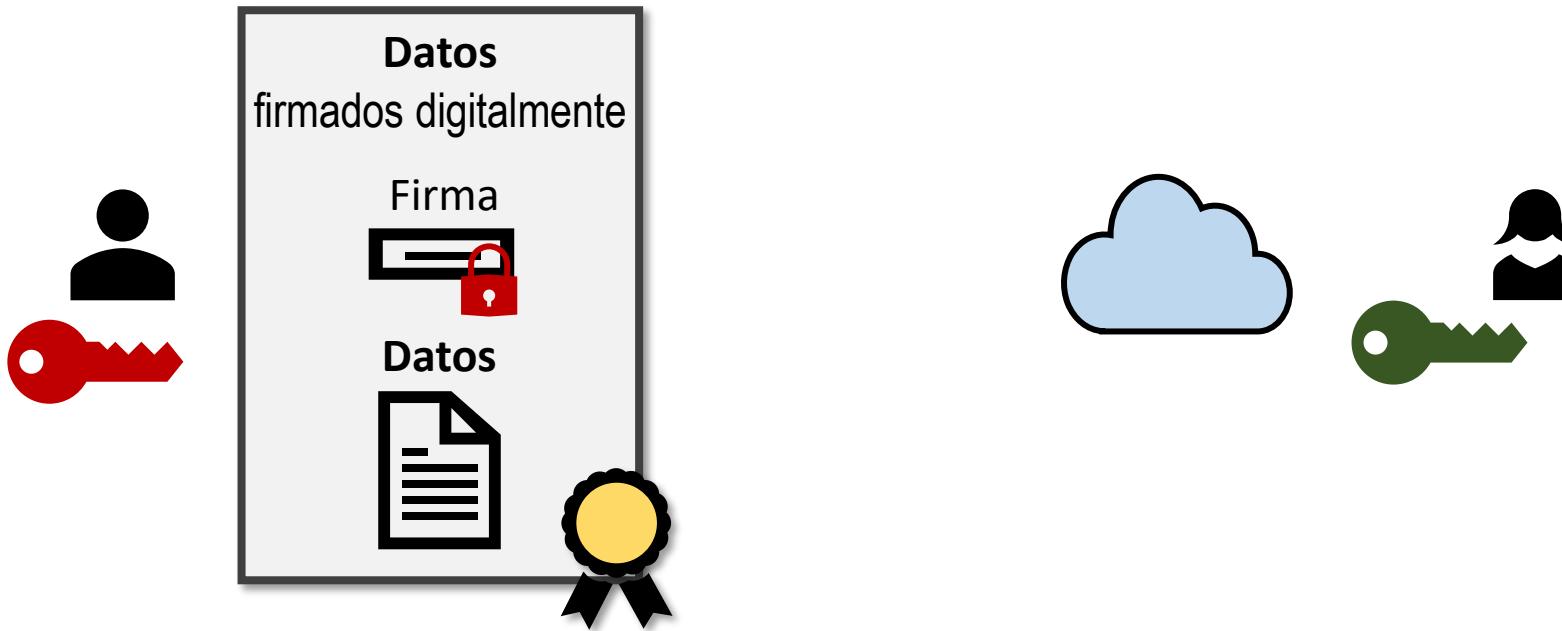
Obteniendo una firma digital mediante su clave privada

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- Utiliza la clave privada para firmar un hash del mensaje



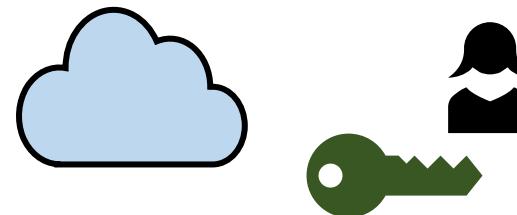
Empaque su mensaje junto con la firma digital obtenida

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- Utiliza la clave privada para firmar un hash del mensaje



Envía el mensaje firmado digitalmente a María

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- | Utiliza la clave privada para firmar un hash del mensaje



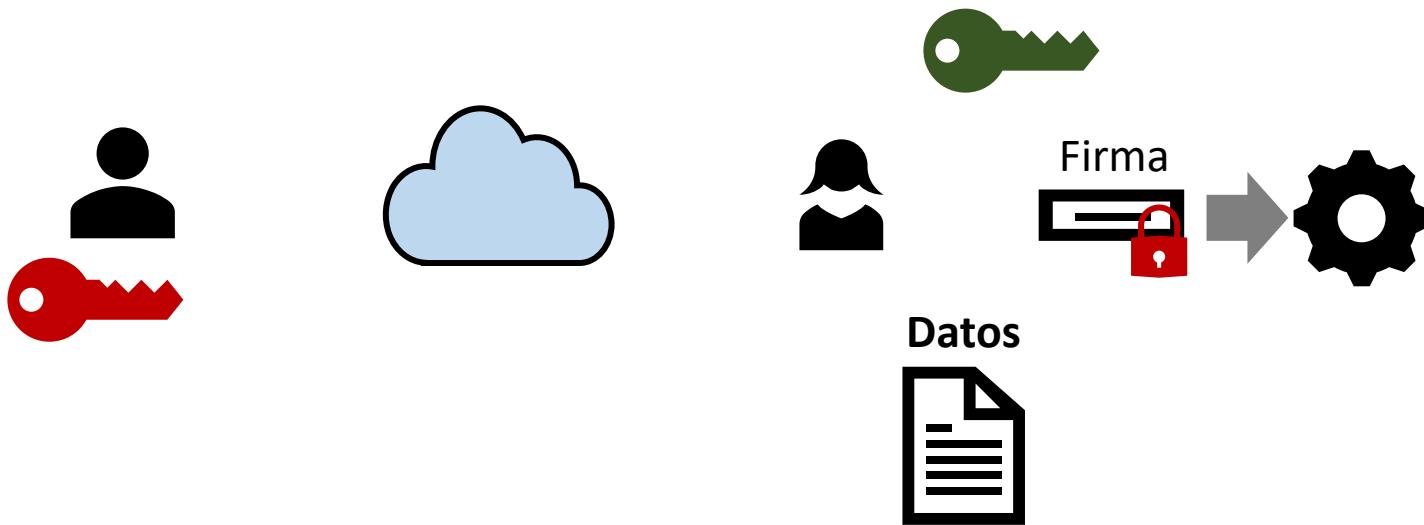
María tiene ahora el mensaje, la firma digital y la clave pública de Juan

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- | Utiliza la clave privada para firmar un hash del mensaje



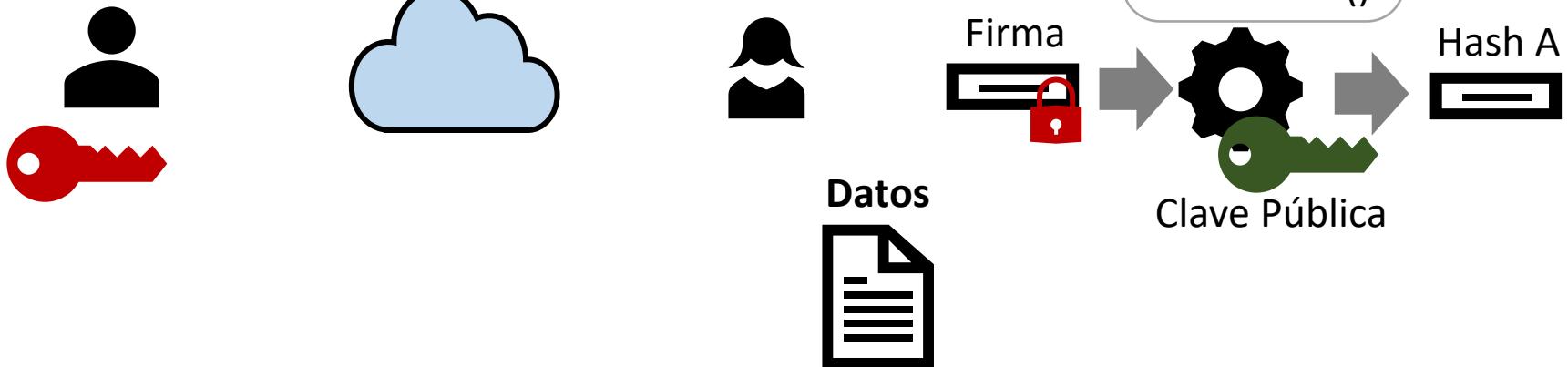
María tiene ahora el mensaje, la firma digital y la clave pública de Juan

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

- Utiliza la clave privada para firmar un hash del mensaje



Mediante la clave pública de Juan, descifra la firma y obtiene de nuevo el hash original

Criptografía básica para blockchain

Criptografía Asimétrica

03BFirma digital

- Utiliza la clave privada para firmar un hash del mensaje



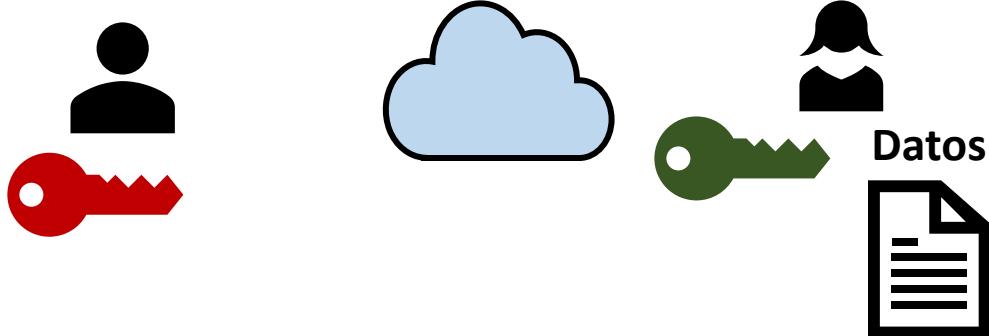
Calcula el hash del documento directamente

Criptografía básica para blockchain

Criptografía Asimétrica

03B Firma digital

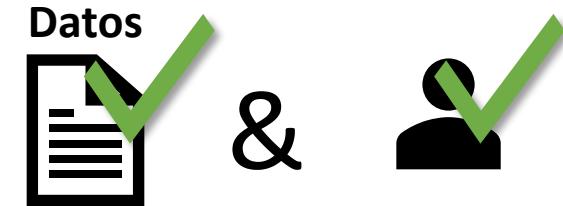
- | Utiliza la clave privada para firmar un hash del mensaje



Compara ambos hash... si coinciden...

If Hash A == Hash B

Then

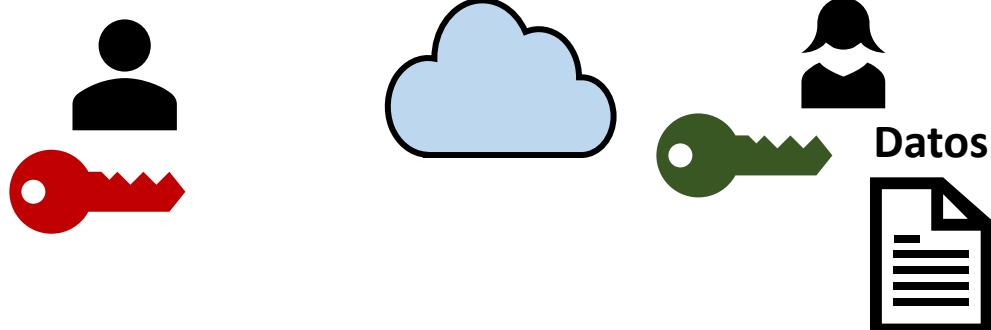


Criptografía básica para blockchain

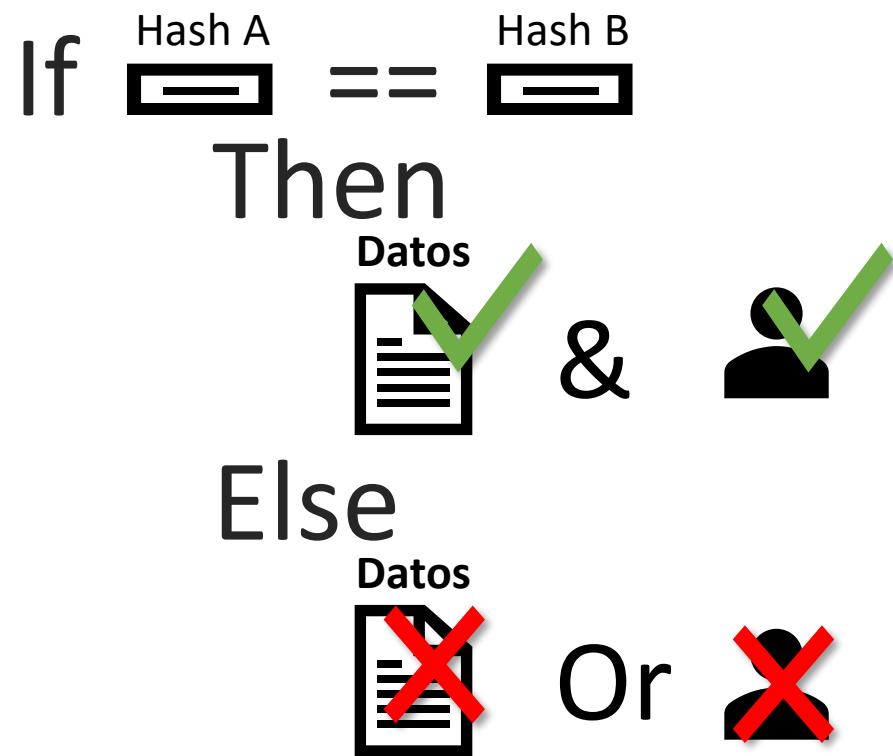
Criptografía Asimétrica

03B Firma digital

- Utiliza la clave privada para firmar un hash del mensaje



...Si no coinciden...

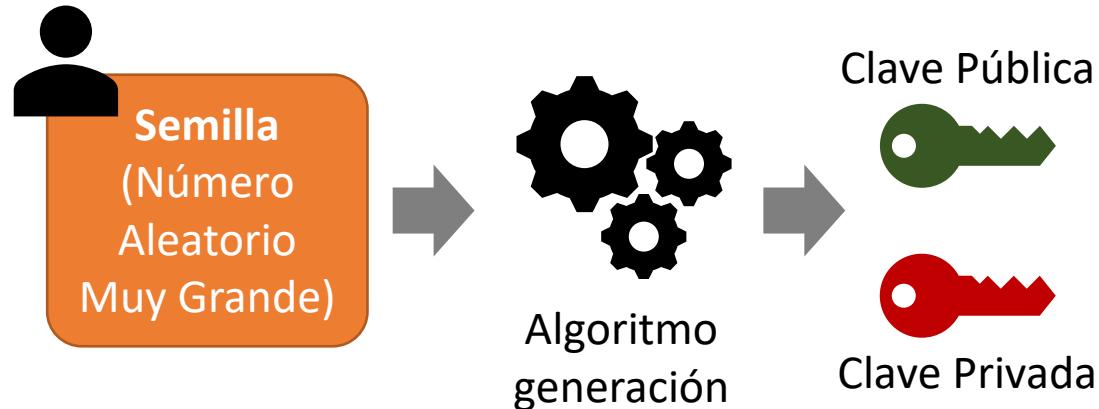


Criptografía básica para blockchain

Criptografía Asimétrica

03 Criptografía Asimétrica

Utiliza un par de claves para encriptar y desencriptar una información



Principalmente lo utilizamos para :

03A Cifrado de clave pública

03B Firma digital

Criptografía básica para blockchain

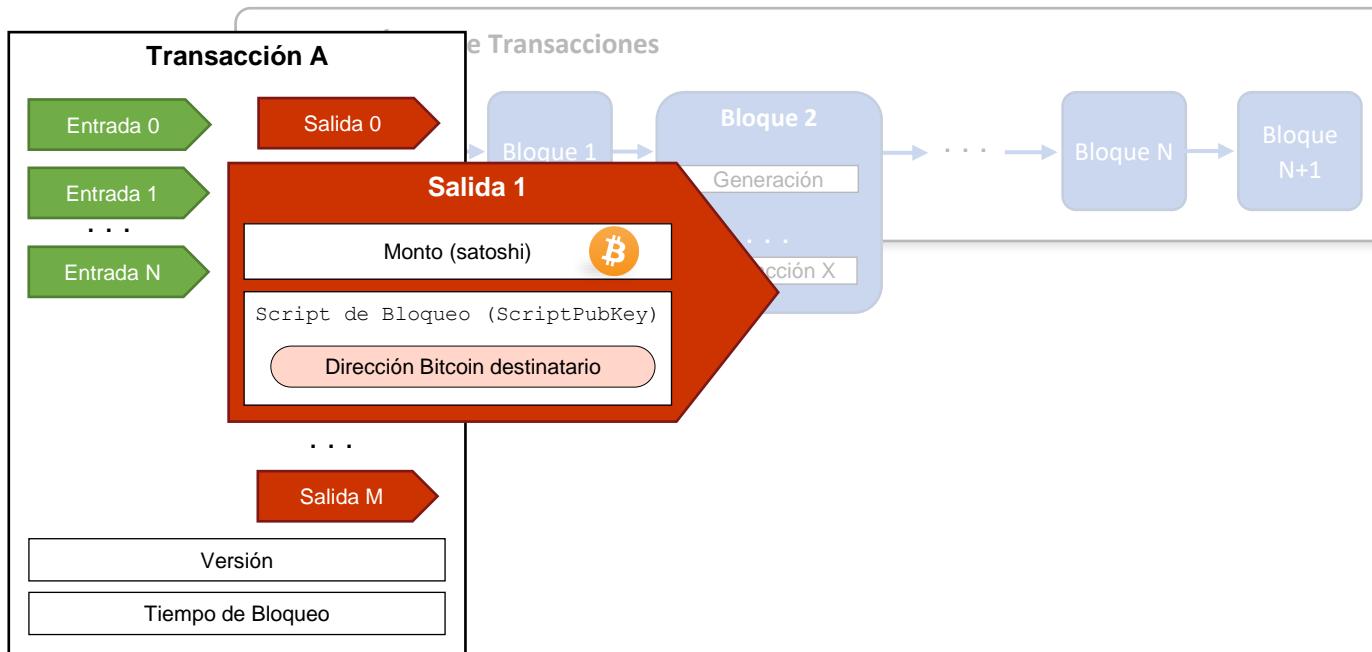
Criptografía Asimétrica

03 Criptografía Asimétrica

- | Utiliza un par de claves para encriptar y desencriptar una información
- | Algoritmos tradicionales más utilizados: RSA, DSA
- | Limitaciones:
 - Tiempo de proceso elevado
 - Claves muy largas
 - El mensaje cifrado ocupa más espacio que el original
- | Criptografía de Curva Elíptica (ECDSA)
 - Variante de criptografía asimétrica más rápida y con claves más cortas

