

Ciberseguridad

Grado en Ingeniería Informática

M6 - Tecnología blockchain

Bitcoin, 2009

Satoshi
Nakamoto

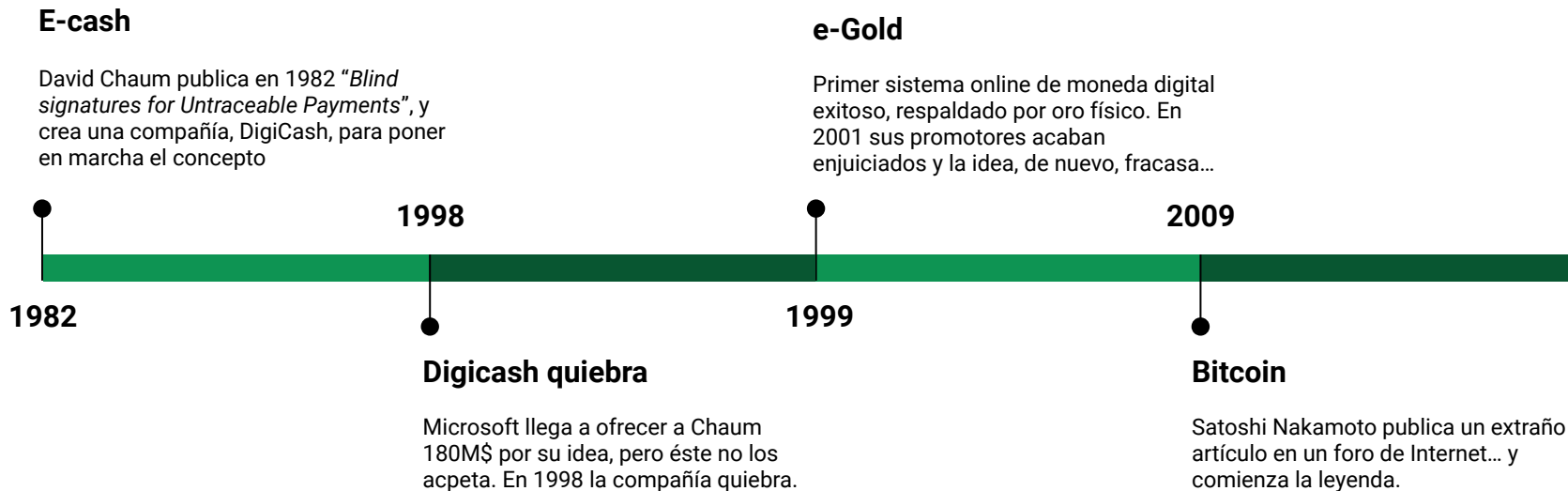


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Érase una vez...



Bitcoin es una red de pagos y una moneda digitales

Anónima

No
traceable

Transferencias
(casi) inmediatas

Comisiones
reducidas (?)

Descentralizada

Creada en
2009

Se ha convertido en...



¿Qué hace esta idea diferente?

