BLOCKCHAIN Y CONTRATOS INTELIGENTES

Joel A. Gómez Treviño

Presidente Fundador de la Academia Mexicana de Derecho Informático
Coordinador del Comité de Derecho de las TIC y Datos Personales de ANADE
Profesor de Posgrado de la Universidad Panamericana Campus Guadalajara
Socio Director de Lex Informática Abogados, S.C.

REVOLUCIONES INDUSTRIALES

@JoelGomezMX

Tecnología

Mecánica

Conocimiento Intelectual

Pre-Revolución Industrial

- Antes de 1730
- **Economía rural** basada fundamentalmente en la **agricultura** y el **comercio**.

1ª Revolución Industrial

- 1730-1850
- Gran Bretaña
- Energía: **Carbón**
- Sector Industrial: Textil y Metalurgia.
- **Economía de carácter urbano**, industrializada y mecanizada.
- Concentración de capitales.

2ª Revolución Industrial

- 1870-1940
- Europa, USA y Japón
- Energía: **Gas, electricidad y Petróleo**
- SI: Siderometalurgia, química y transporte.
- Nuevos sistemas de transporte (avión y automóvil) y comunicación (teléfono y radio).

3ª Revolución Industrial

- 1960-2000
- Se asienta sobre nuevas **tecnologías de la información** y la comunicación, así como en el desarrollo de energías renovables.
- Se le conoce como “la revolución digital o de la ordenador”.

3A REVOLUCIÓN INDUSTRIAL

Breve historia de internet.

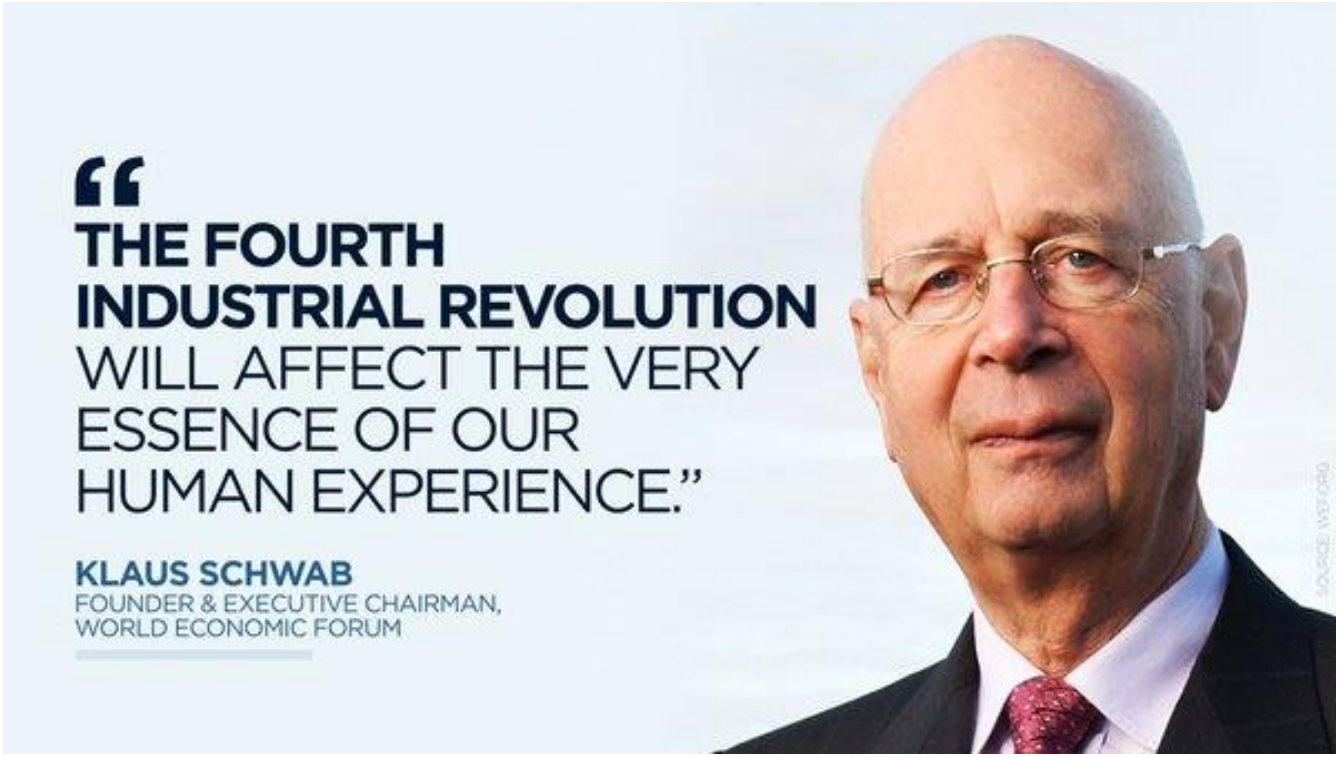
- En **1969** se envió el **primer mensaje a través de la red de computadoras** ARPANET, entre las Universidades de California en Los Ángeles y el Instituto de Investigación de Stanford.
- En **1971** se envió el **primer correo electrónico**.
- En **los setentas Intel desarrolló el primer microprocesador** que sentó las bases para la revolución de las **microcomputadoras**.
- En los **ochentas** fue posible **convertir tecnología que estaba en formato análogo a formato digital**.
- En **1981** se define el protocolo TCP/IP y la palabra «Internet».
- En **1984** había 1,000 computadoras conectadas.
  - 1989 > 100,000 de computadoras conectadas
  - 1992 > 1,000,000 de computadoras conectadas
  - 1996 > 10,000,000 de computadoras conectadas
- En los **noventa** (**1991**) nace la **WWW**.
- En **2001** explota la “burbuja.com”.