Cadena de Bloques (Blockchain)

Transacciones Tx

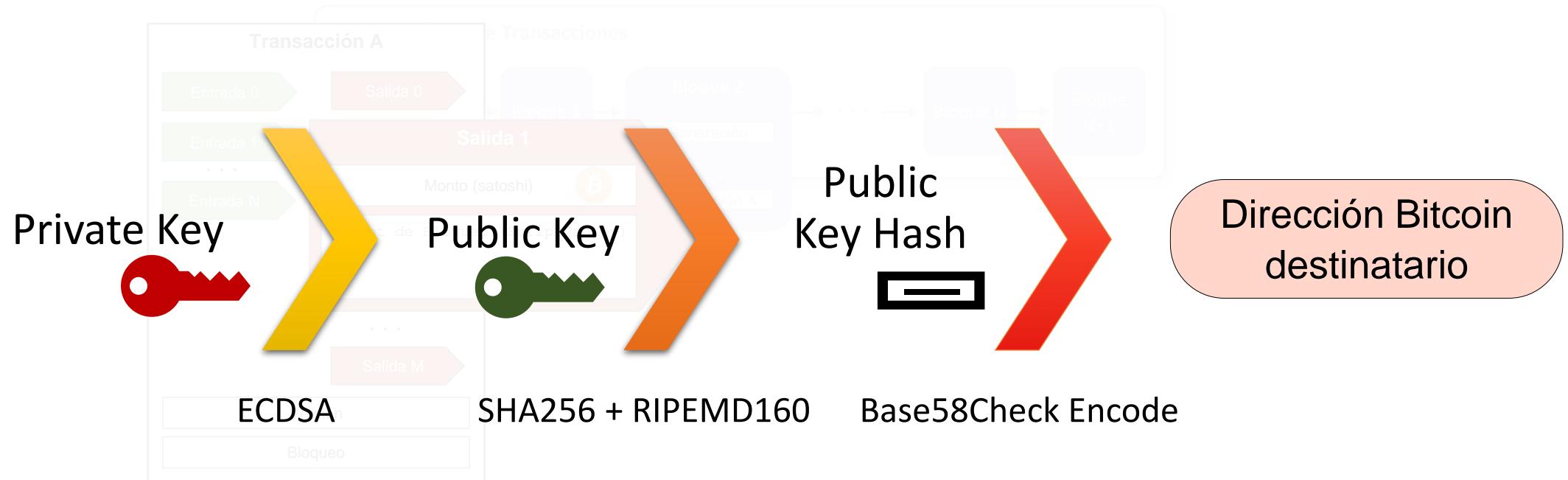


Blockchain



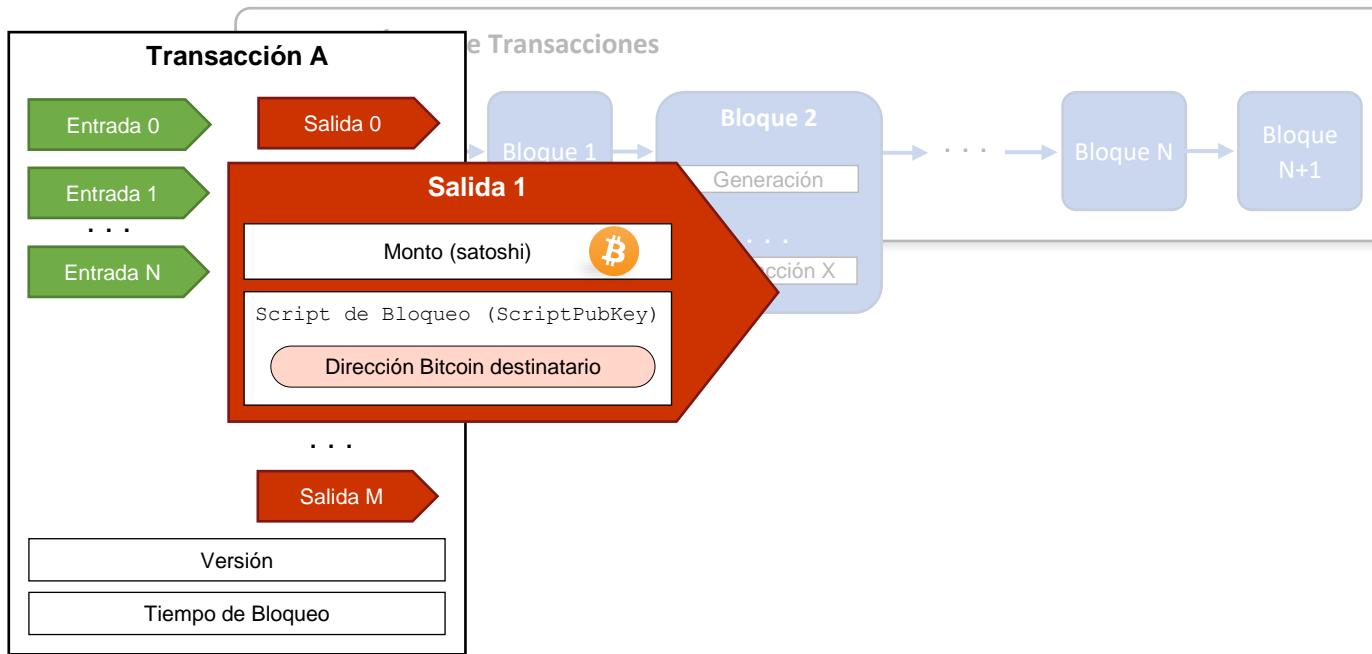
Cadena de Bloques (Blockchain)

Dirección Bitcoin



Cadena de Bloques (Blockchain)

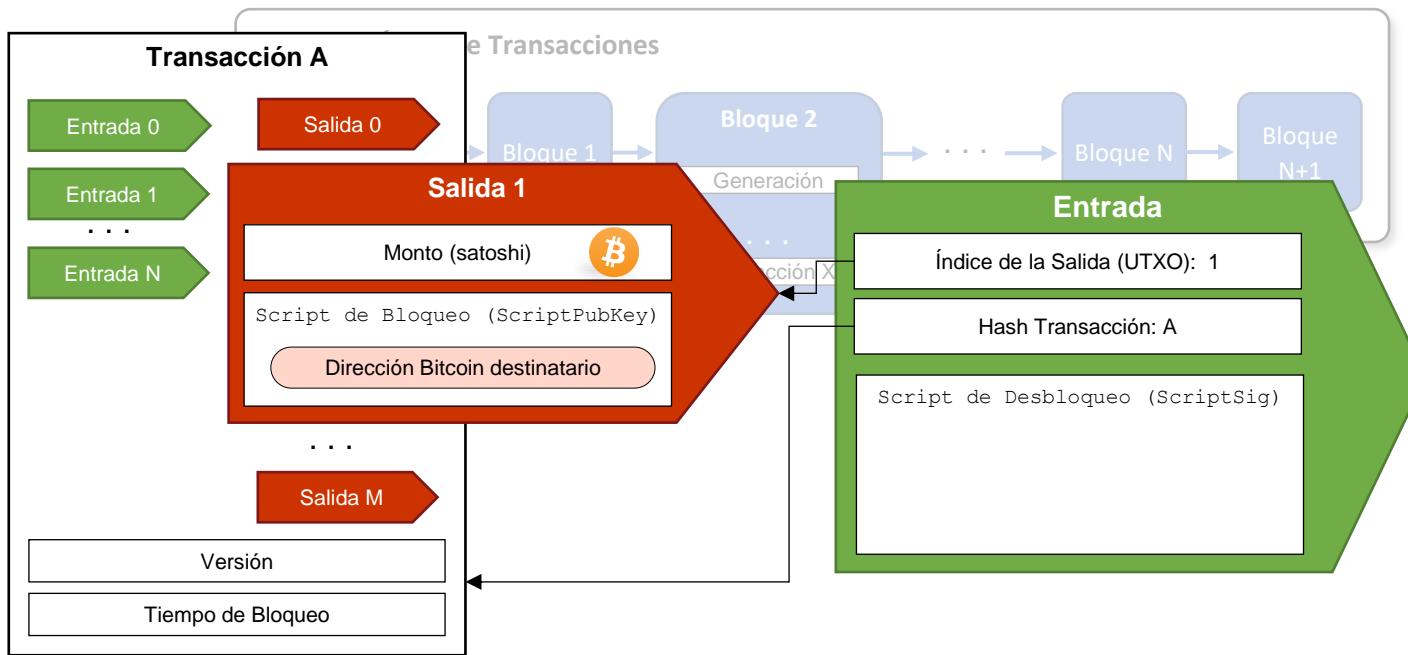
Transacciones Tx



Blockchain

Cadena de Bloques (Blockchain)

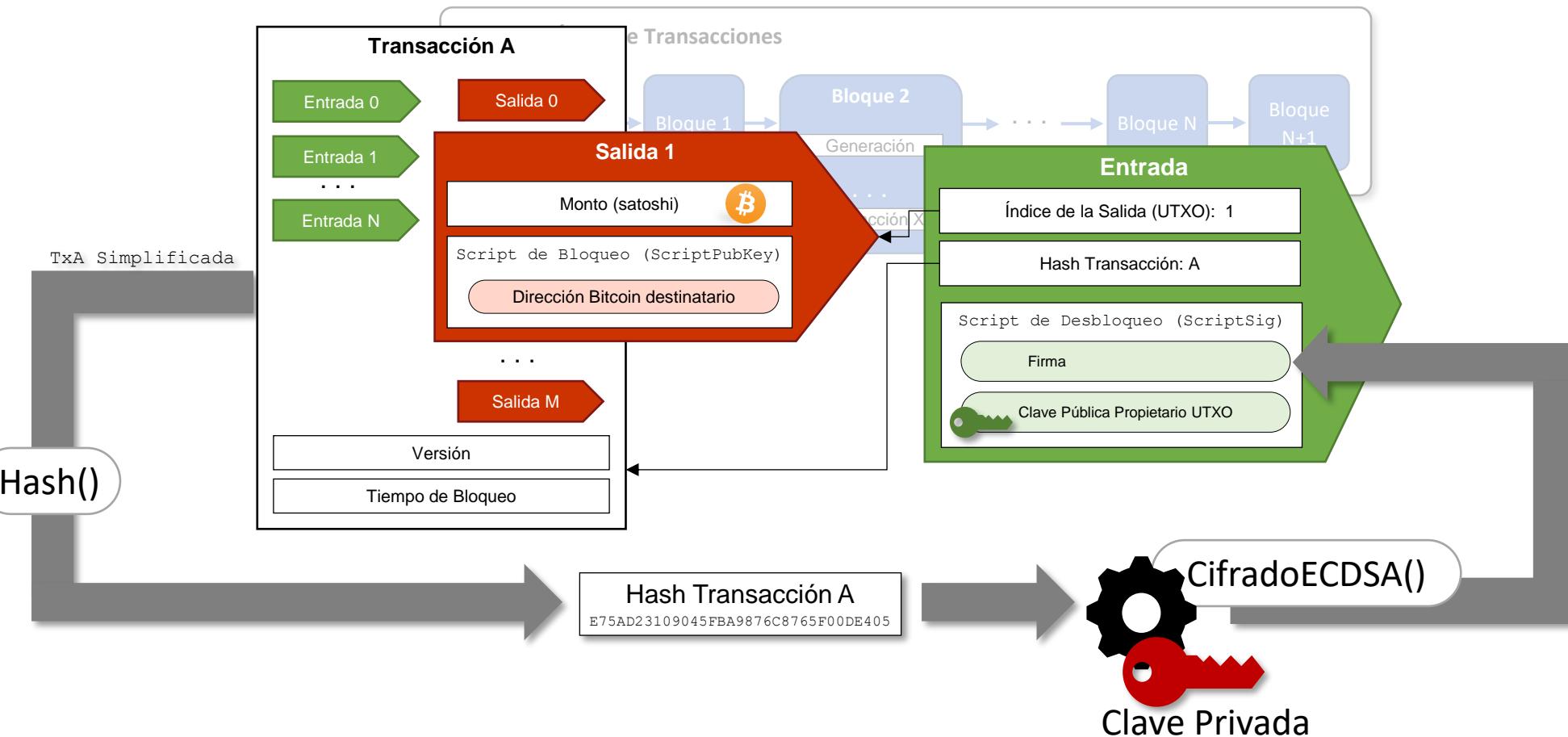
Transacciones Tx



Blockchain

Cadena de Bloques (Blockchain)

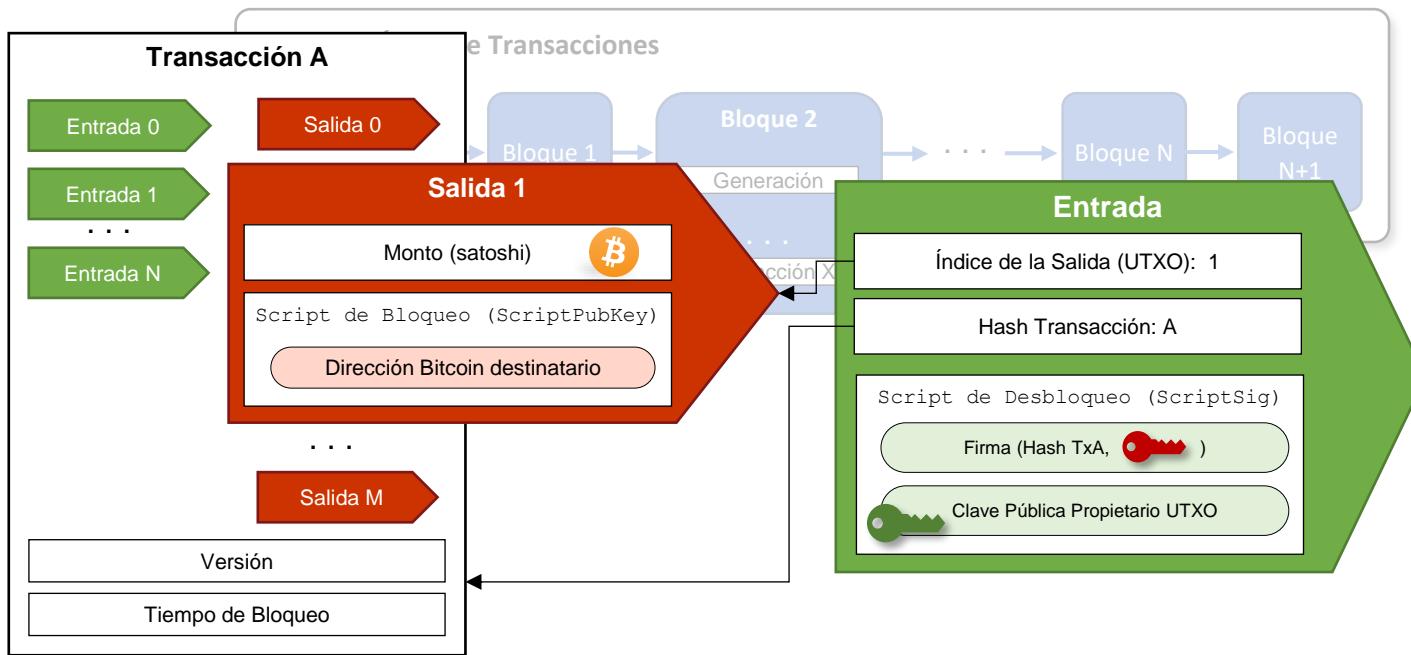
Transacciones Tx



Blockchain

Cadena de Bloques (Blockchain)

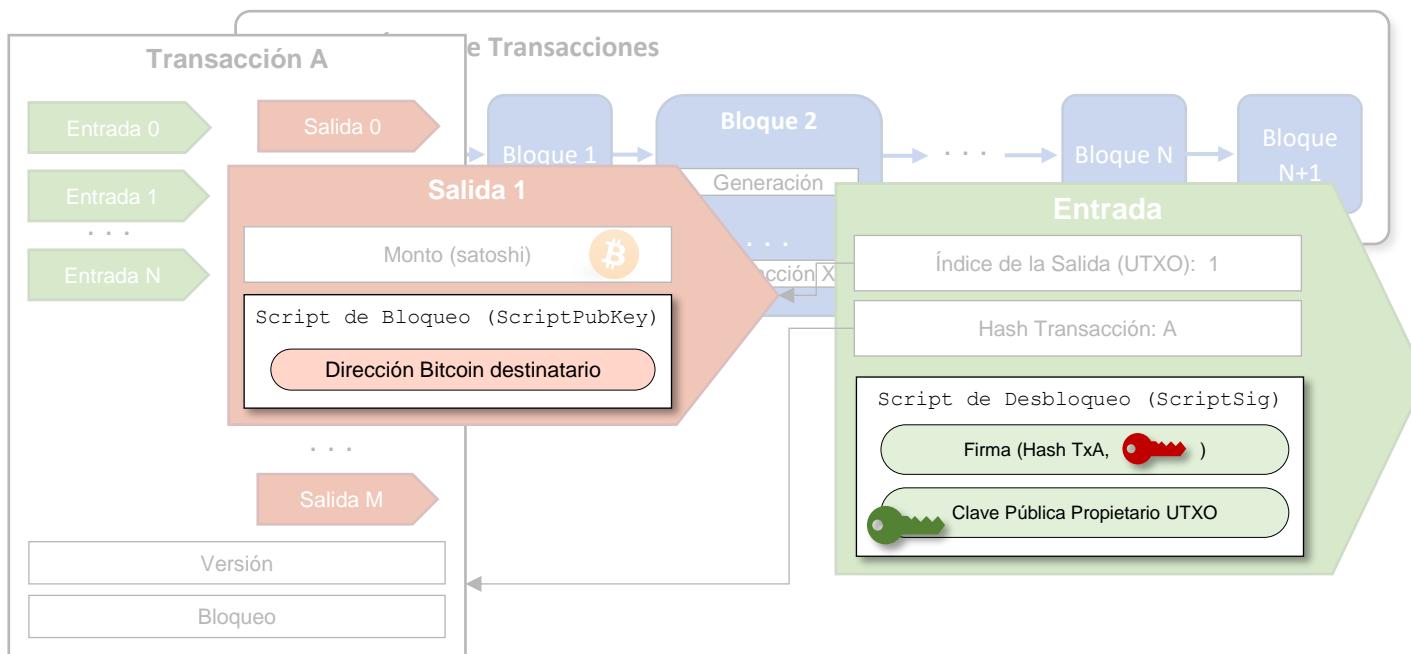
Transacciones Tx



Blockchain

Cadena de Bloques (Blockchain)