No **autoridad
central**

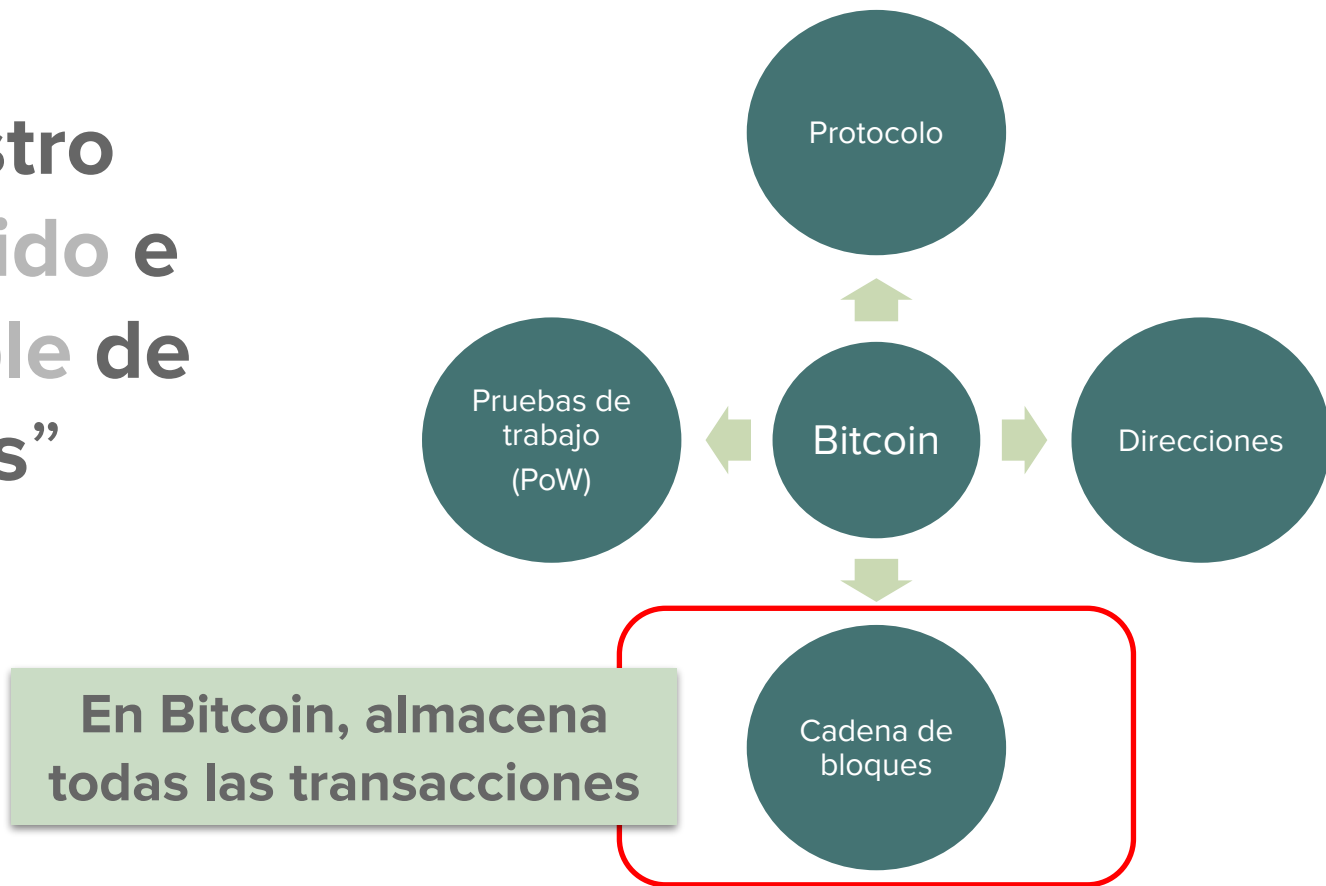
=

No fallo,
no corrupción,
no prohibición

CADENAS DE BLOQUES

¿Qué son?

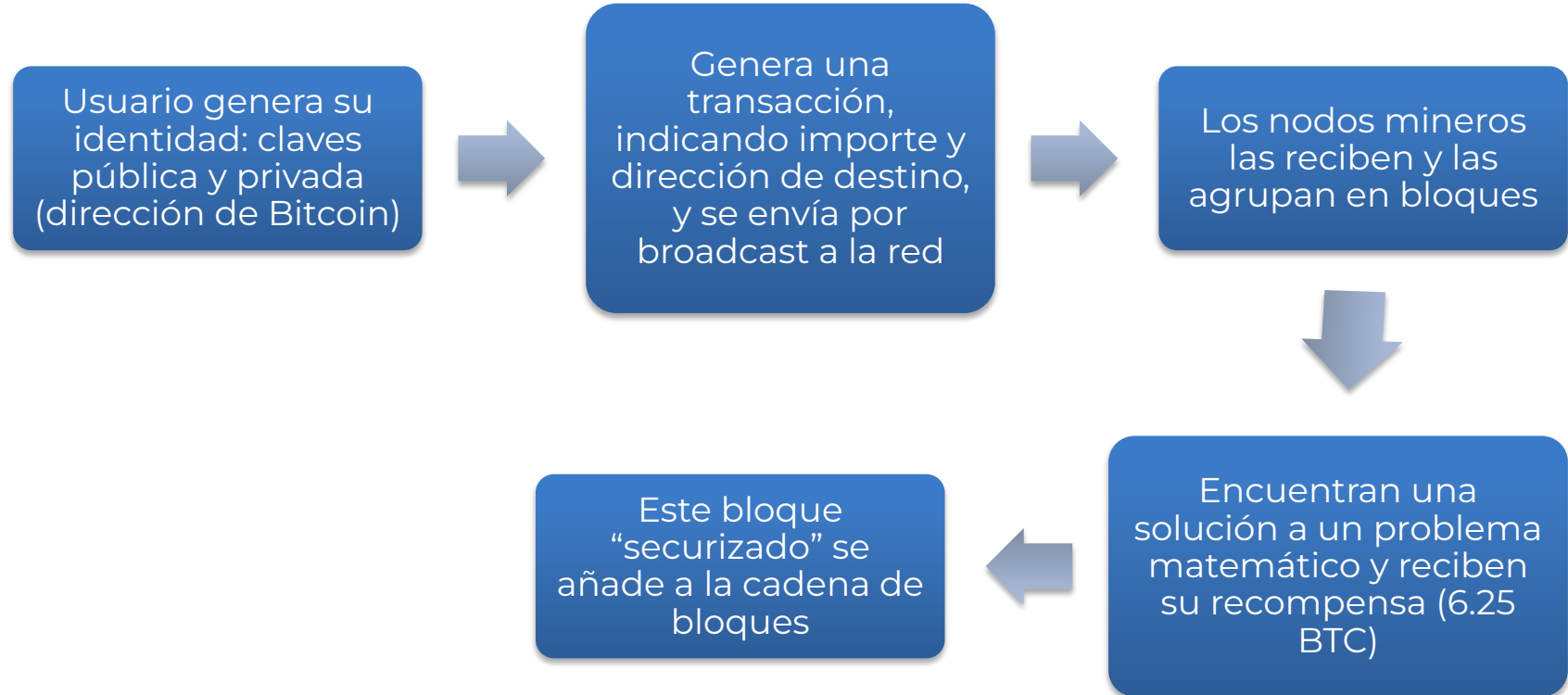
**“Registro
distribuido e
inmutable de
datos”**