KLAUS SCHWAB Y LA 4ª R.I.

- El fundador y director general del Foro Económico Mundial afirma que **hoy estamos en los albores de una cuarta revolución industrial**. Esta comenzó a principios de este siglo y se basa en la **revolución digital**.
- Se caracteriza por un **internet más ubicuo y móvil**, por sensores más pequeños y potentes, y por la **inteligencia artificial** y el aprendizaje de la(s) máquina(s).

KLAUS SCHWAB Y LA 4ª R.I.

Schwab piensa que la cuarta revolución industrial **se caracteriza por una fusión de tecnologías** que está difuminando las líneas entre las esferas física, digital y biológica.



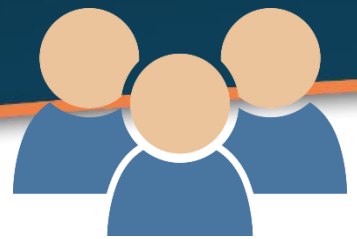
BLOCKCHAIN Y LA 4ª REVOLUCIÓN INDUSTRIAL

Nick Ismail, Information Age:

La 4ª Revolución Industrial es la extensión lógica de una serie de innovaciones tecnológicas que datan del siglo XIX. Donde la tercera revolución industrial nos trajo internet, las redes sociales y el comercio electrónico, **la cuarta se caracterizará por inteligencia artificial, robótica, nanotecnologías, biotecnologías y blockchain**.

- En la 4ª R.I. los procesos simples que actualmente se llevan a cabo manualmente se llevarán a cabo mediante sistemas digitales autónomos, respaldados por tecnologías de blockchain.
- Sus capacidades disruptivas ya han sido bien documentadas en el sector financiero, donde las plataformas blockchain están desafiando la actividad de los intermediarios, que pueden verificar la información de forma rápida y segura sin intervención manual.
- Blockchain simplificará los procedimientos en muchas industrias, se convertirá en un pilar fundacional y fundamental de la 4ª Revolución Industrial.