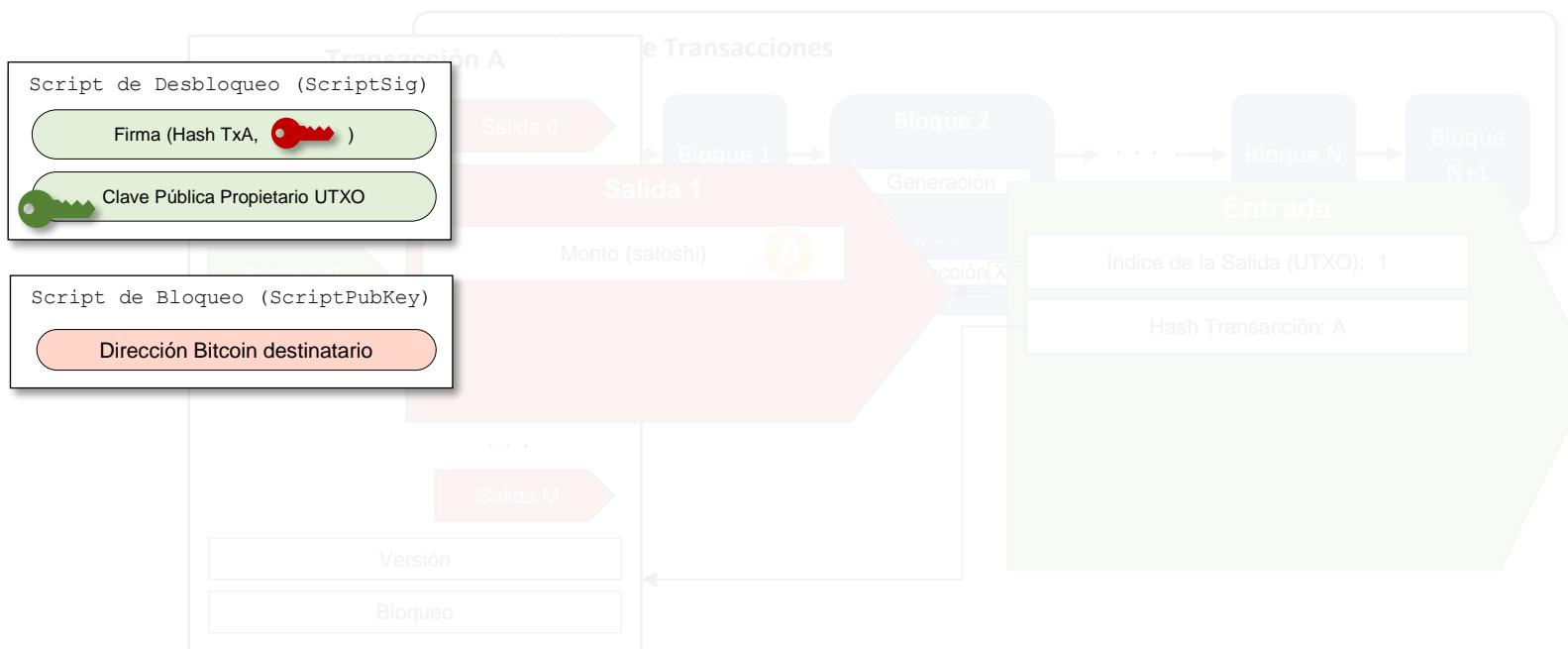
Smart-Contracts Script Verification



Blockchain

Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification

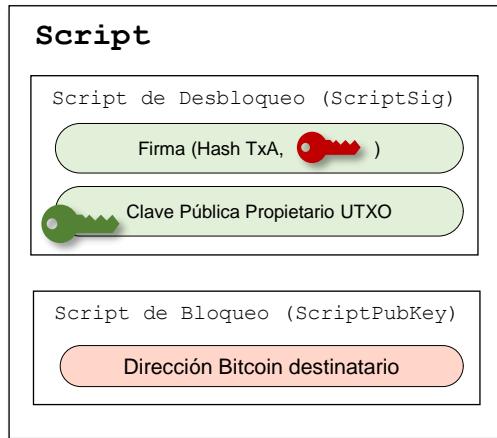


Blockchain



Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification



01 Script de Desbloqueo

El usuario que desea acceder al UTXO debe proporcionar las **credenciales** necesarias para **demostrar que le pertenece**

02 Script de Bloqueo

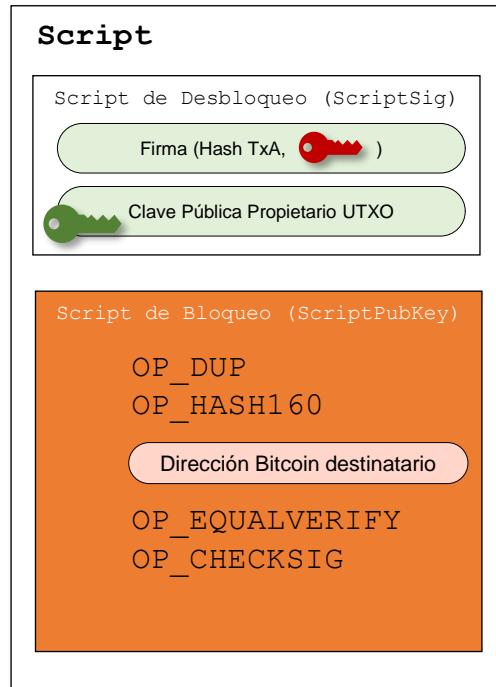
Especifica qué **condiciones** se deben **cumplir** para que alguien pueda acceder al UTXO

demostrar que la dirección bitcoin del UTXO le pertenece



Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification



01 Script de Desbloqueo

El usuario que desea acceder al UTXO debe proporcionar las credenciales necesarias para demostrar que le pertenece

02 Script de Bloqueo

Especifica qué condiciones se deben cumplir para que alguien pueda acceder al UTXO

demostrar que la dirección bitcoin del UTXO le pertenece



Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification

00 Cargamos credenciales en la pila
| Cargamos la Firma





Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification



00 Cargamos credenciales en la pila

| Cargamos la Firma

| Cargamos la Clave Pública



Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification

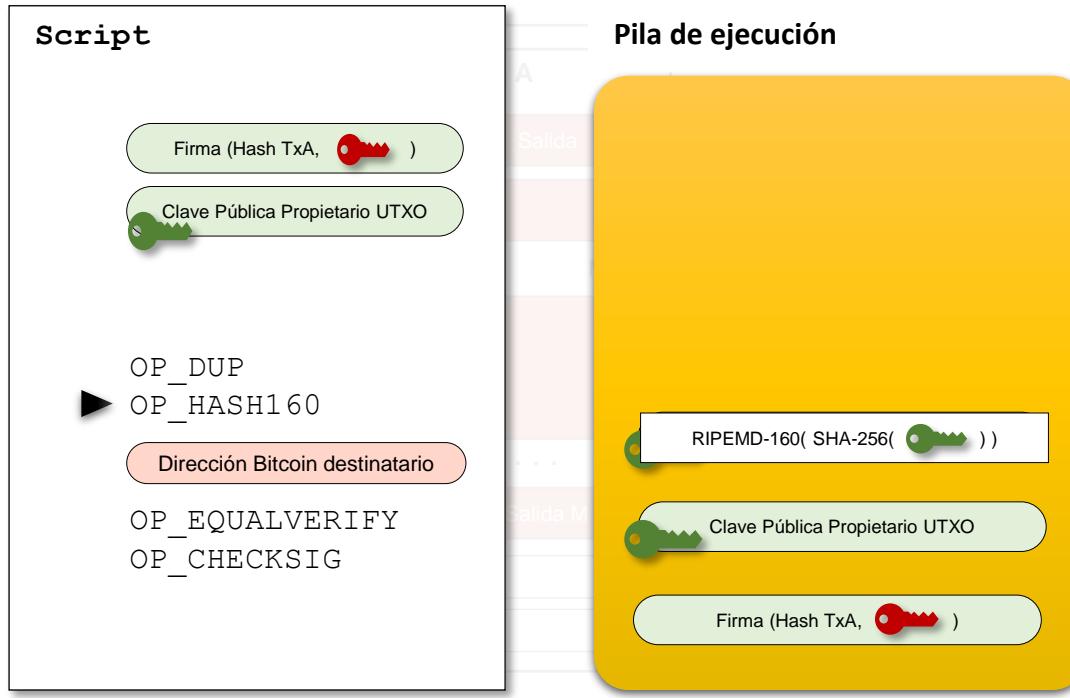


- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
| Duplicamos la Clave Pública

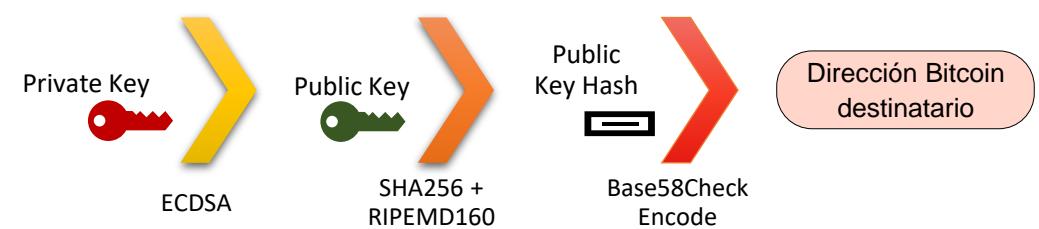


Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification



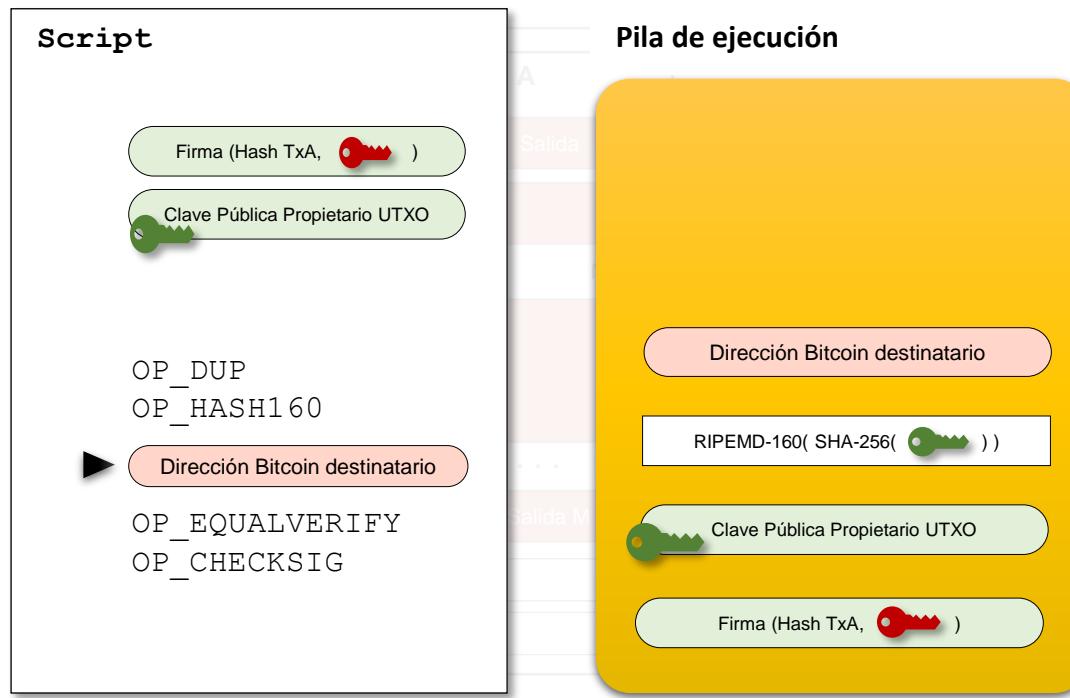
- 00 Cargamos credenciales en la pila
01 Verificar si la Clave Pública corresponde a la Dirección
- | Duplicamos la Clave Pública
 - | Le aplicamos un Hash



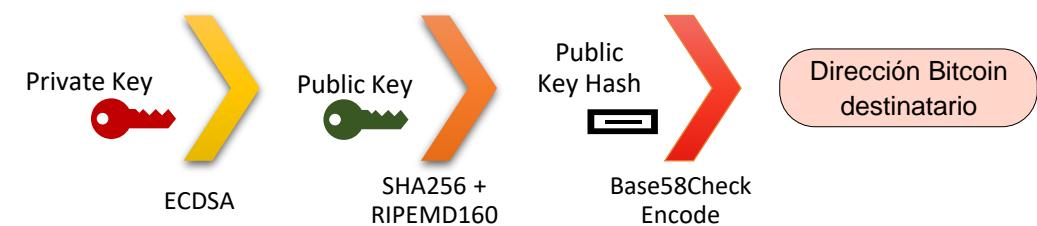
Cadena de Bloques (Blockchain)



Smart-Contracts Script Verification



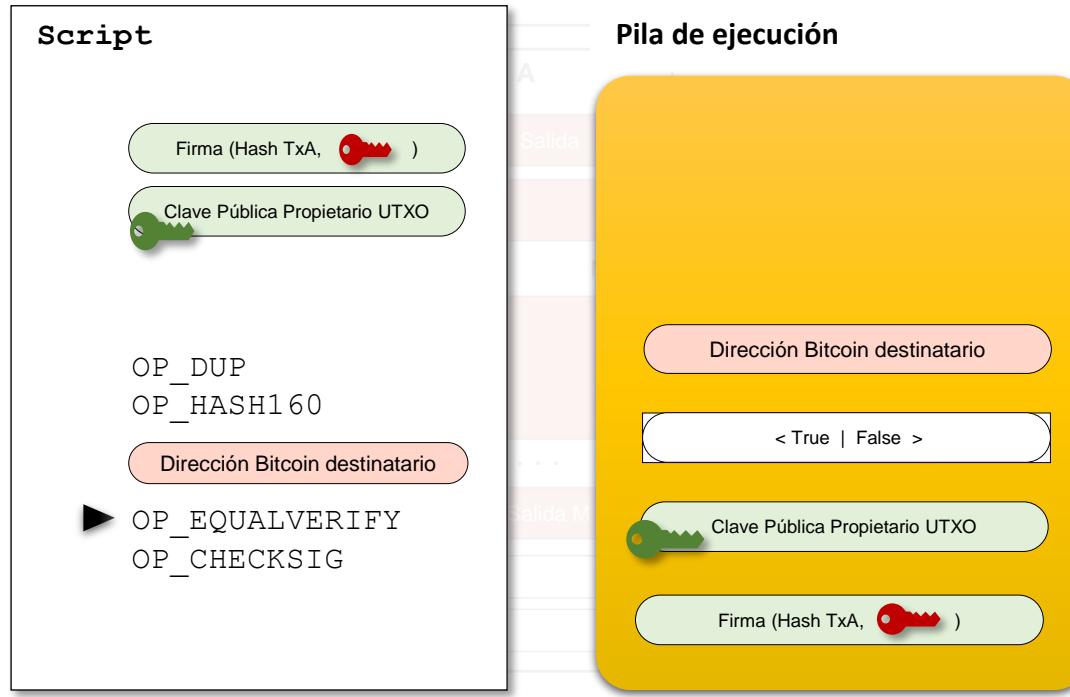
- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
 - | Duplicamos la Clave Pública
 - | Le aplicamos un Hash
 - | Cargamos la Dirección



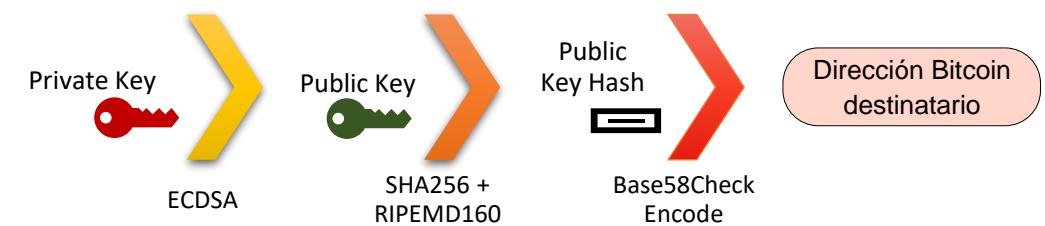


Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification



- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
 - | Duplicamos la Clave Pública
 - | Le aplicamos un Hash
 - | Cargamos la Dirección
 - | Verificamos si son equivalentes





Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification

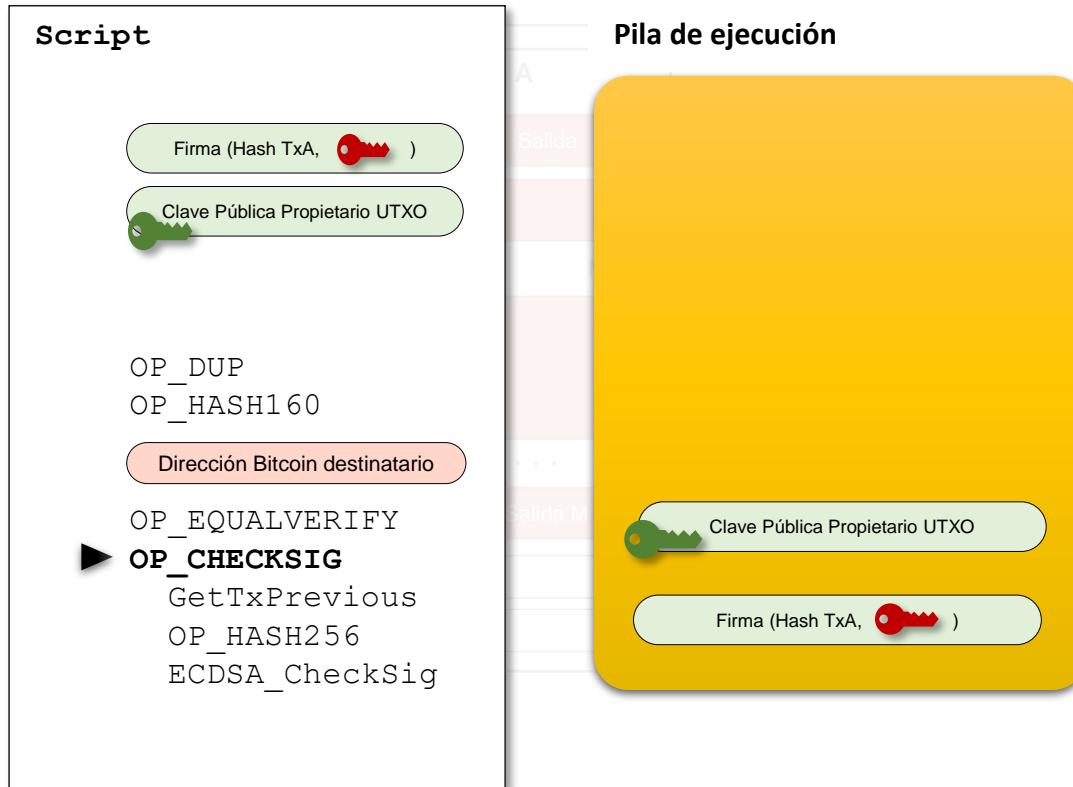


- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
- 02 Verificar si la **Firma** es correcta (si se generó con la Clave Privada)

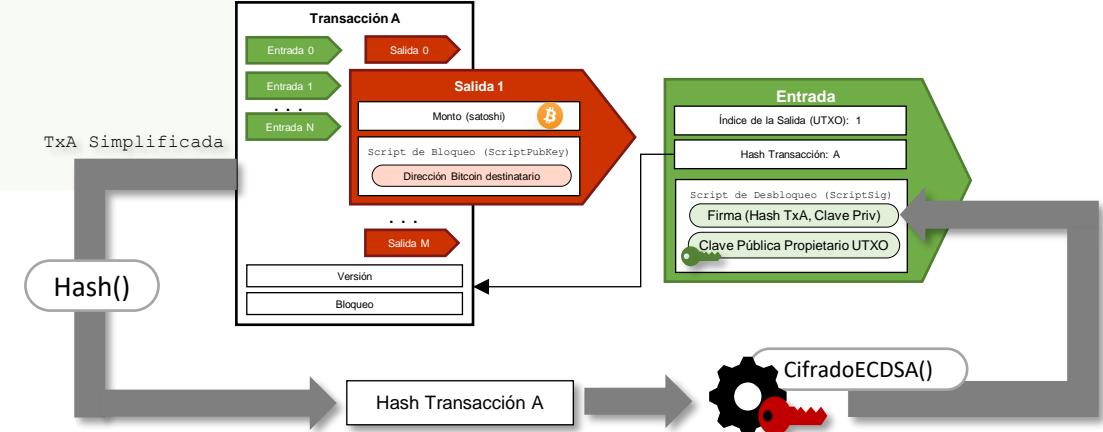


Cadena de Bloques (Blockchain)

Smart-Contracts Script Verification



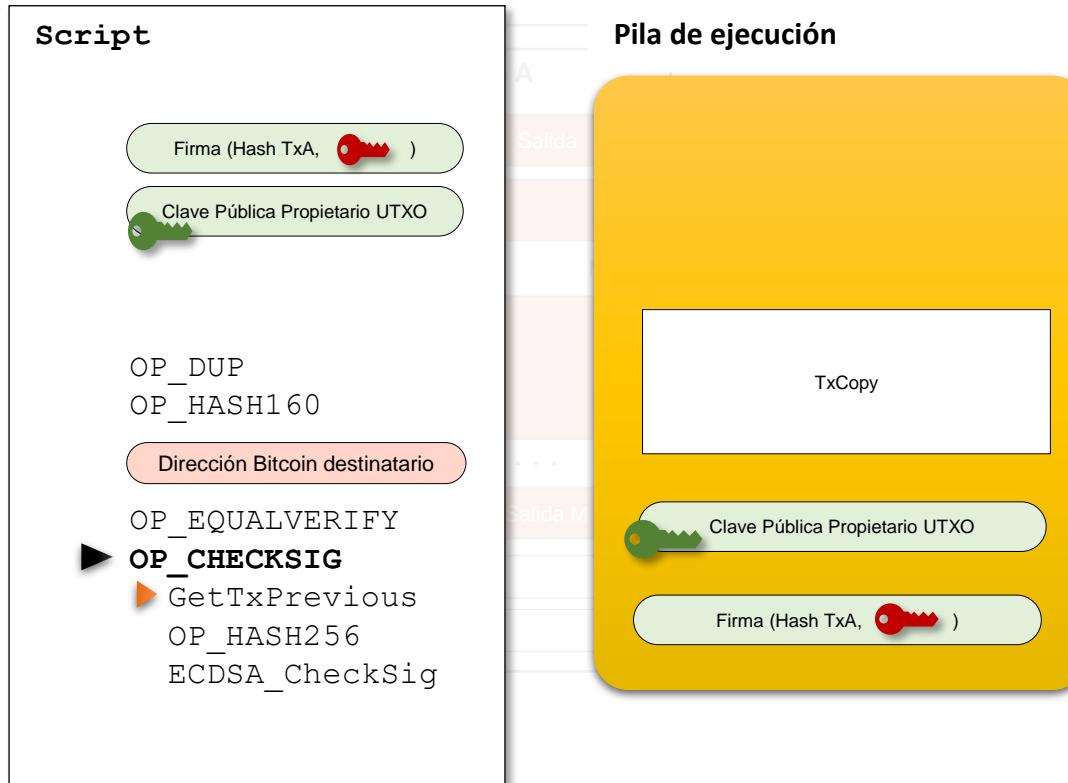
- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
- 02 Verificar si la **Firma** es correcta (si se generó con la Clave Privada)



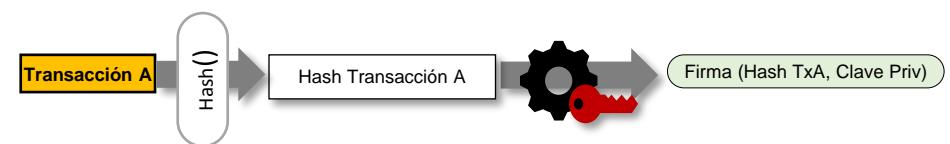
Cadena de Bloques (Blockchain)



Smart-Contracts Script Verification



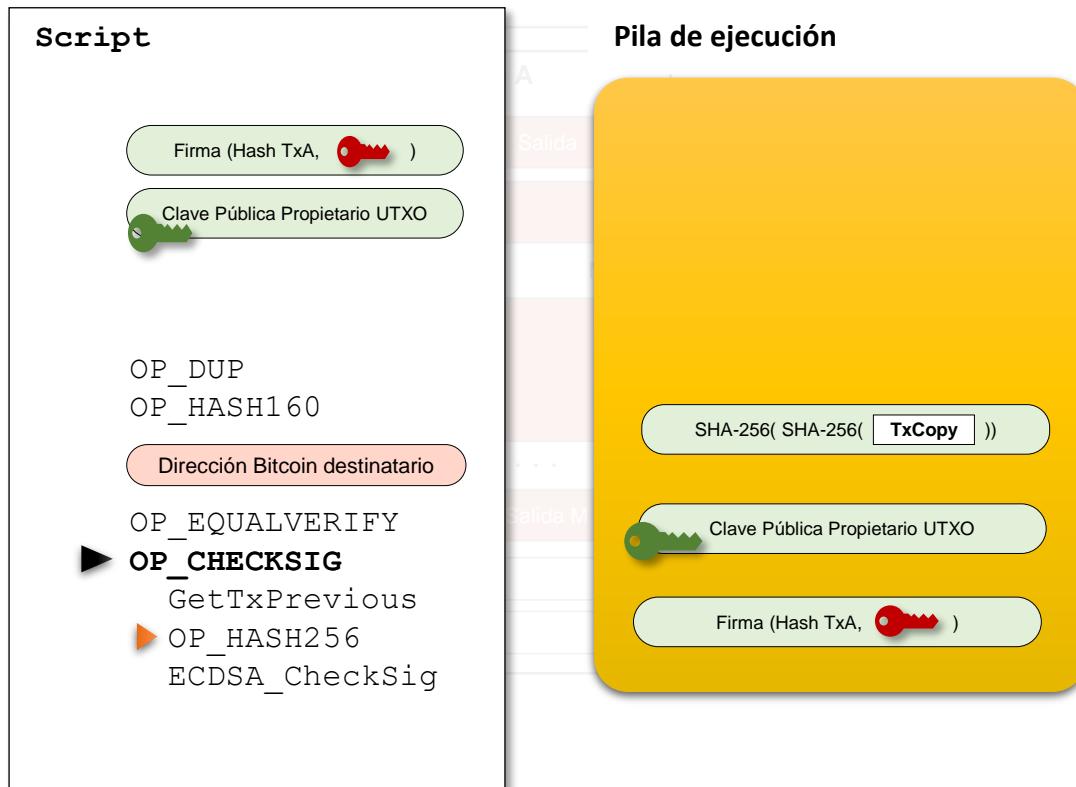
- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
- 02 Verificar si la **Firma** es correcta (si se generó con la Clave Privada)
| Obtenemos la transacción original



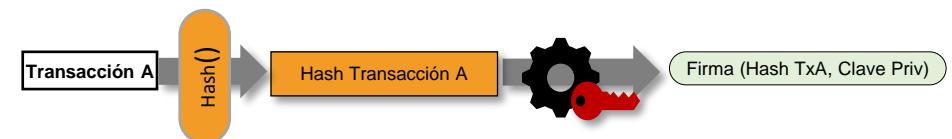
Cadena de Bloques (Blockchain)



Smart-Contracts Script Verification



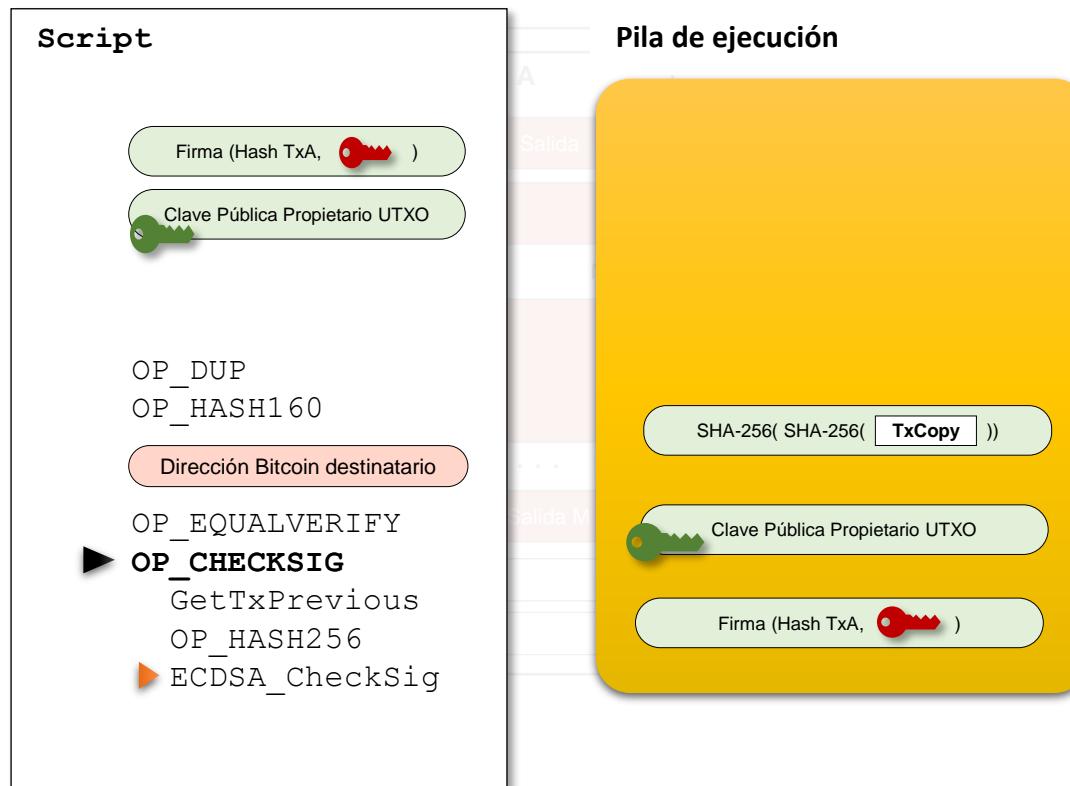
- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
- 02 Verificar si la **Firma** es correcta (si se generó con la Clave Privada)
 - | Obtenemos la transacción original
 - | Le aplicamos un Hash



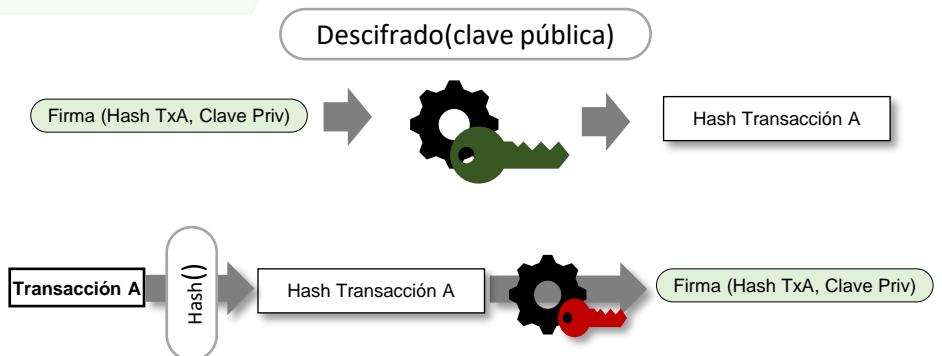
Cadena de Bloques (Blockchain)



Smart-Contracts Script Verification



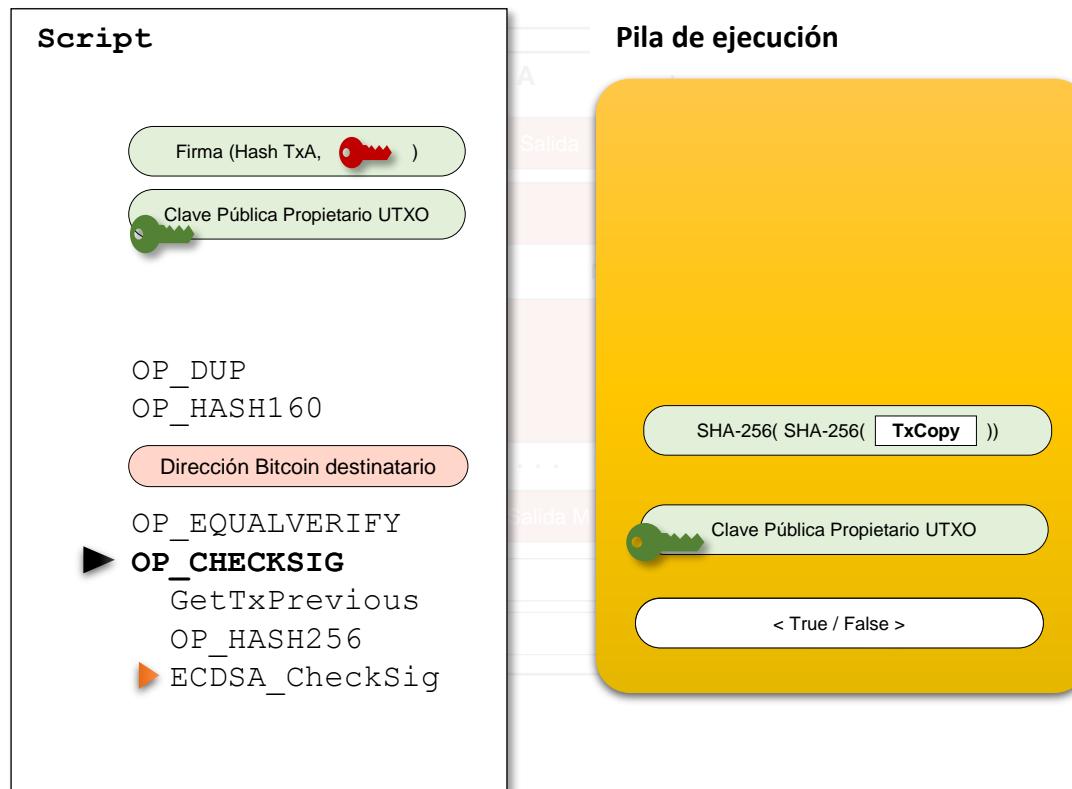
- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
- 02 Verificar si la **Firma** es correcta (si se generó con la Clave Privada)
 - | Obtenemos la transacción original
 - | Le aplicamos un Hash
 - | Verificamos que la firma es correcta



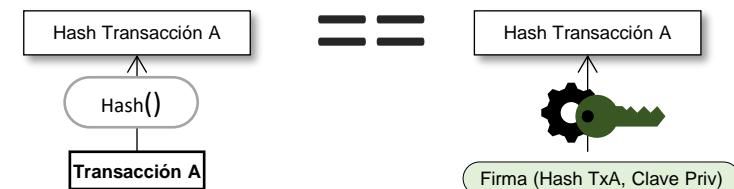
Cadena de Bloques (Blockchain)