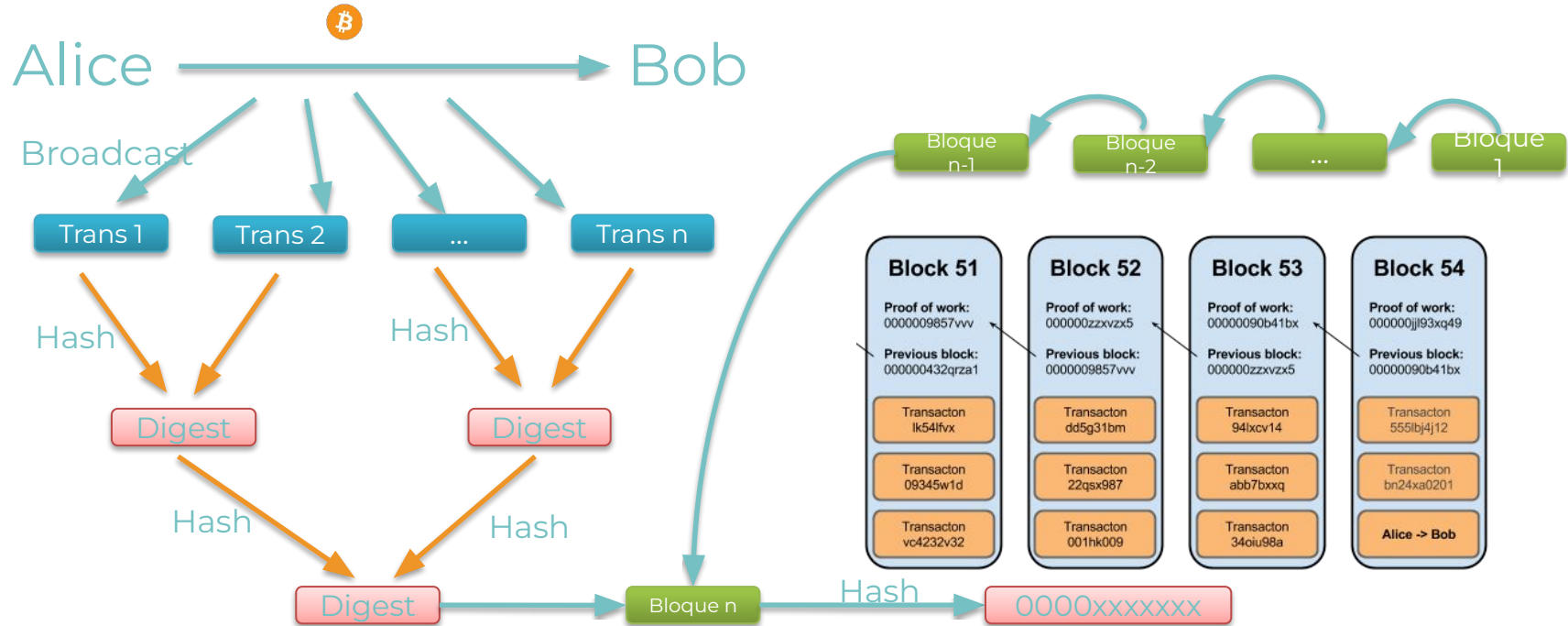
CADENAS DE BLOQUES

¿Cómo funcionan?

Protocolo



Cadena de bloques




Proof-of-work (minado)

Premisa: sistema descentralizado →
NO autoridad ni BD central



Solución: copias de la BD en cada
nodo (blockchain)



Problema: ¿cómo mantener la
coherencia?



Solución: mecanismo de consenso
distribuido → *prueba de trabajo* →
demuestra interés en el bien común

Proof-of-work

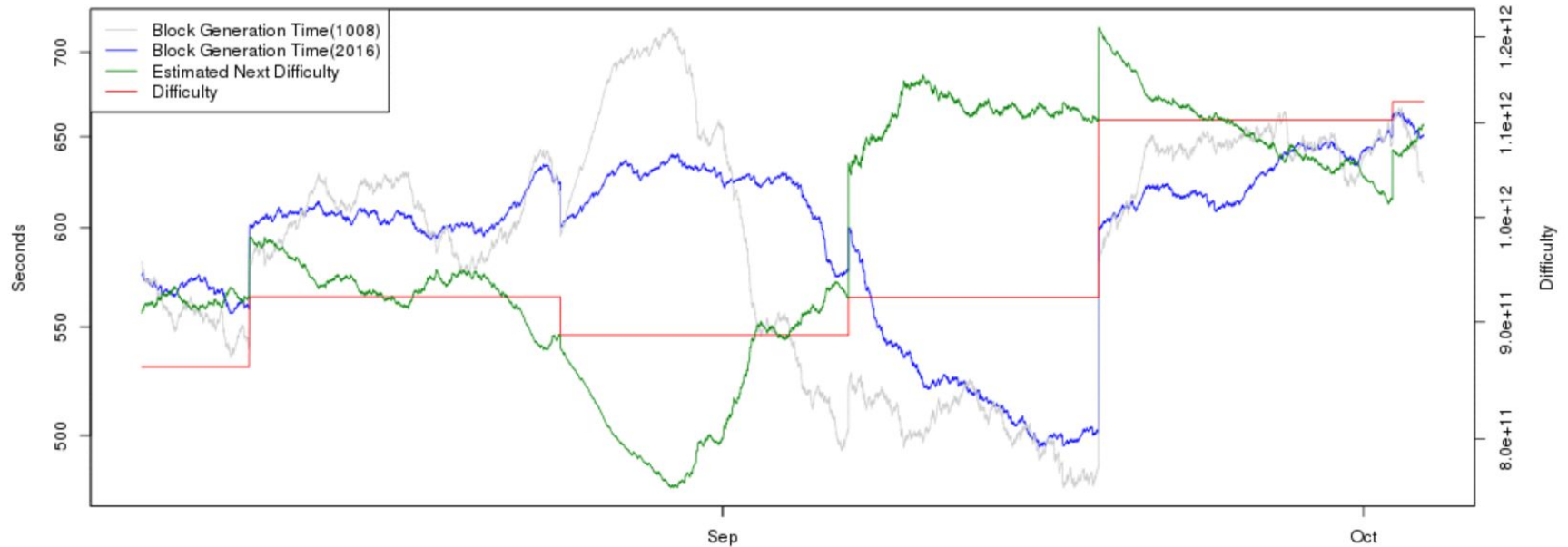
- Prueba matemática de que hemos dedicado una cantidad de tiempo y trabajo computacional a resolver una tarea

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfd65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

- Inversión parcial de hash
- Sirve, también, para ajustar la dificultad (origen de los 10 minutos)