Smart-Contracts Script Verification



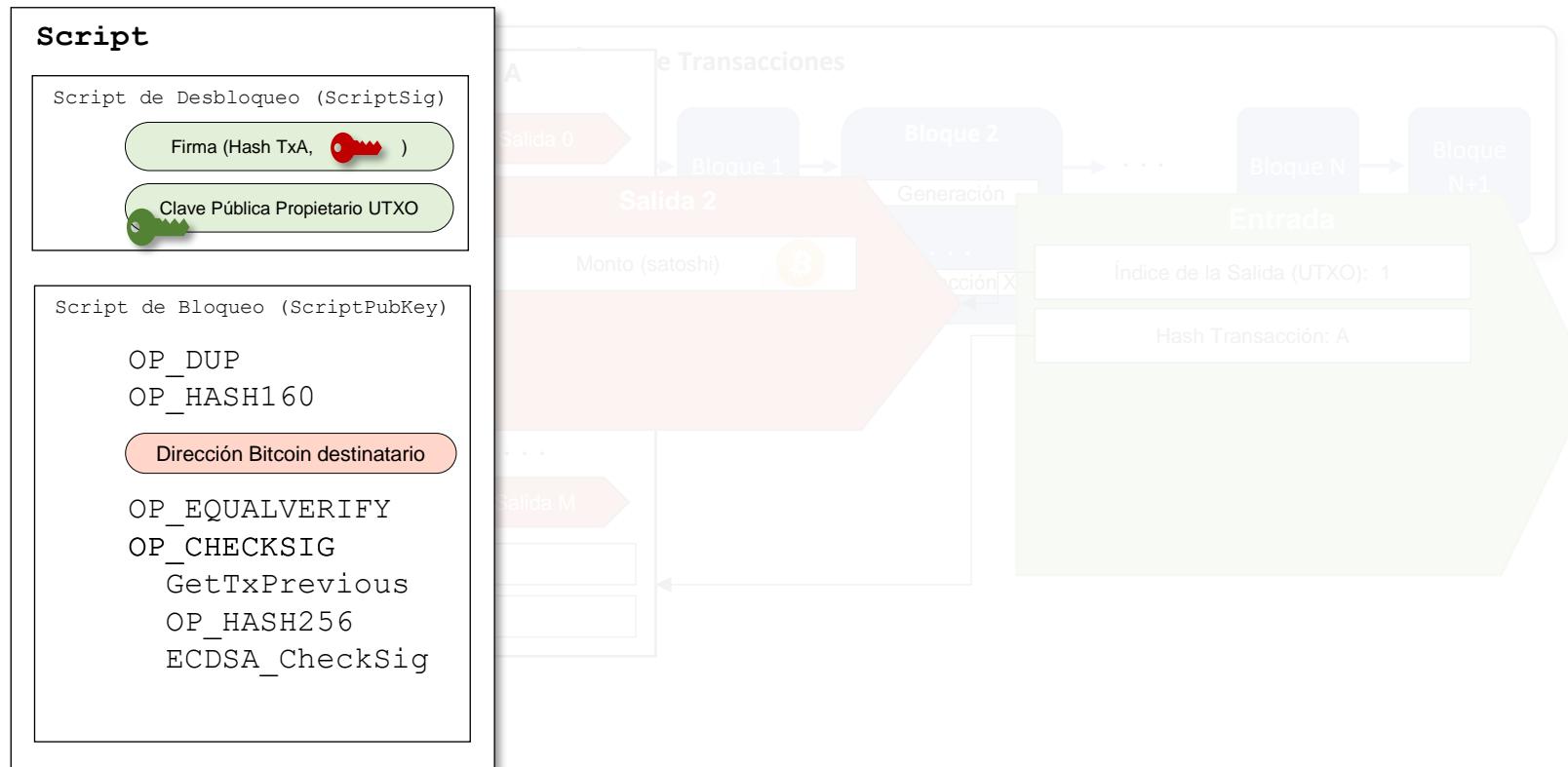
- 00 Cargamos credenciales en la pila
- 01 Verificar si la Clave Pública corresponde a la Dirección
- 02 Verificar si la **Firma** es correcta (si se generó con la Clave Privada)
 - | Obtenemos la transacción original
 - | Le aplicamos un Hash
 - | Verificamos que la firma es correcta
 - | El resultado será valor de la cima de la pila: TRUE o FALSE





Cadena de Bloques (Blockchain)

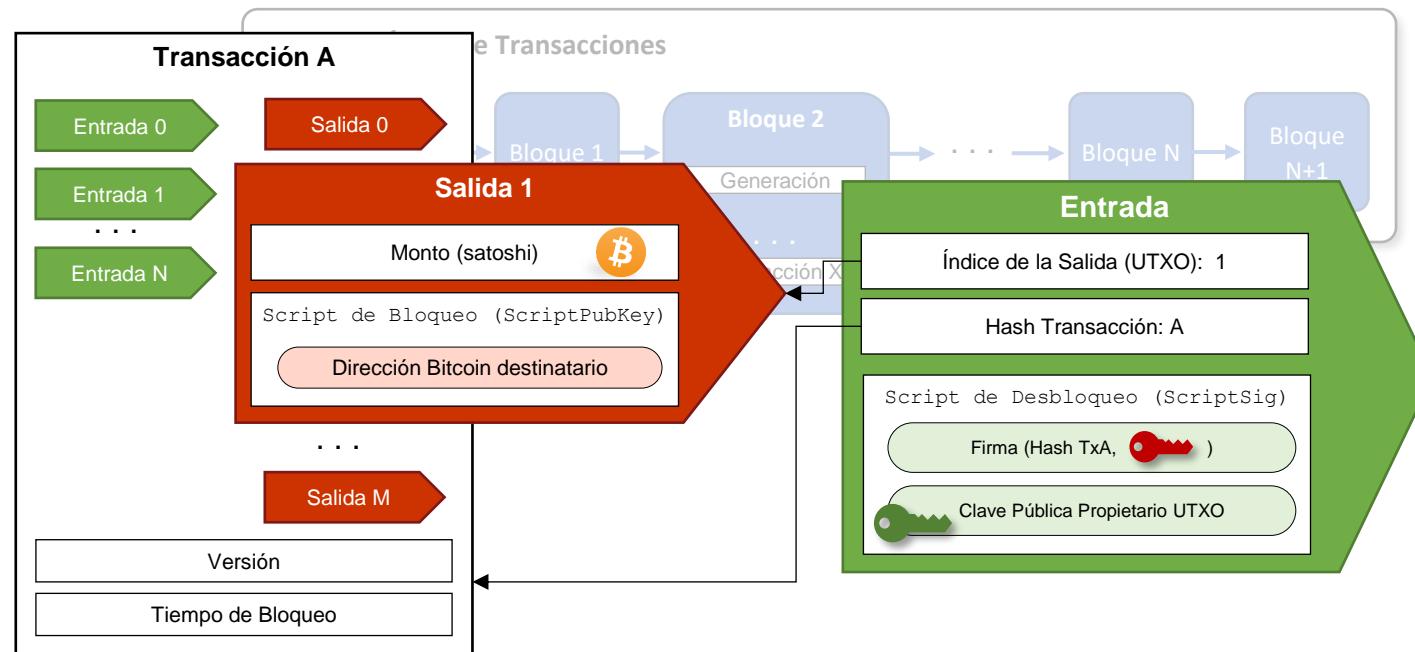
Smart-Contracts Script Verification



Cadena de Bloques (Blockchain)



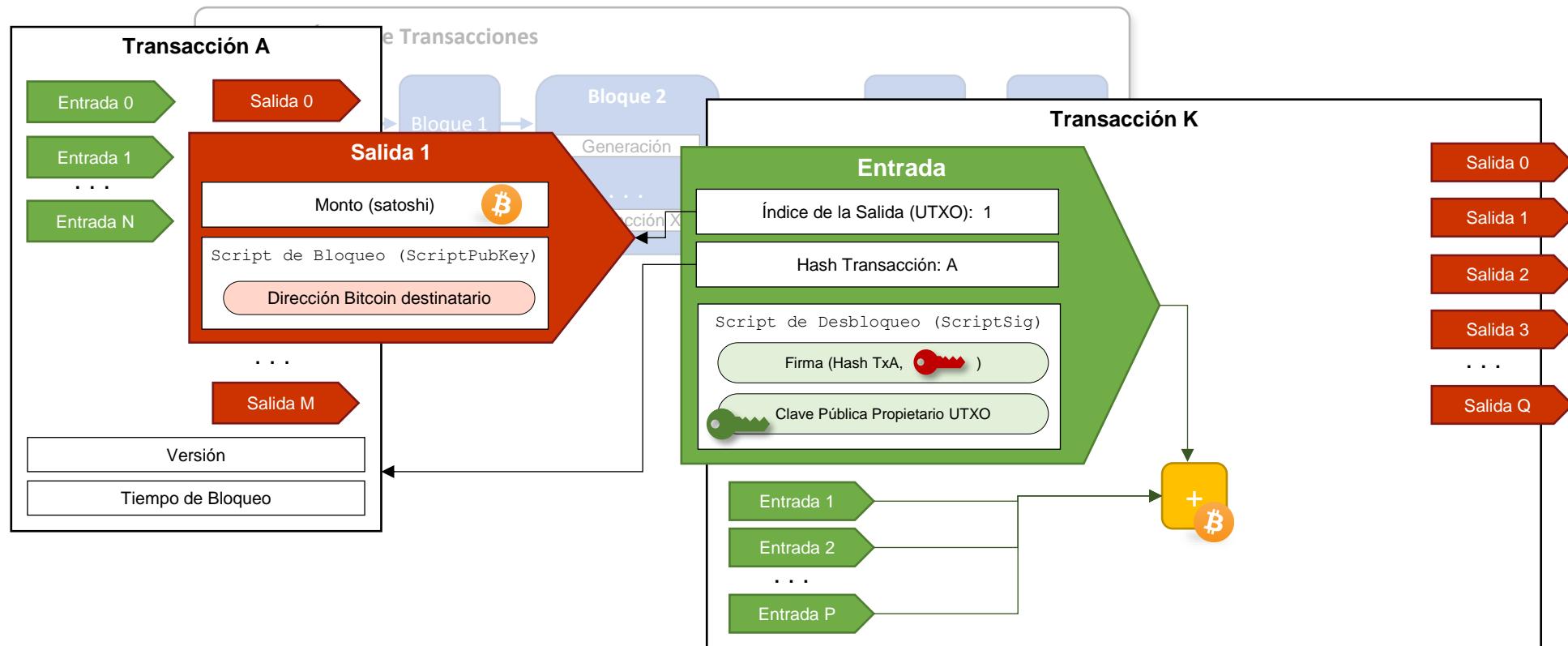
Transacciones Tx



Cadena de Bloques (Blockchain)



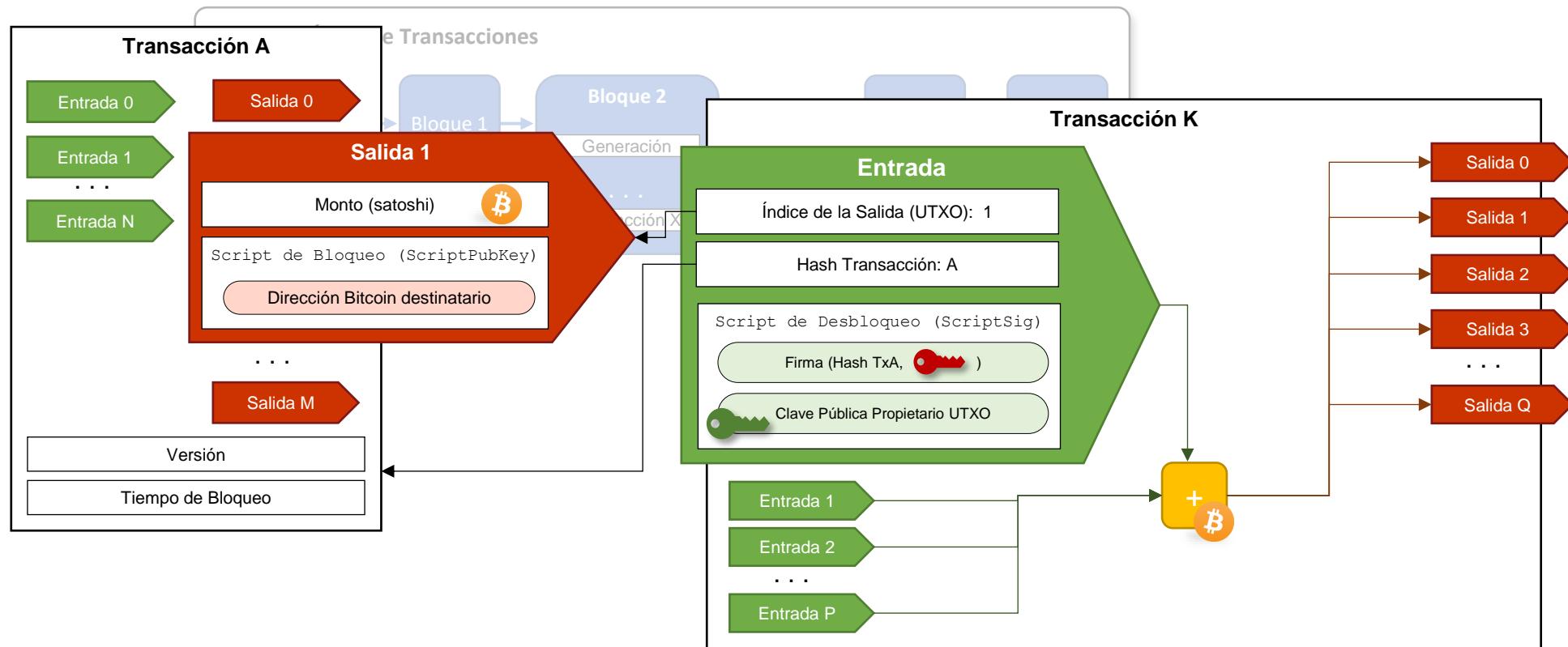
Transacciones Tx



Cadena de Bloques (Blockchain)



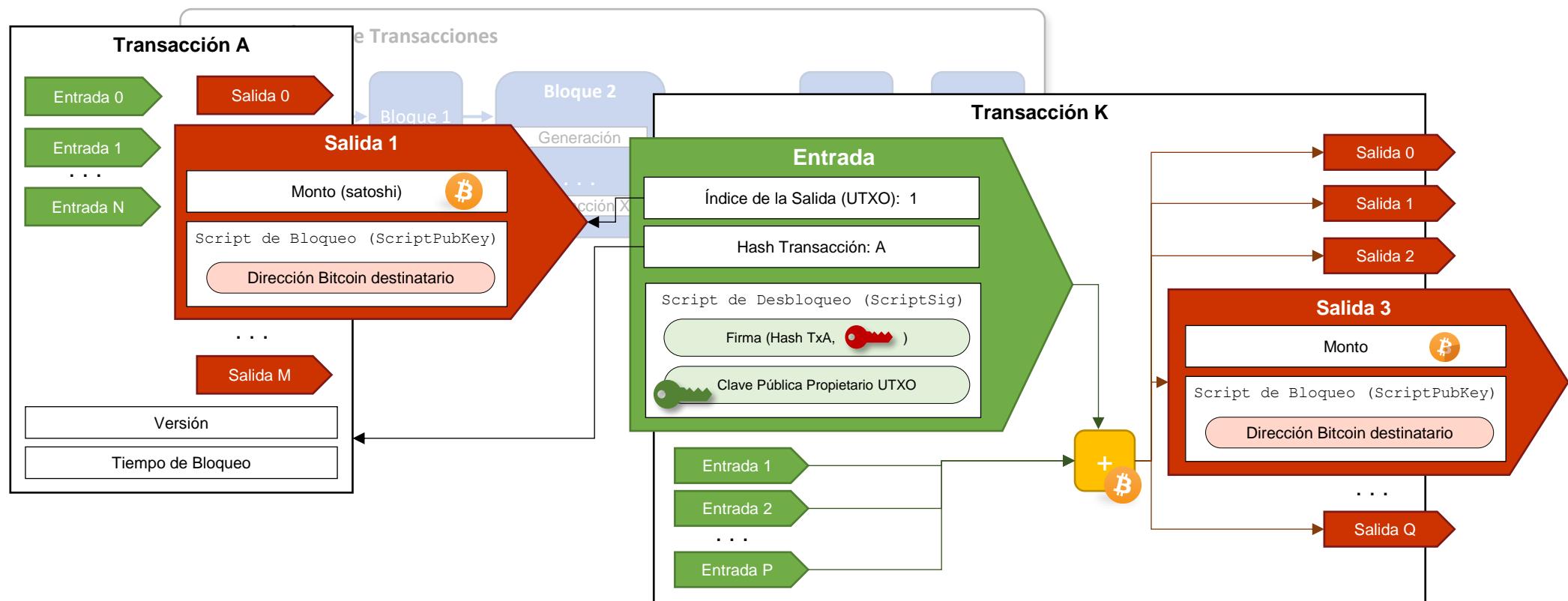
Transacciones Tx



Cadena de Bloques (Blockchain)



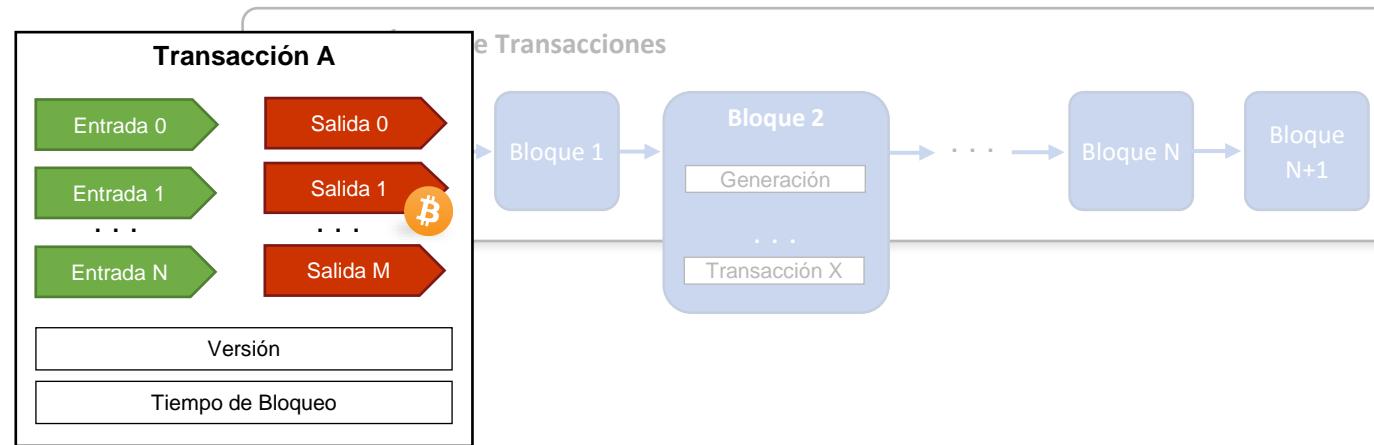
Transacciones Tx



Cadena de Bloques (Blockchain)



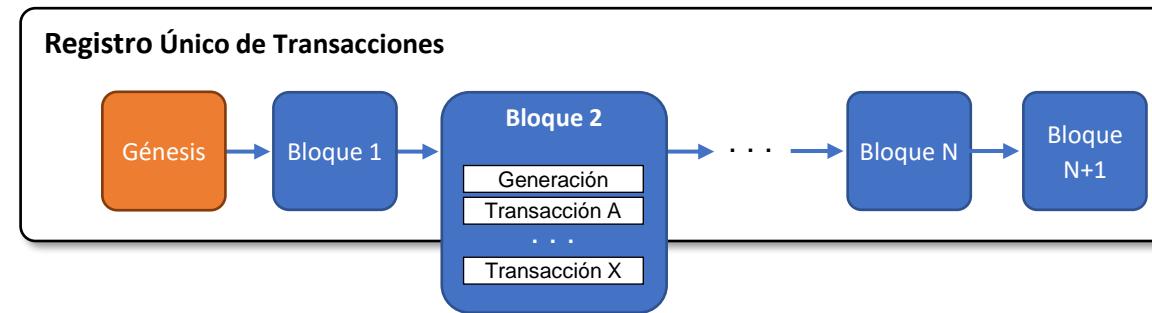
Transacciones Tx



Cadena de Bloques (Blockchain)



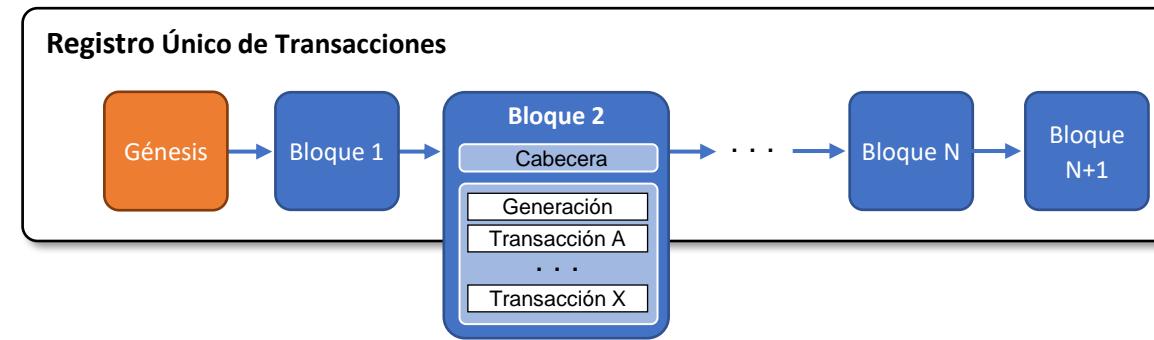
Transacciones Tx



Cadena de Bloques (Blockchain)



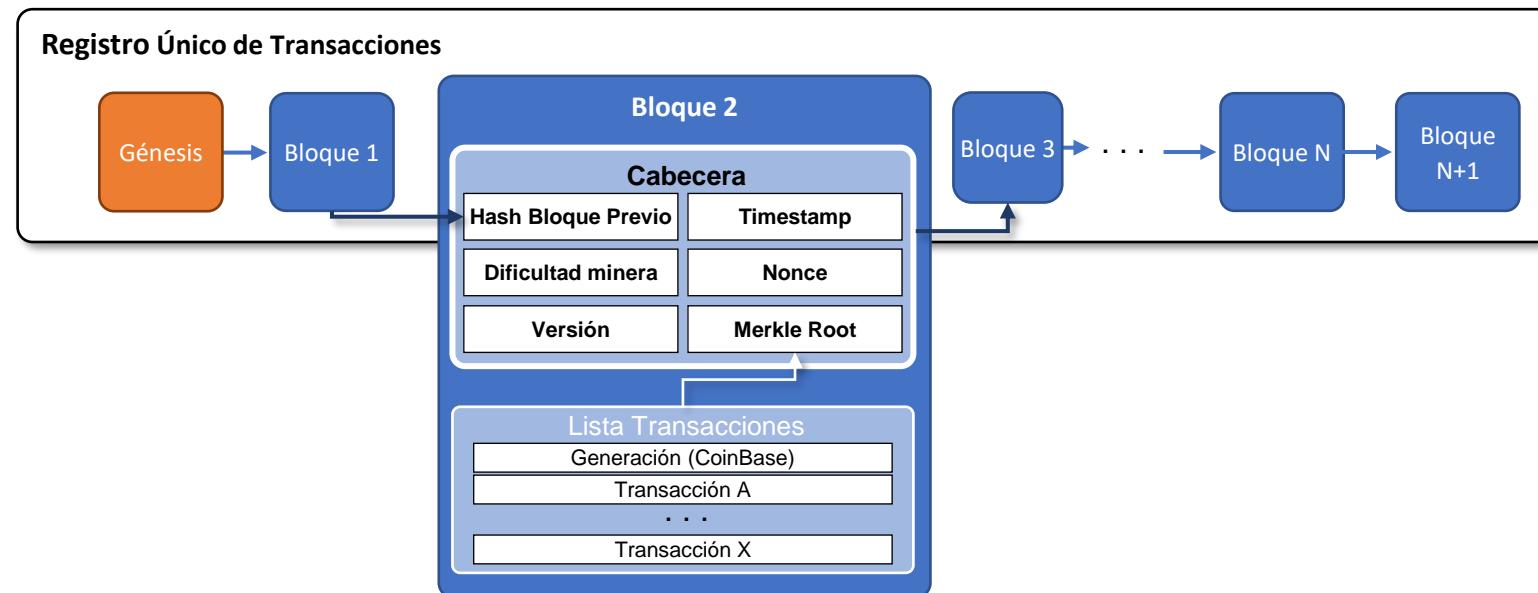
Cabecera de bloque



Cadena de Bloques (Blockchain)



Cabecera de bloque



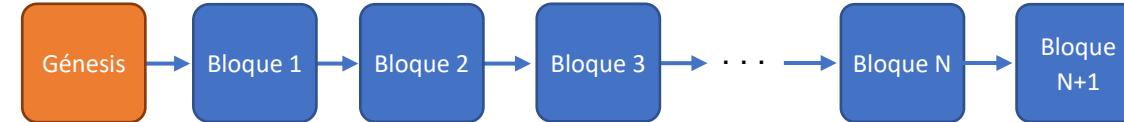


Cadena de Bloques (Blockchain)

Cabecera de bloque



Registro Único de Transacciones



Red P2P





Red P2P Bitcoin

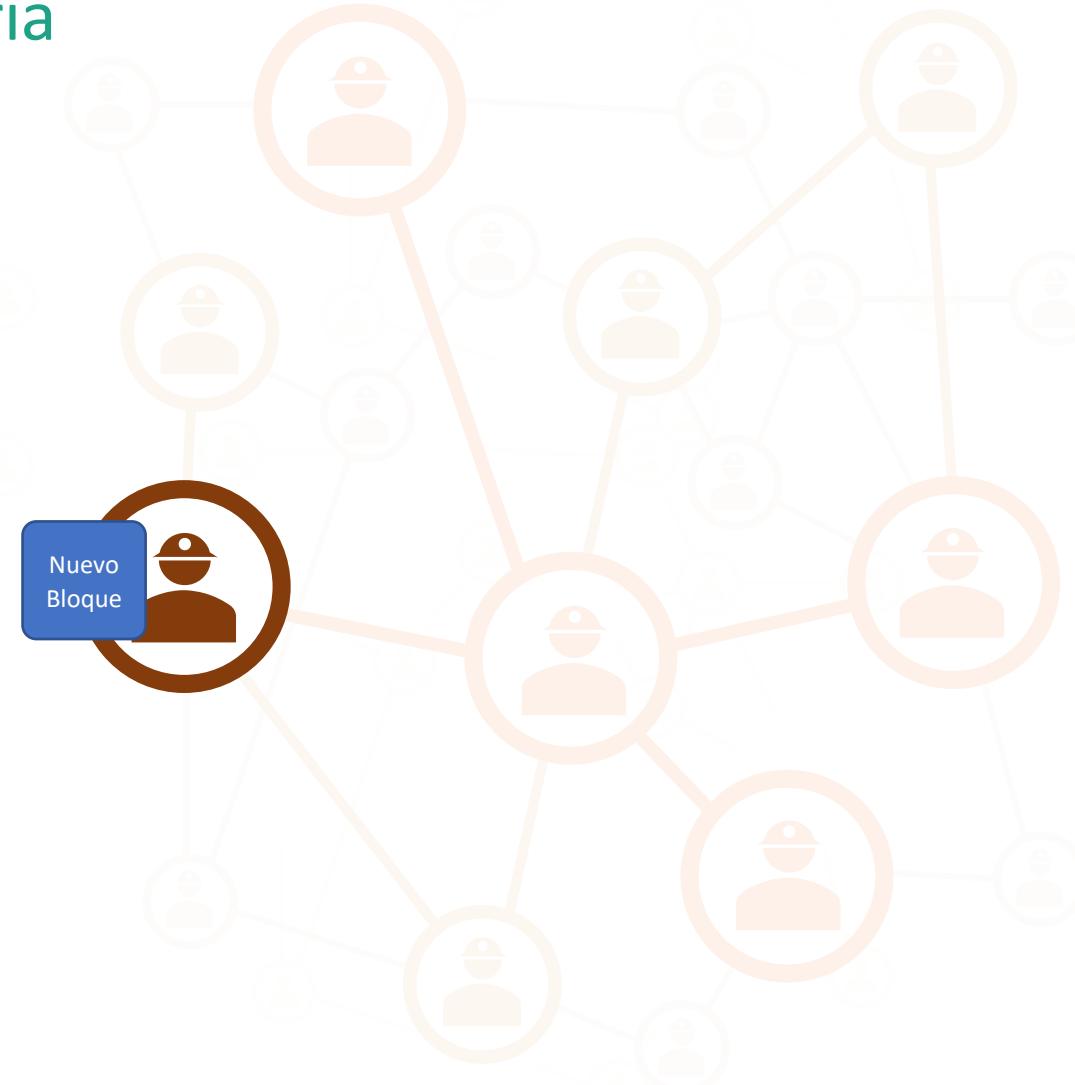
Mineros y Minería





Red P2P Bitcoin

Mineros y Minería





Red P2P Bitcoin

Mineros y Minería



01 PC / Workstation

- | Arquitectura de propósito general
- | Poco eficiente
- | Alto consumo

02 GPU

- | Arquitectura para gráficos
- | Eficiente en operaciones matemáticas
- | Consumo medio/alto

03 ASIC

- | Arquitectura a medida
- | Muy eficiente
- | Medio/bajo consumo





Red P2P Bitcoin

Mineros y Minería



03 ASIC

- | Arquitectura a medida
- | Muy eficiente
- | Medio/bajo consumo



04 Clusters de nodos

- | Cientos o miles de nodos
- | Alto ratio de Hash (TH/s)
- | Enorme consumo y calor

05 Consorcio de mineros (Pools)

- | Trabajo colaborativo
- | Reparto de los beneficios
- | Estrategias más complejas





Red P2P Bitcoin

Mineros y Minería



03 ASIC

- Arquitectura a medida
- Muy eficiente
- Medio/bajo consumo

Bitcoin Core

- Software nodo de red bitcoin
- Gratuito y de código abierto
- Proporciona una **billetera** de bitcoin que verifica completamente los pagos



Red P2P Bitcoin

Mineros y Minería

01 Cada nuevo nodo se conecta (puerto TCP 8333) al menos a otro nodo de la red

- | Mediante direcciones IP establecidas en el código
- | Mediante consulta al nodo dnsseed.bluematt.me que proporciona IPs actualizadas

02 Tras la conexión

- | Descubre nuevos nodos para asegurar conectividad: intercambio de IPs de vecinos entre nodos
- | Debe descargar toda la cadena y validarla (proceso lento y consume muchos recursos)

03 Comunicación entre nodos por inundación. Por cada nueva transacción o bloque recibidos:

- | Validar
- | Transmitirla a nodos vecinos





Red P2P Bitcoin

Mineros y Minería



03 ASIC

- Arquitectura a medida
- Muy eficiente
- Medio/bajo consumo

Bitcoin Core

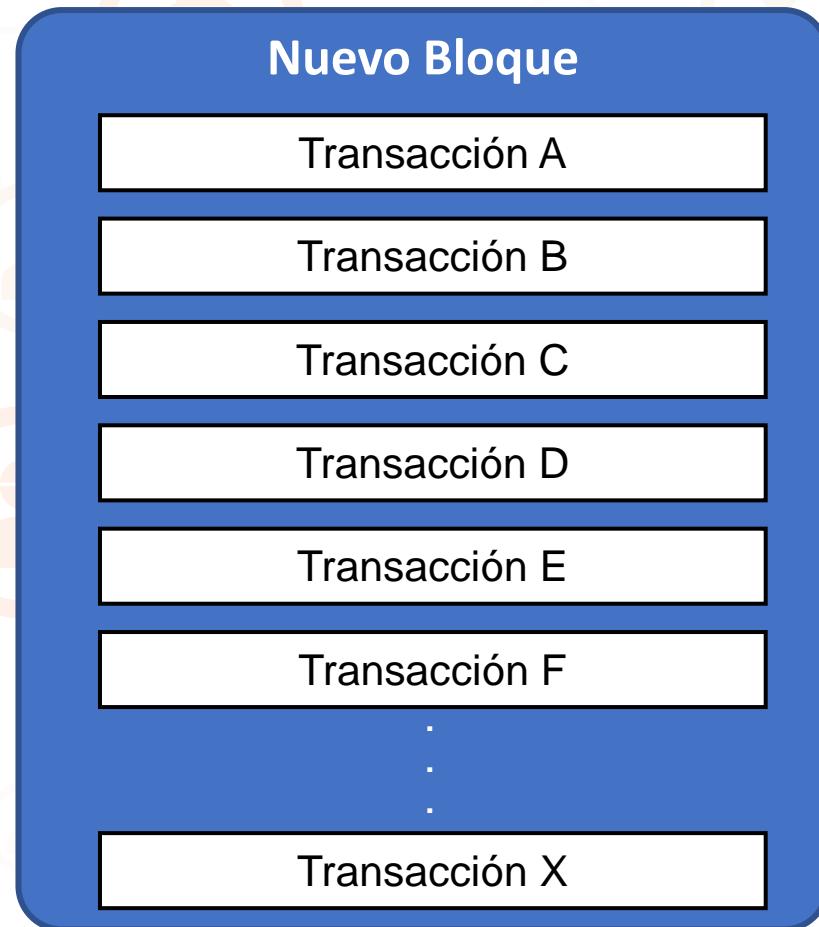
- Software nodo de red bitcoin
- Gratuito y de código abierto
- Proporciona una **billetera** de bitcoin que verifica completamente los pagos