Proof-of-work

Bitcoin Block Generation Time vs Difficulty



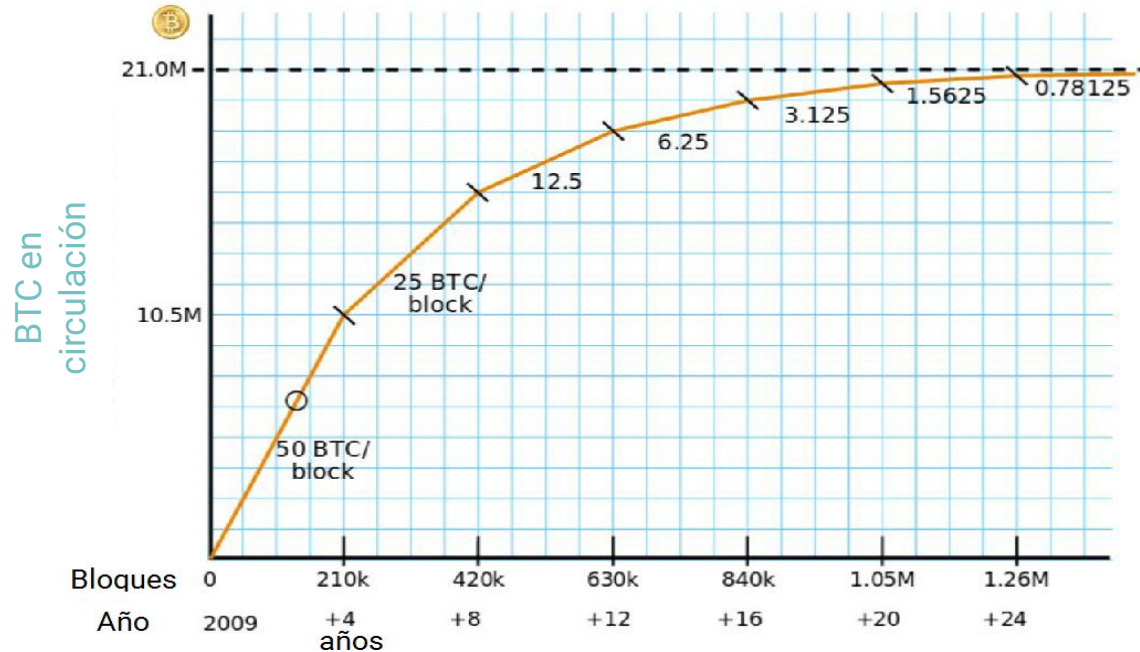
Proceso de minado



¿Por qué es necesario?



Evolución futura de los costes por transacción



Actualmente,
la **recompensa**
por bloque
produce más
del 99%
beneficio de un
minero

Carteras

Exchanges

- También permiten la compra de criptomoneda con moneda fiduciaria

X No tenemos control

Carteras locales

- Necesario descargar toda la cadena de bloques (~430Gb)

X Pueden perderse

Carteras offline (“frías”)

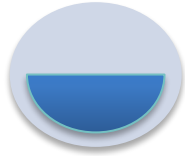
- Papel
- Dispositivos específicos

X Incómodas
✓ Más seguras (teóricamente)

Unidades BTC

Unit	Abbreviation	Decimal (BTC)
Algorithmic Max	-	20,999,999.9769 ^[1]
megaBitcoin	MBTC	1,000,000
kiloBitcoin	kBTC	1,000
Original Block Reward	-	50
Current Block Reward	-	25
decaBitcoin	daBTC	10
Bitcoin	BTC	1
deciBitcoin	dBTC	0.1
centiBitcoin	cBTC	0.01
milliBitcoin	mBTC	0.001
microBitcoin	μBTC	0.000001
Finney ^[5]	-	0.0000001
satoshi	-	0.00000001

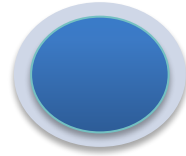
Blockchain - Resumen



Orígenes

Tecnología
“auxiliar” de
Bitcoin

Contiene TODAS
las transacciones
del sistema
desde 2009



Características

Garantiza la
integridad de los
datos, utilizando
mecanismos de
consenso
distribuido

Ejercicio 1

En este ejercicio, vamos a empezar a tomar contacto con la cadena de bloques de Bitcoin. Para ello utiliza algún explorador de la misma, como **www.blockchain.info**, y responde a las siguientes preguntas:

1. En las últimas 24 horas, averigua estas cantidades:
 - a. Tiempo medio entre bloques
 - b. Número total de transacciones
 - c. Volumen de negocio, en dólares.
2. En las últimas 24 horas, ¿cuál ha sido el tamaño medio del bloque? ¿Y el máximo absoluto? ¿A qué es debido?

CADENAS DE BLOQUES

Taxonomía

Blockchains públicas, semi-públicas y privadas

Tipo de cadena	Permiso		Tipo consenso	Usos	Plataformas
	Lectura	Escritura			
Pública	✓	✓	PoW	Notaría digital, IoT	Bitcoin, Ethereum (PoS)
Semi-pública	✓	✗	PoW, PoS	Certificación cadenas productivas	Ethereum
	✗	✓		Auditoría	Hyperledger, Quorum (!)
Privada (Consortios)	✗	✗	PoA	Sistema de pagos interbancarios, otros (?)	

Proof-of-stake

Mecanismo de consenso **alternativo** a PoW:

“El **creador** del próximo bloque se elige con probabilidad **proporcional** al stock de moneda cada usuario”

Proof-of-stake // Pros - con



+

No hay minado:
enorme ahorro
energético,
simplificación del
sistema

Ethereum
implementó este
mecanismo hace
unos meses



-

Mecanismo
elitista:

- Mínimo stock para “votar”, 32 ETH
- Cuanto más tienes, más posibilidades tienes de recibir la recompensa

Proof-of-Authority

- Nodos identificados y pre-autorizados (certificados digitales)
- Un nodo *validador* rotatorio autoriza las transacciones
- ¡No hay incentivo económico!
- Caso **Alastria**

Proof-of-Authority // Pros - con

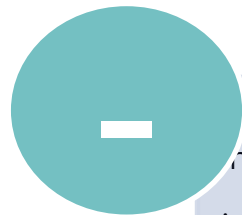


Blockchain
privada

Todos los nodos
se conocen entre
sí

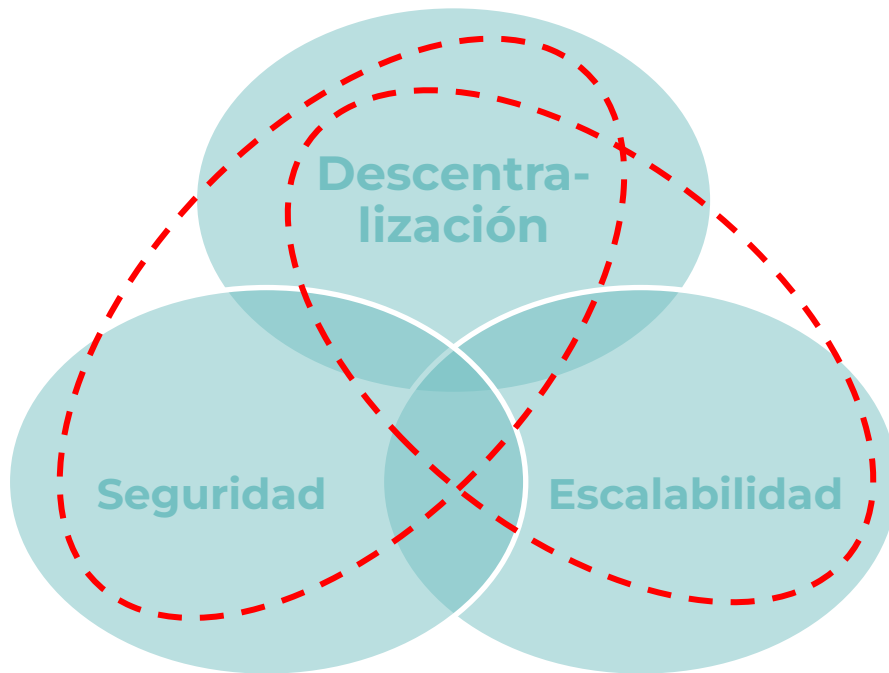
El consenso se
mantiene sin
minado

Puede cifrar las
transacciones y
smart contracts,
opcionalmente



Si el número de
nodos es bajo o se
concentran los
intereses, se facilita
mucho el ataque
del 51%
¡Colusión!

El trilema de las cadenas de bloques



Las cadenas de bloques solo pueden tener simultáneamente dos de estas propiedades

¿Públicas o privadas?

Tipo de cadena	Tipo consenso (¿Colusión?)	Modelo de incentivo	Modelo de gobernanza
Pública	Difícil, con la actual potencia computacional	Criptomoneda	No es necesario
Semi-pública	Puede ser fácil, dependiendo del número de actores y, sobre todo, sus intereses	Normalmente no existe (intento de Libra)	Debe ser definida externamente
Privada (Consortios)		No existe	

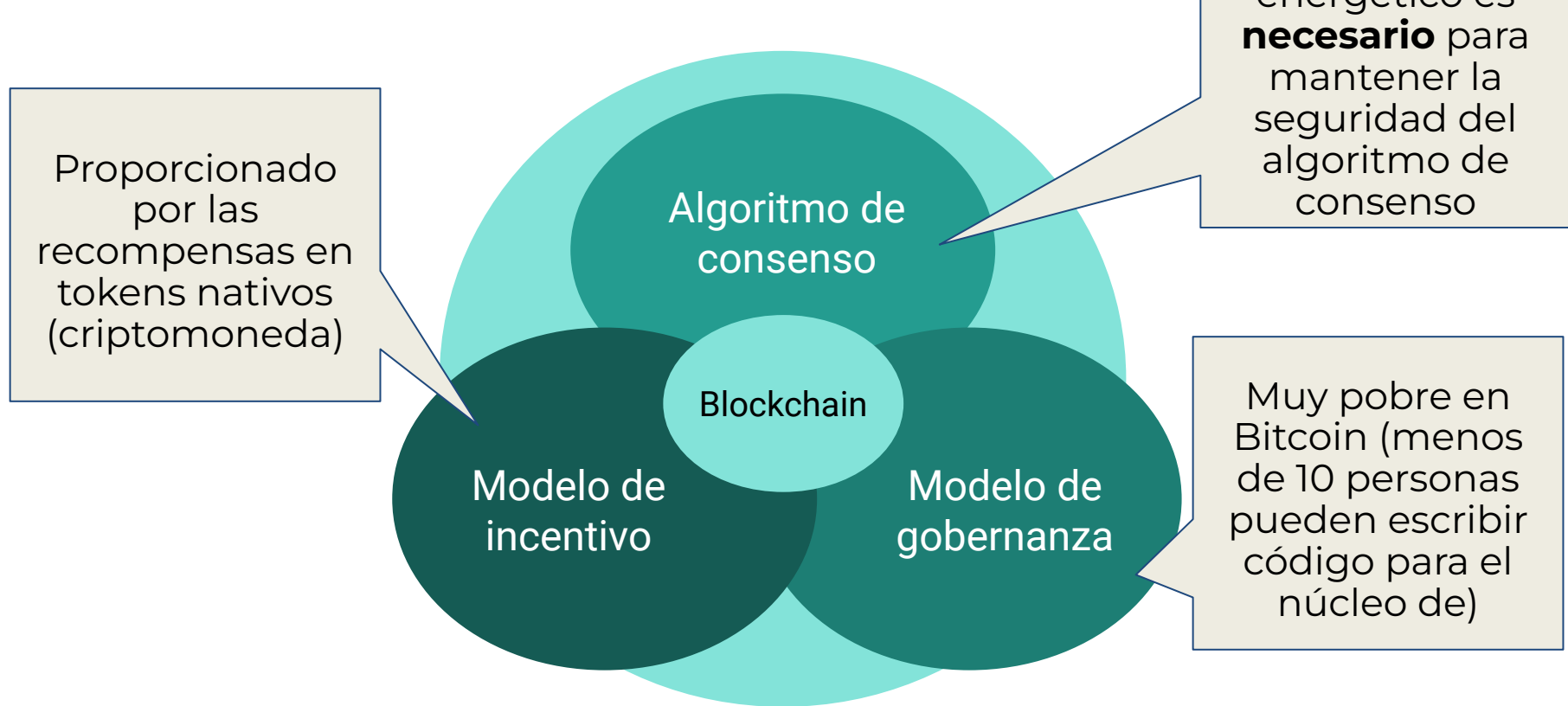
¿Públicas o privadas?