Red P2P Bitcoin

Mineros y Minería





Red P2P Bitcoin

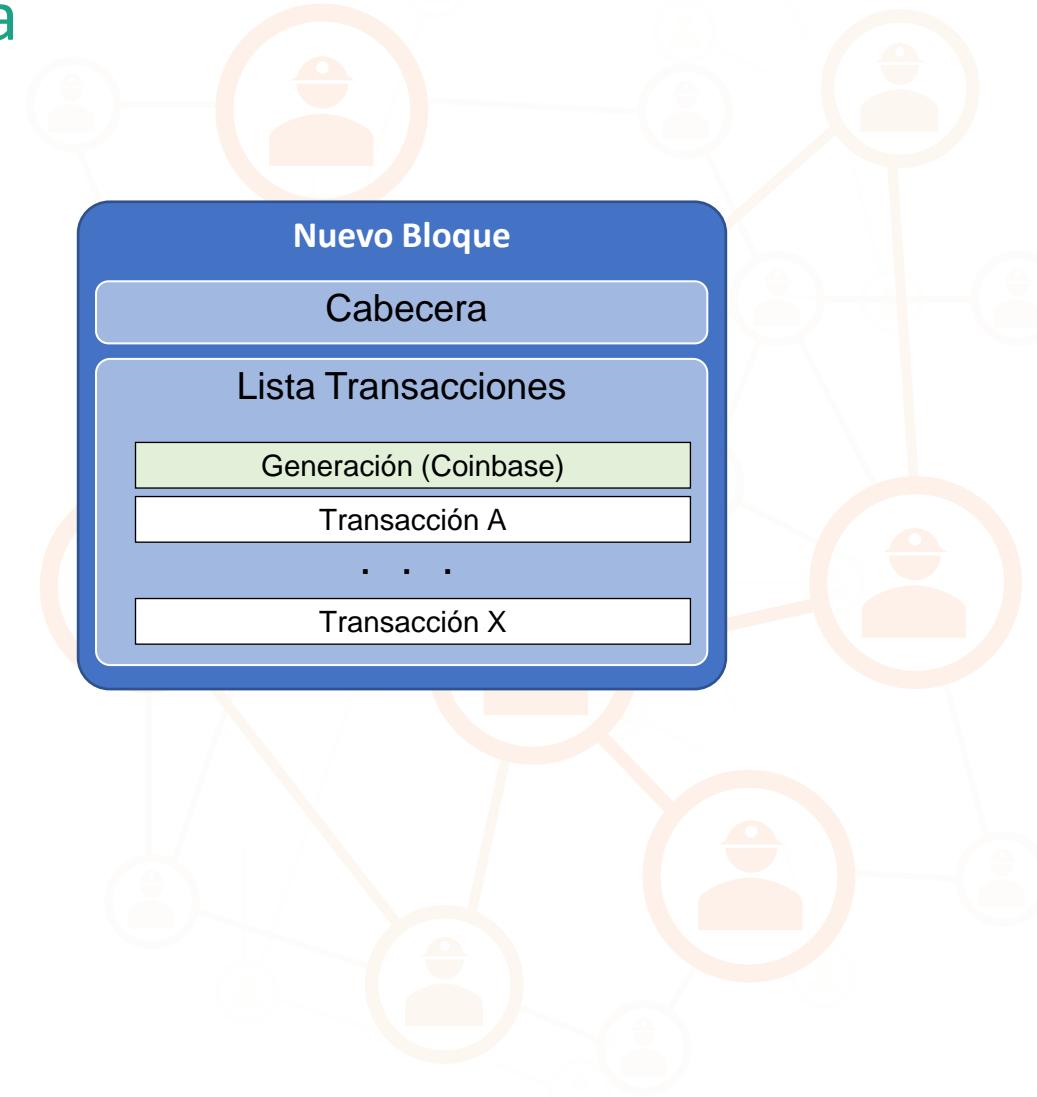
Mineros y Minería





Red P2P Bitcoin

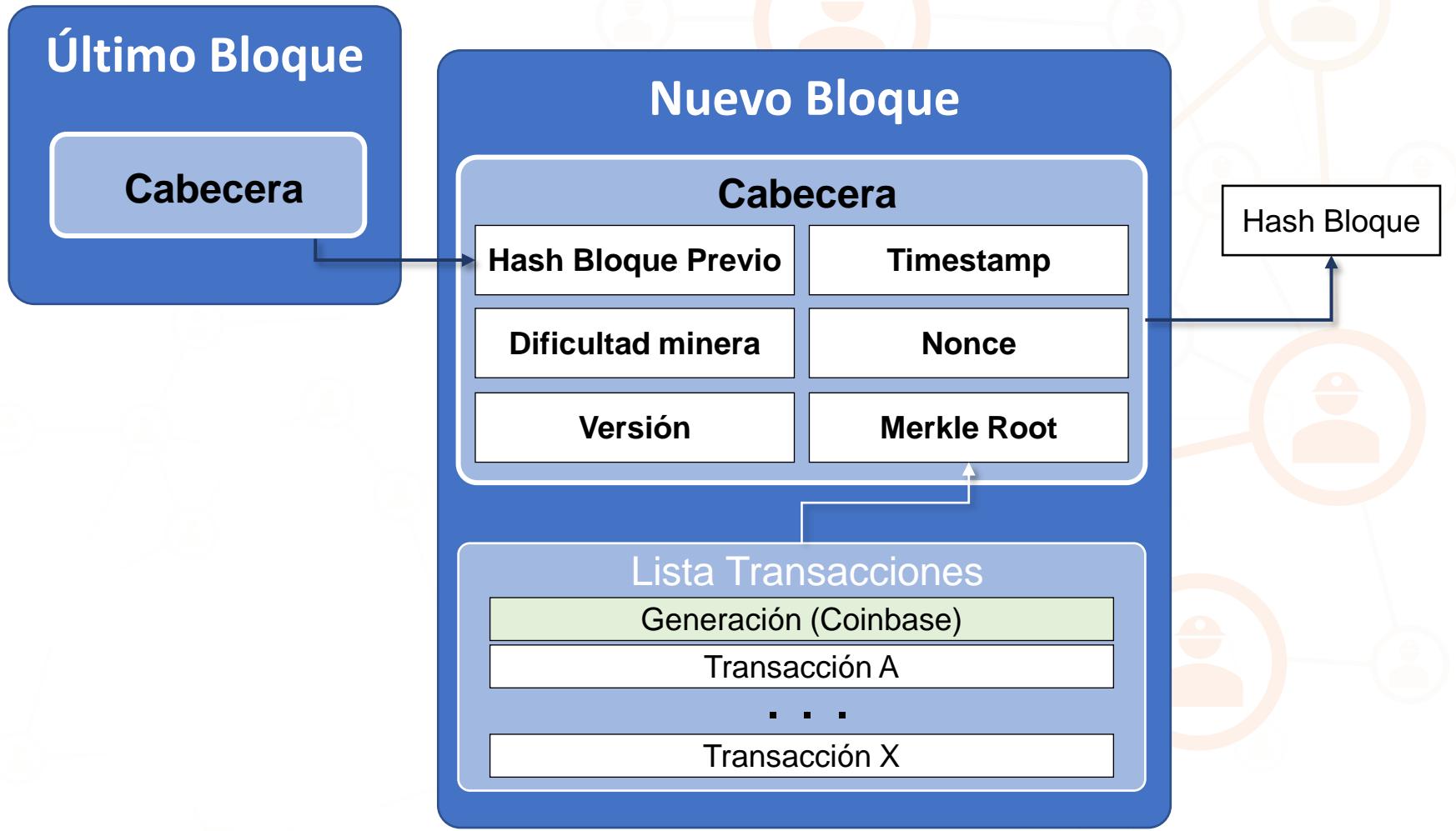
Mineros y Minería





Red P2P Bitcoin

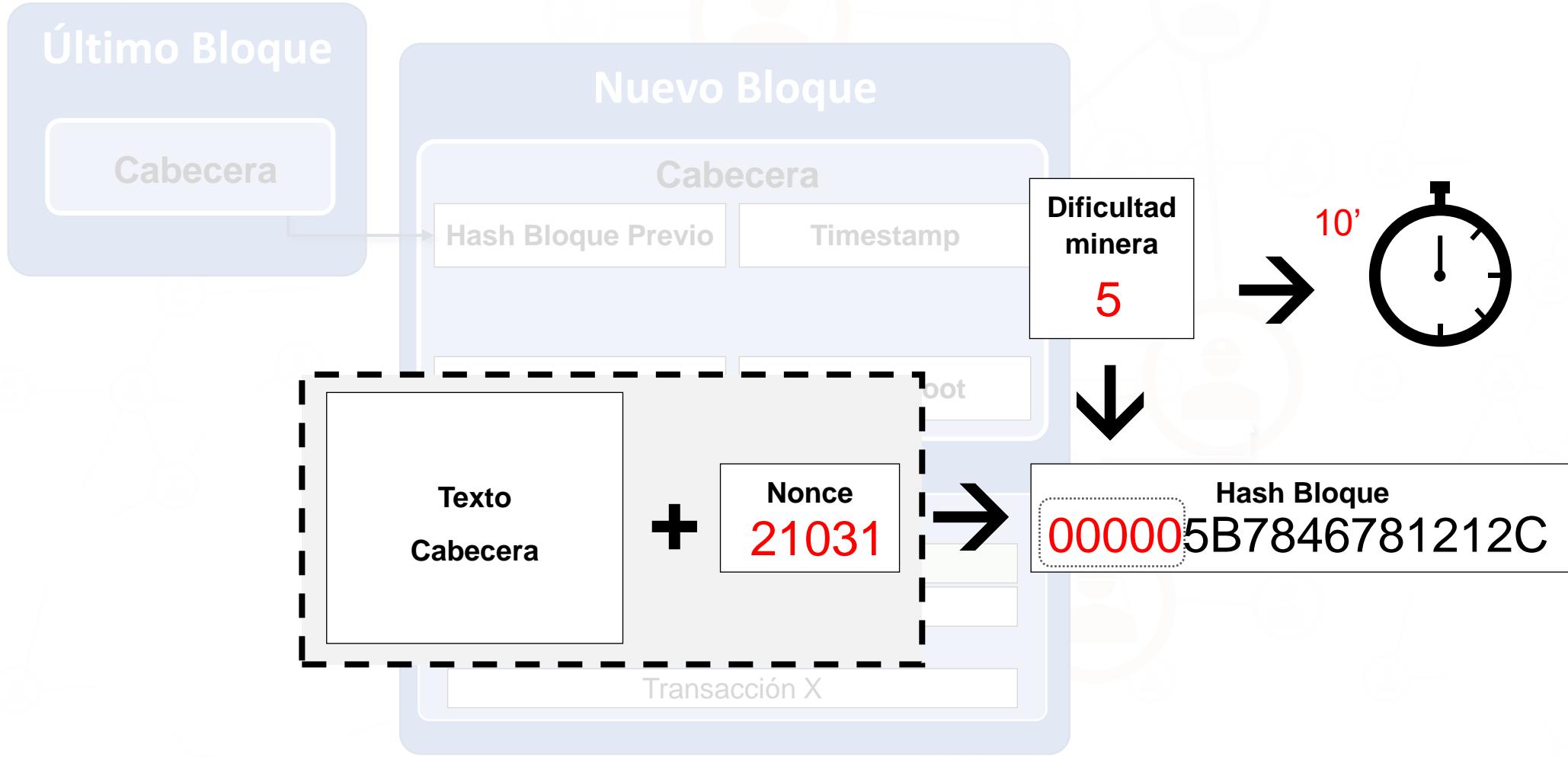
Minando un Bloque





Red P2P Bitcoin

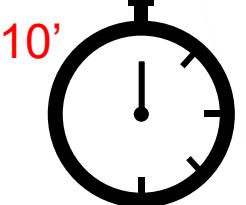
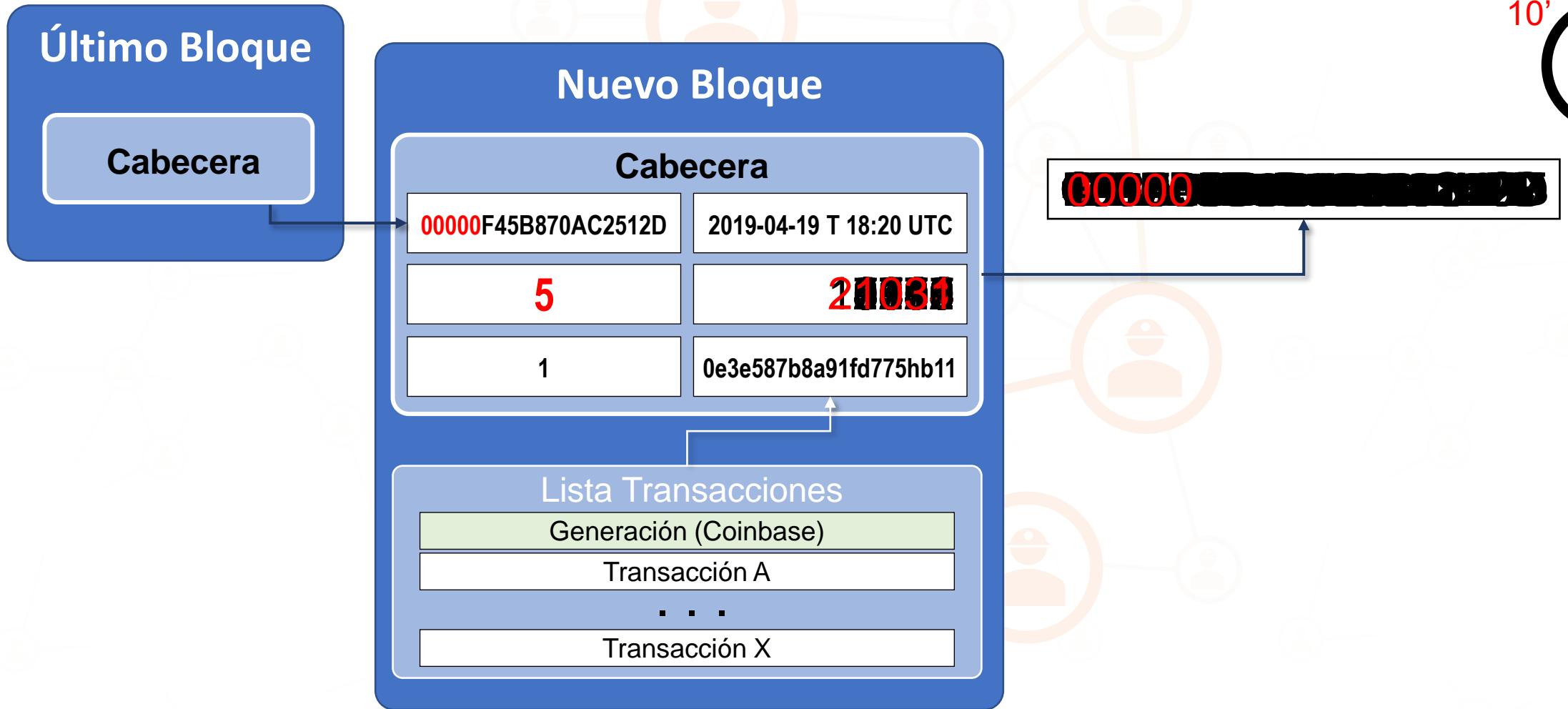
Prueba de trabajo Proof-Of-Work system