“Una **cadena de bloques** (pública o privada) aplica en aquellos escenarios donde haya actores con distintos **intereses**. Si no, es simplemente una BD distribuida muy cara”

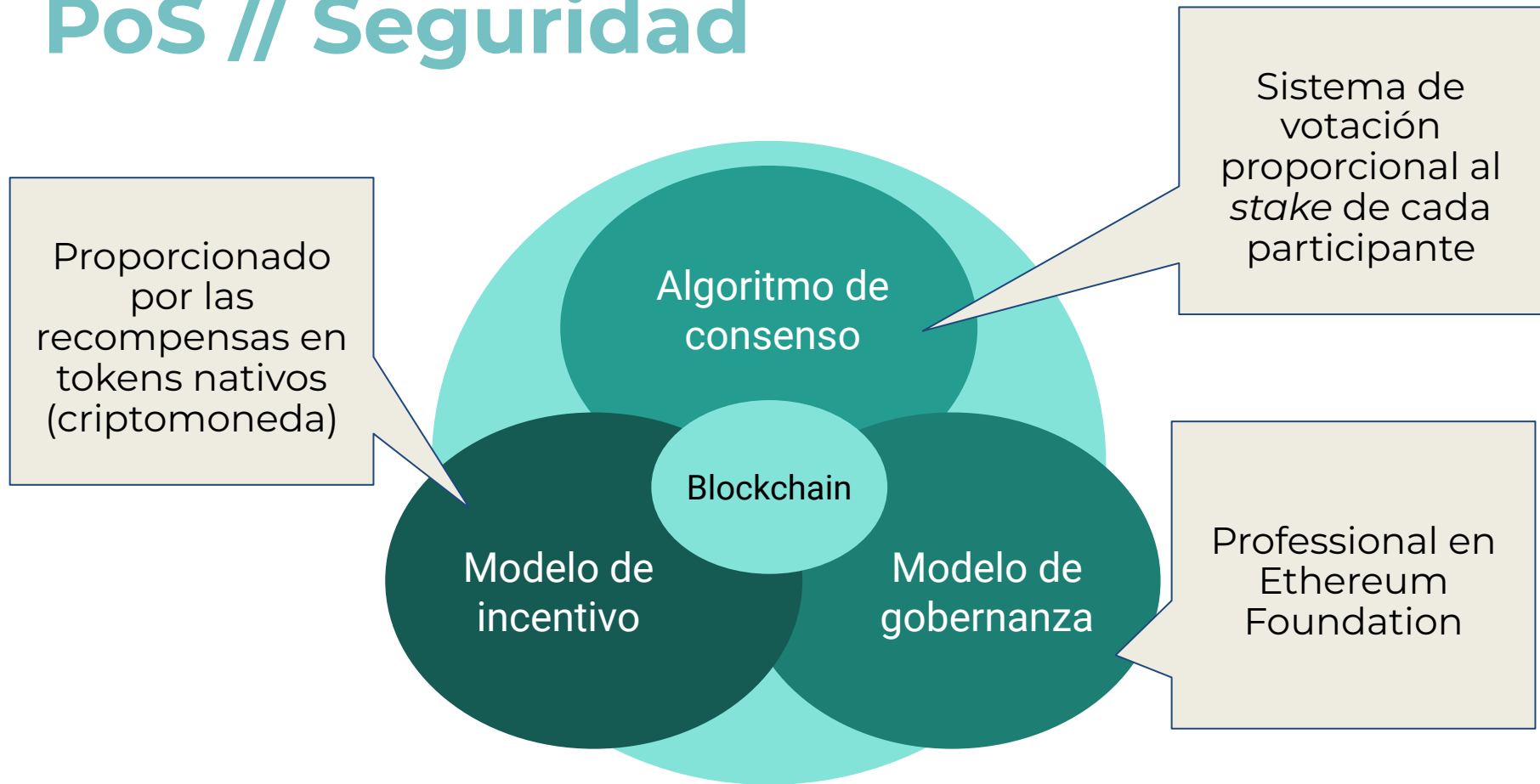
CADENAS DE BLOQUES

Seguridad