Red P2P Bitcoin

Prueba de trabajo Proof-Of-Work system





Red P2P Bitcoin

Mineros y Minería





Red P2P Bitcoin

Mineros y Minería





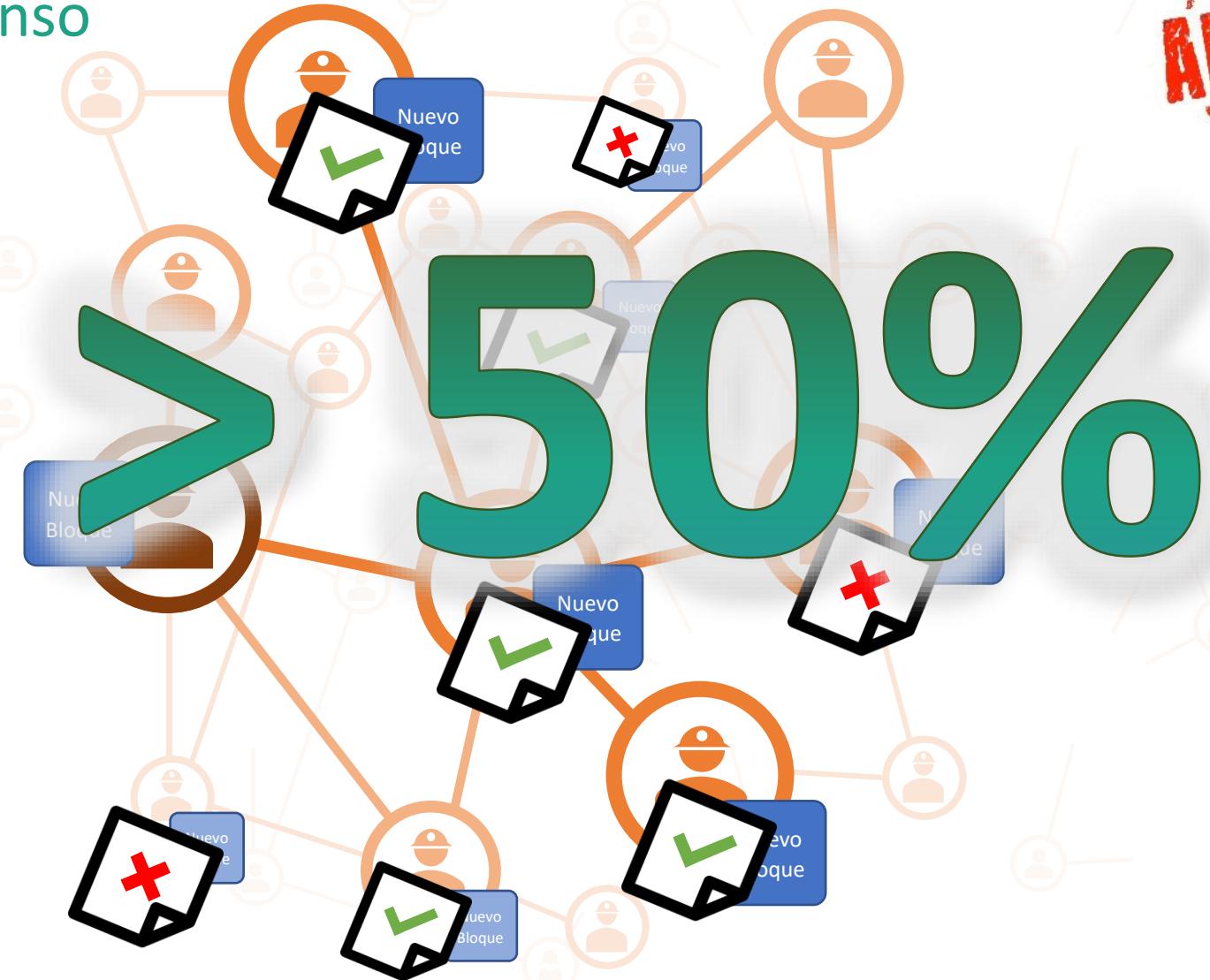
Red P2P Bitcoin

Minería y Consenso



Red P2P Bitcoin

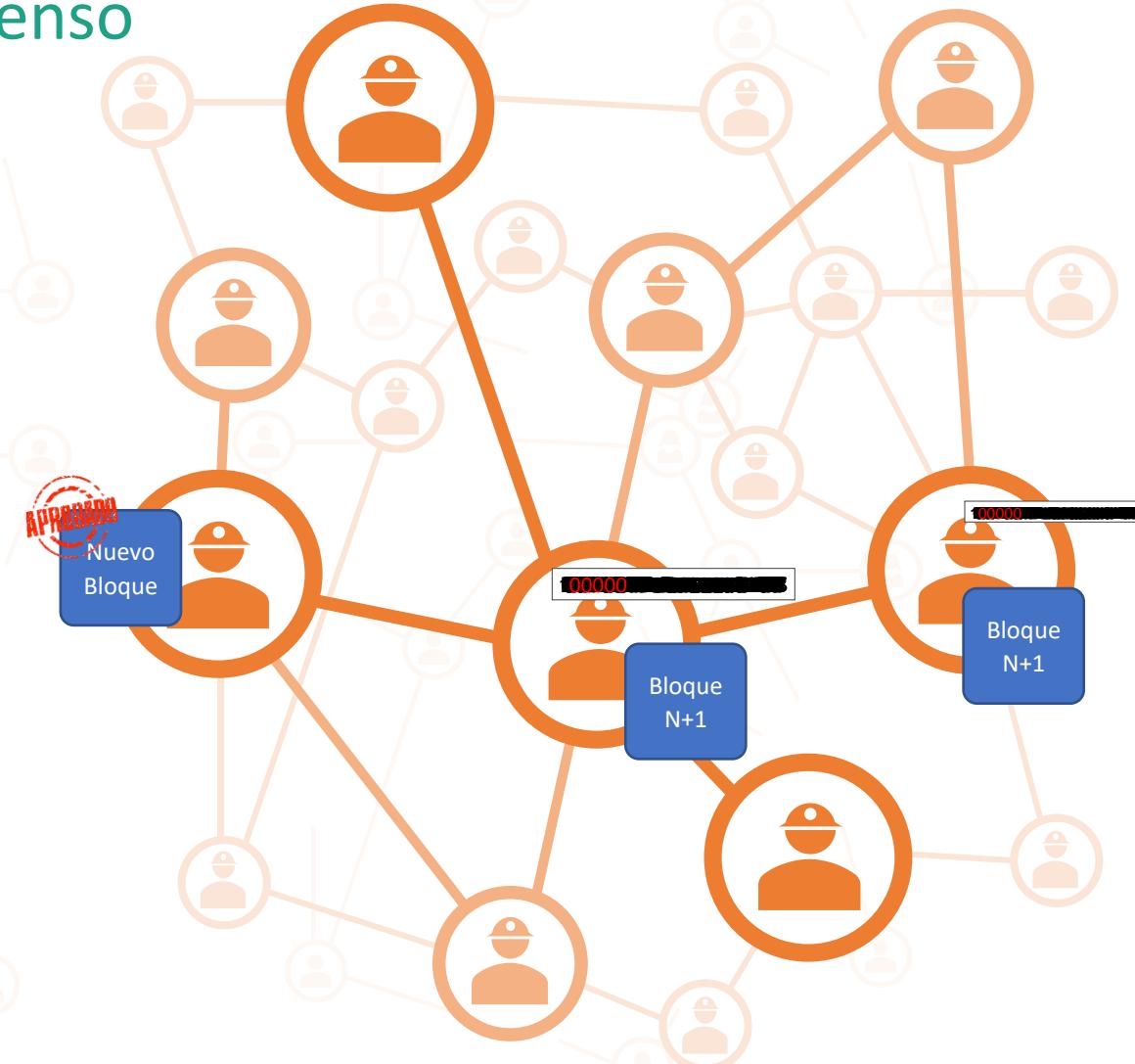
Minería y Consenso





Red P2P Bitcoin

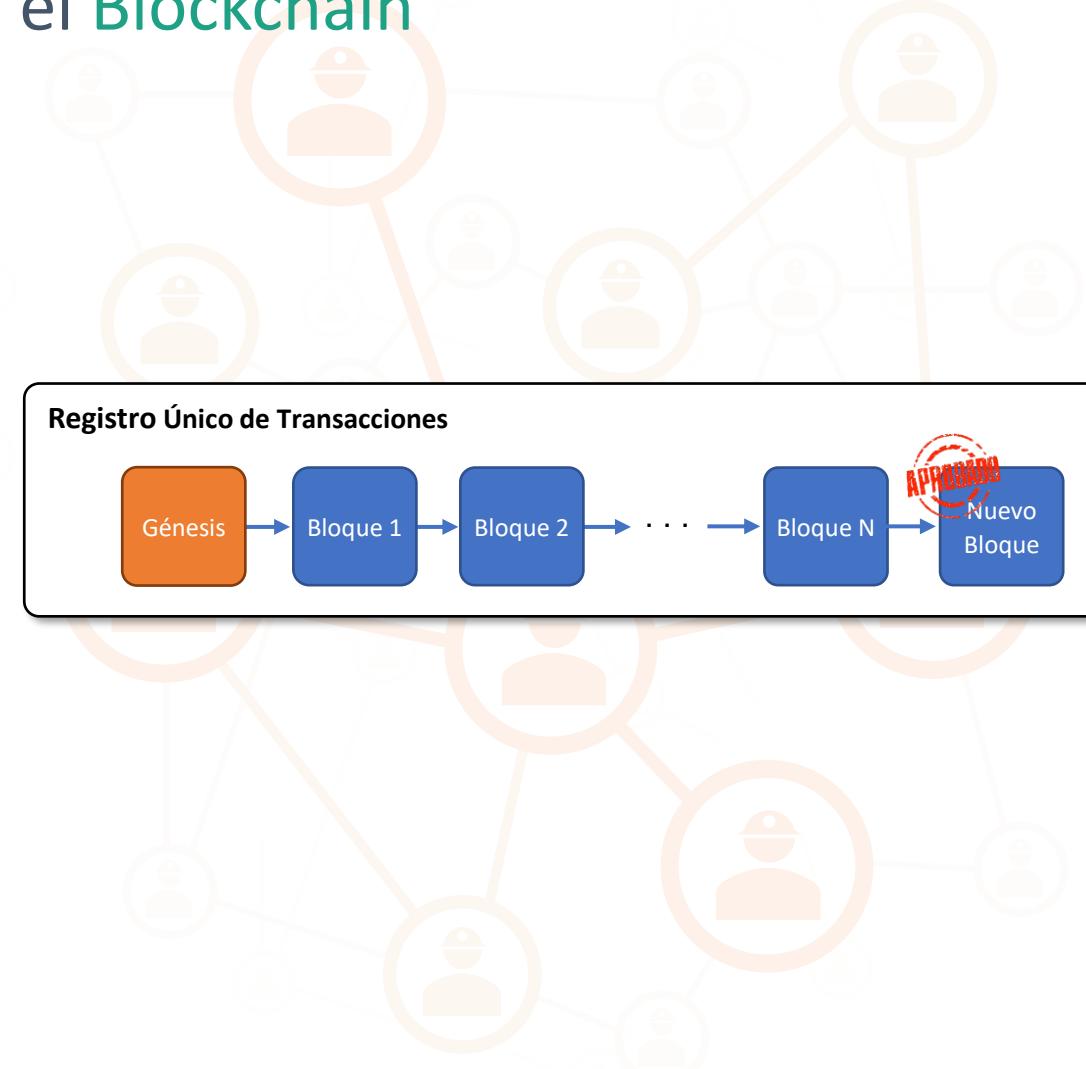
Minería y Consenso





Red P2P Bitcoin

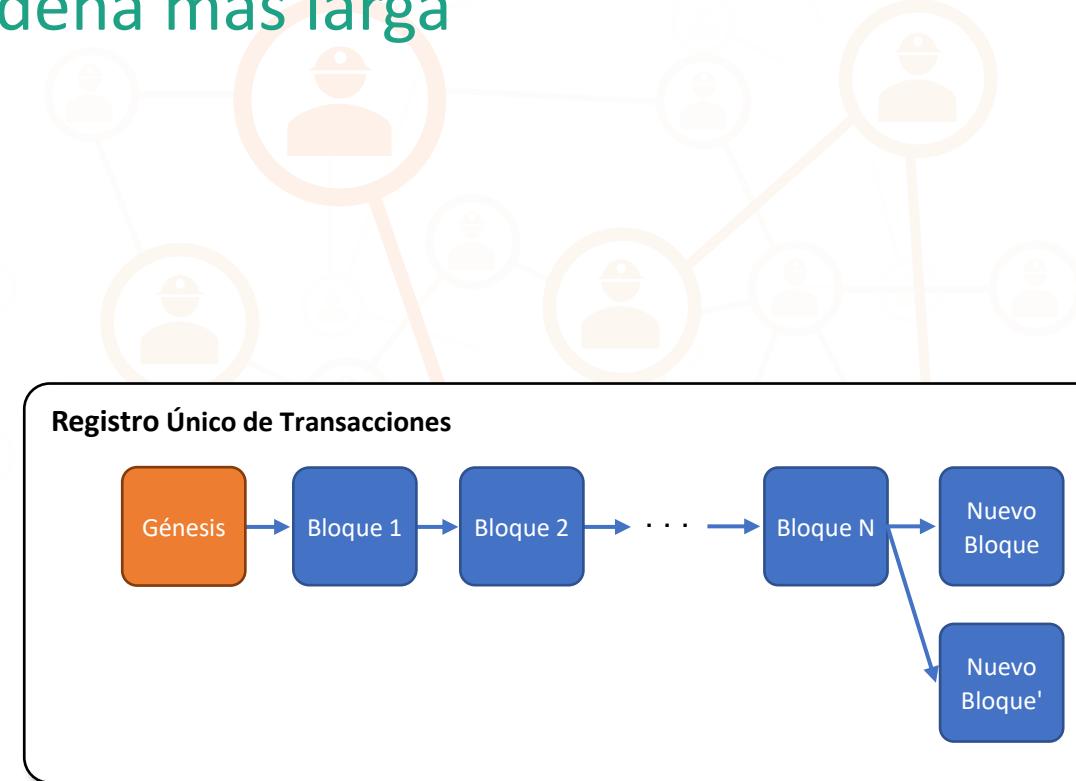
Nuevo Bloque en el Blockchain





Red P2P Bitcoin

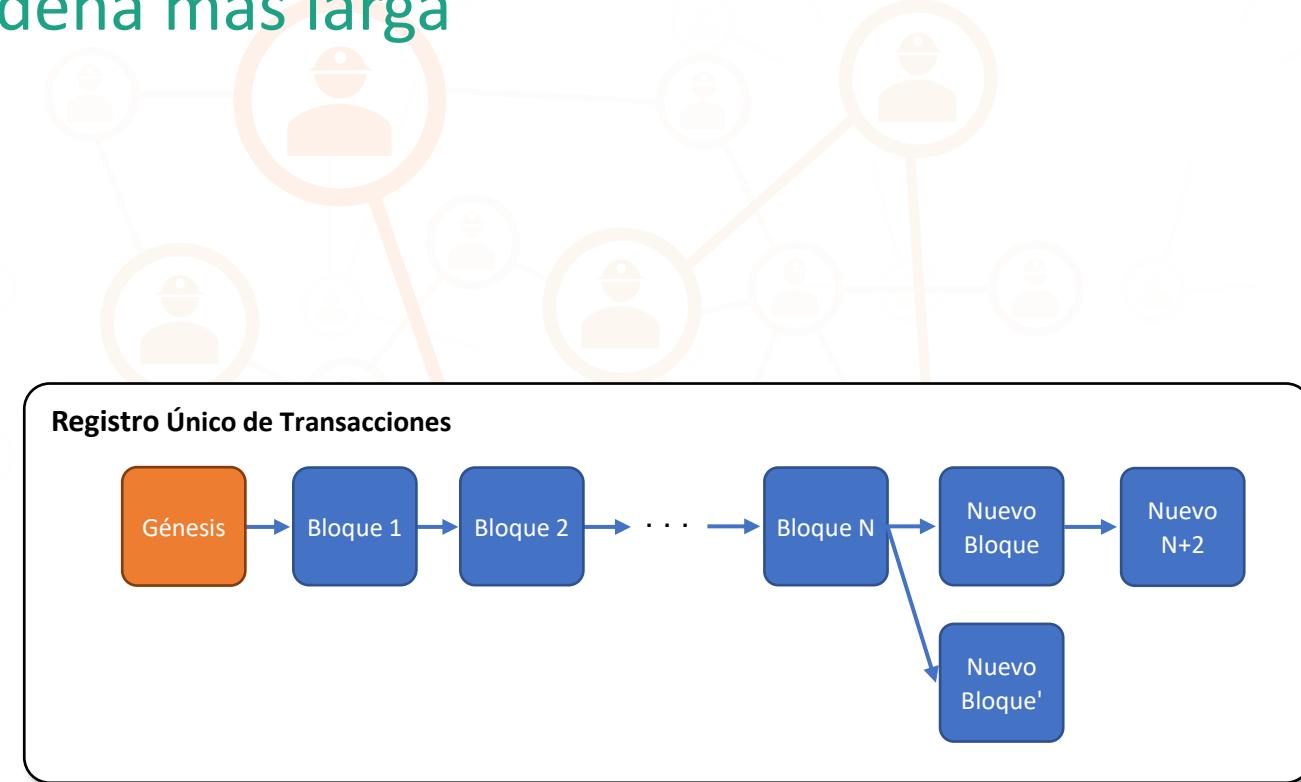
Conflictos y la Cadena más larga





Red P2P Bitcoin

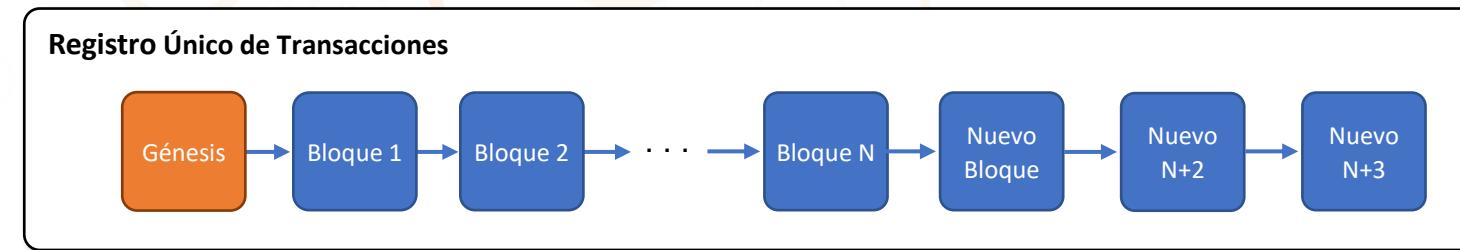
Conflictos y la Cadena más larga



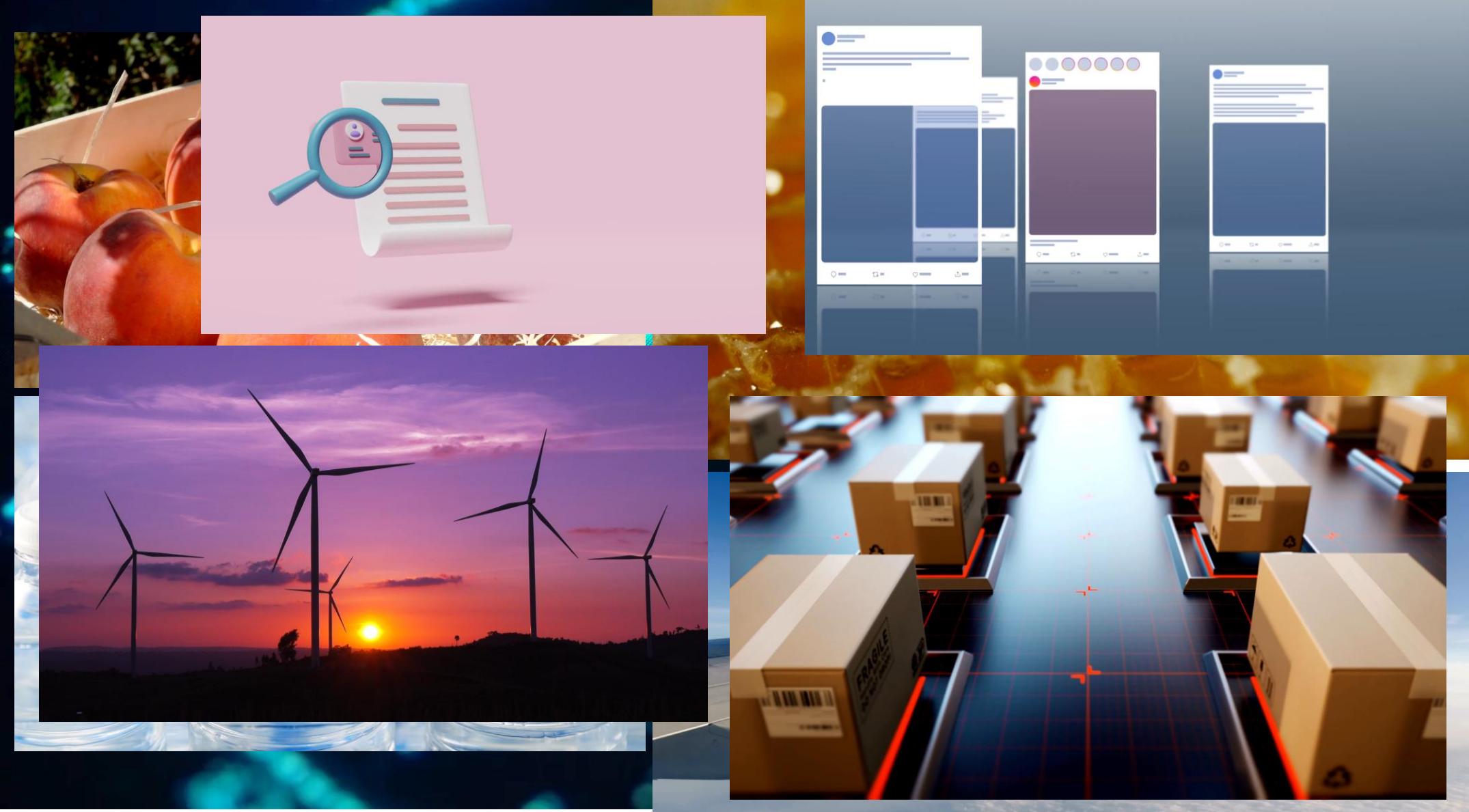


Red P2P Bitcoin

Conflictos y la Cadena más larga



Aplicaciones de Blockchain



Blockchain

Conclusiones

- 01 La **arquitectura descentralizada** de blockchain aumenta la resiliencia del sistema al **eliminar puntos únicos de fallo**
- 02 Blockchain utiliza **técnicas criptográficas avanzadas** para asegurar la **integridad** y la **confidencialidad** de los datos
- 03 Los **mecanismos de consenso**, como Proof of Work (PoW) o Proof of Stake (PoS), aseguran que todos los participantes en la red **acuerden el estado actual** de la cadena de bloques, lo que previene fraudes y manipulaciones

Conclusiones

- 04 Una vez que un **bloque** es **añadido** a la cadena de bloques, es **extremadamente difícil modificar la información** contenida sin alterar todos los bloques subsecuentes, lo que proporciona una **alta integridad** de los datos
- 05 A pesar de sus beneficios, blockchain enfrenta **desafíos** significativos en términos de **escalabilidad** y **rendimiento**.
- 06 Blockchain no solo es útil para las criptomonedas; su **aplicación** se extiende a diversas áreas como la **gestión de identidades**, el seguimiento de la **cadena de suministro**, el voto electrónico, y la gestión de registros médicos, ofreciendo **seguridad y transparencia**

Sistemas Operativos y Distribuidos

Iren Lorenzo Fonseca
iren.fonseca@.ua.es



TEMA 3. Sistemas Distribuidos.

Seguridad en Sistemas
Distribuidos