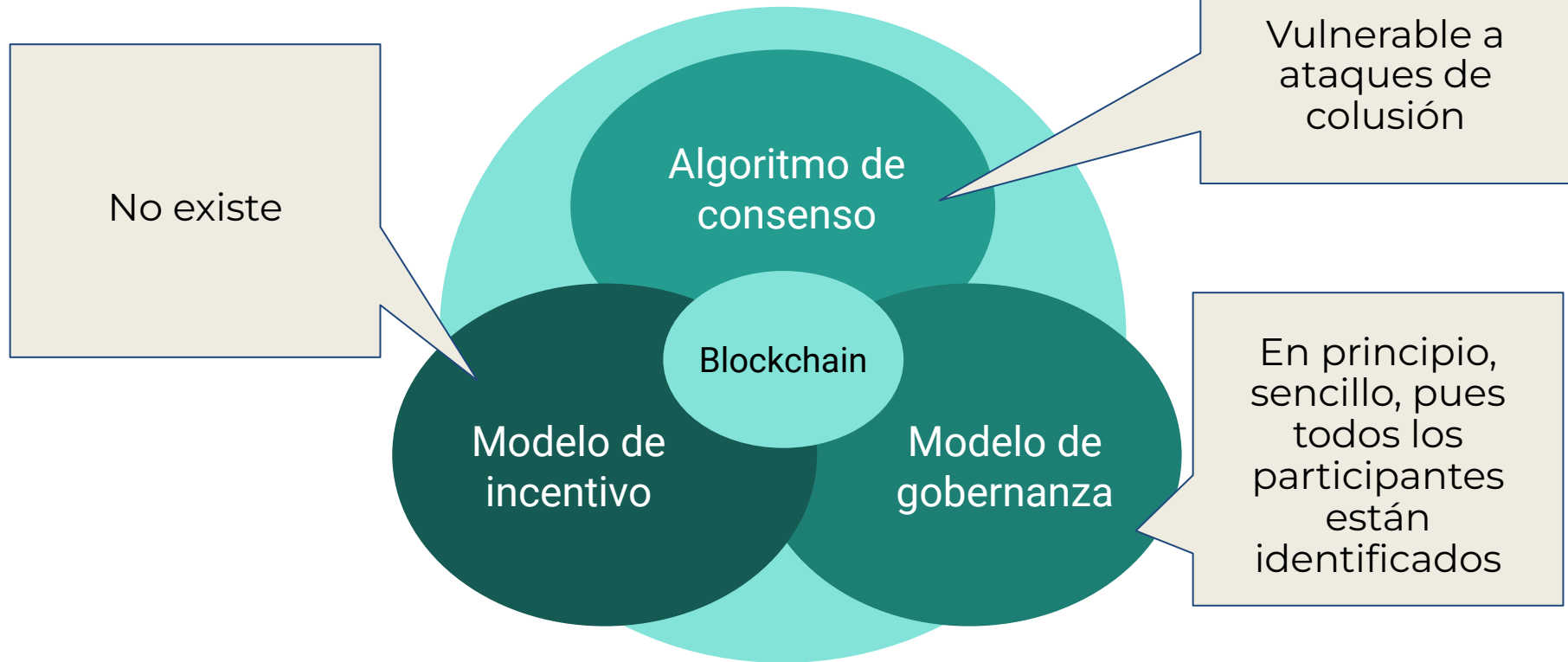
PoW // Seguridad



PoS // Seguridad



PoA // Seguridad



CADENAS DE BLOQUES

Casos de uso



Sector
financiero



Certificación de
información



Tokenización
de activos

Internet de las
Cosas





Sector
financiero



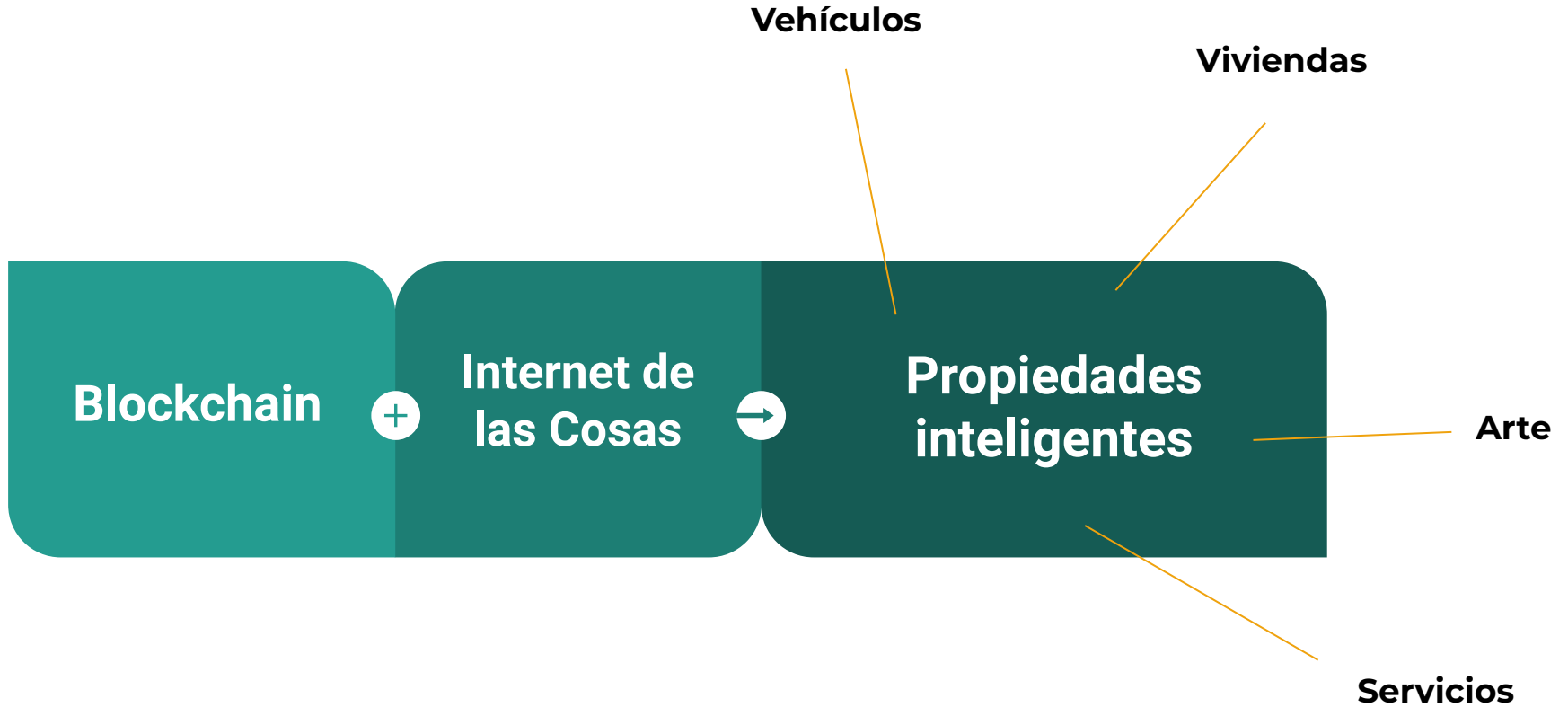
Notaría digital

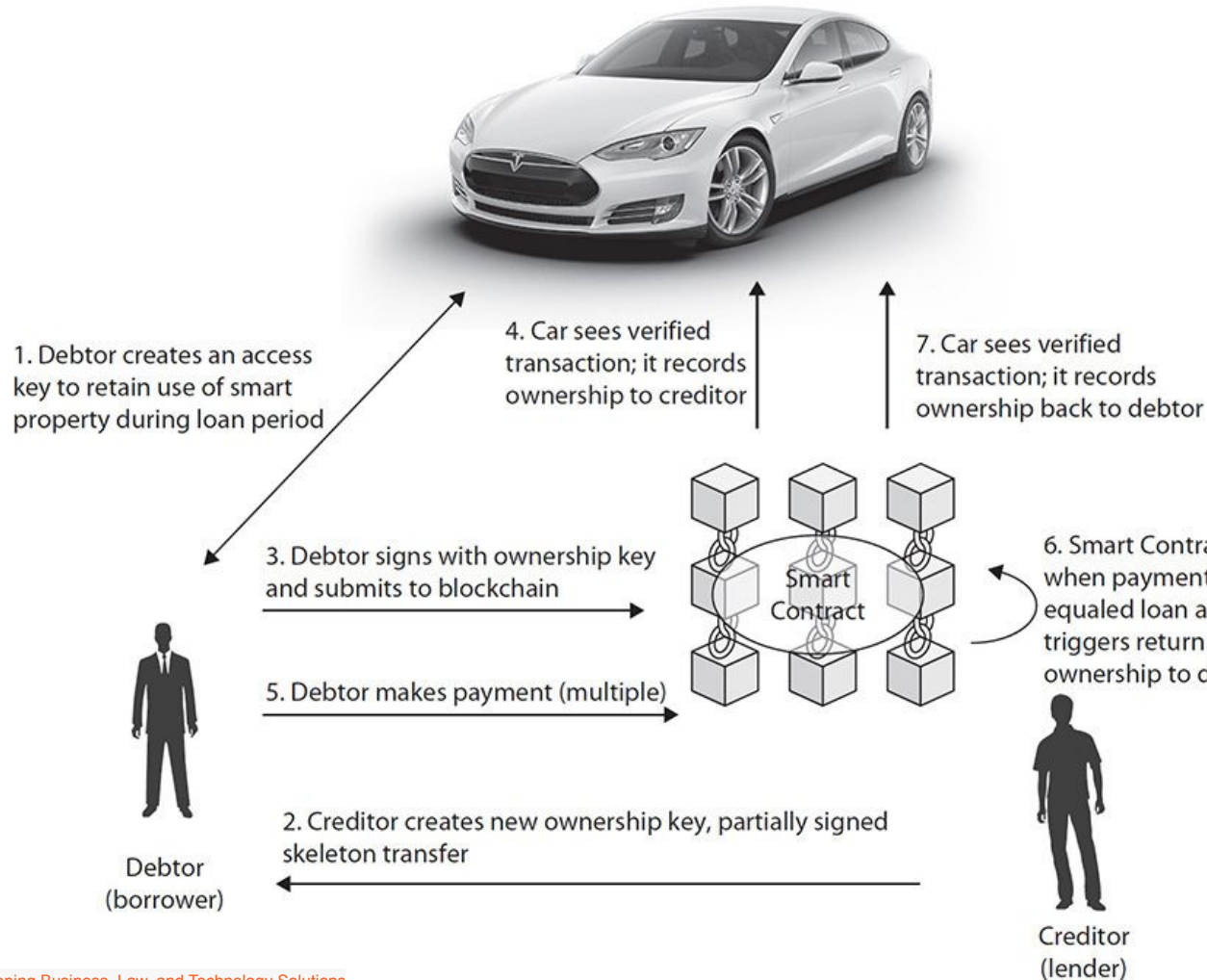


Tokenización
de activos

Internet de las
Cosas

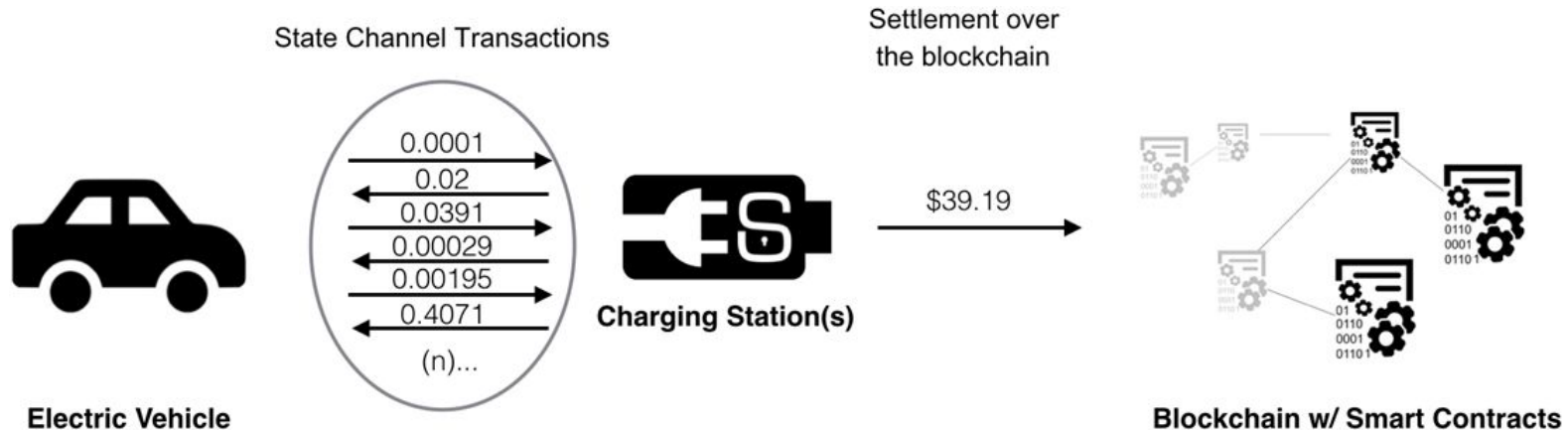






Cargador eléctrico - Vehículos

Micropagos (de verdad)



Aplicaciones en IoT