ANTECEDENTES



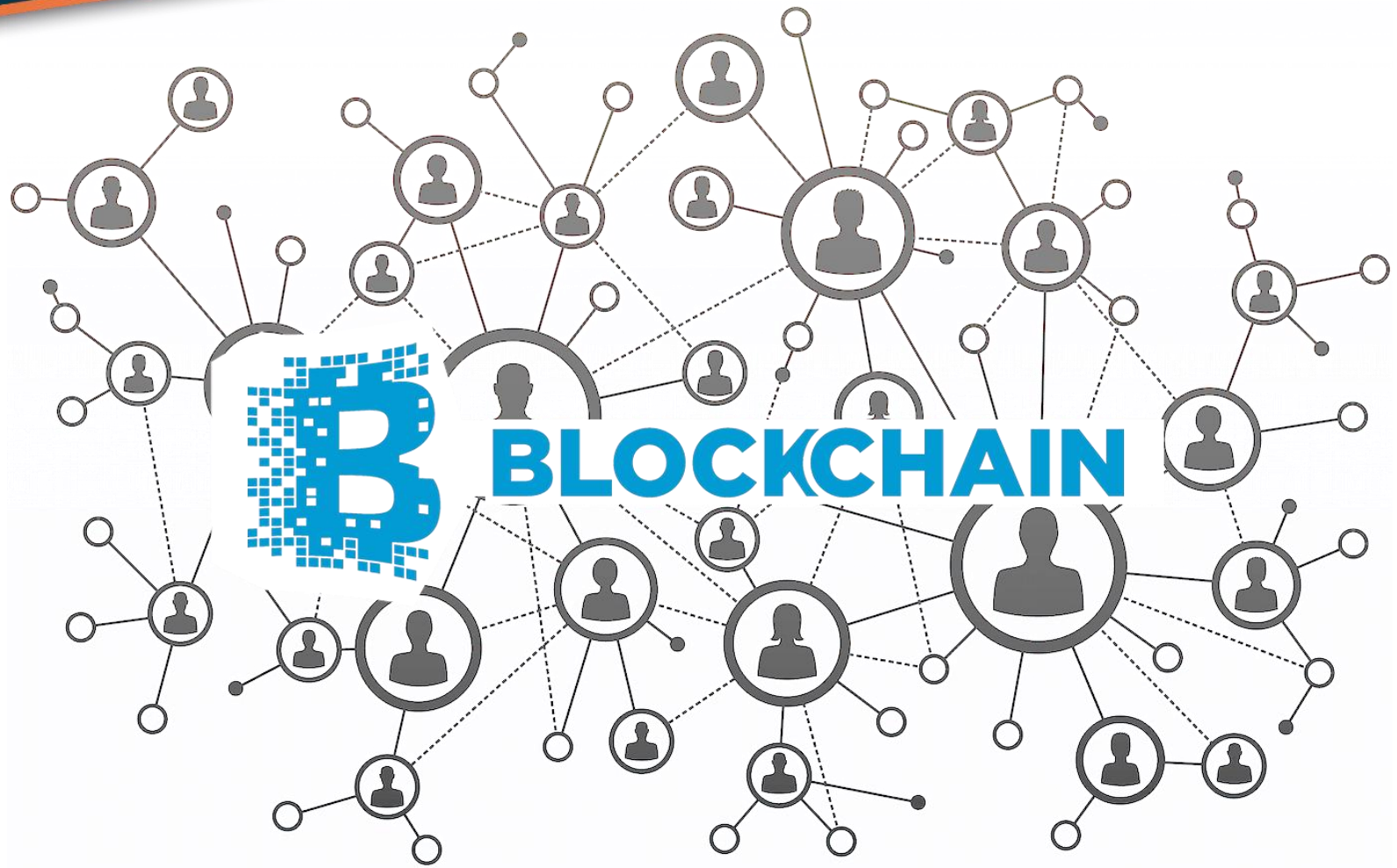
- **Satoshi Nakamoto** es la persona o grupo de personas que crearon el protocolo Bitcoin y su software de referencia, Bitcoin Core.
  - En 2008, Nakamoto publicó un artículo que describía un sistema P2P de dinero digital (*Bitcoin: A Peer to Peer Electronic Cash System*).
  - En **2009**, Nakamoto lanzó el software Bitcoin (aparejadamente con **Blockchain**), creando la red del mismo nombre y las primeras unidades de moneda, llamadas bitcoins.
  - Alrededor de **2014**, los tecnólogos y los inversionistas cambiaron su enfoque de Bitcoin a blockchain, la tecnología subyacente de bitcoin. Aunque Bitcoin y blockchain a menudo se denominan indistintamente, eso es incorrecto. **Bitcoin está basado en una versión (1.0) de una cadena de bloques**.

LIBRO DIGITAL INCORRUPTIBLE

"La cadena de bloques (blockchain) es un libro digital incorruptible de transacciones económicas que pueden programarse para registrar no sólo transacciones financieras sino prácticamente todo tipo de valor."

TAPSCOTT, DON AND TAPSCOTT, ALEX. Blockchain Revolution. 2016.

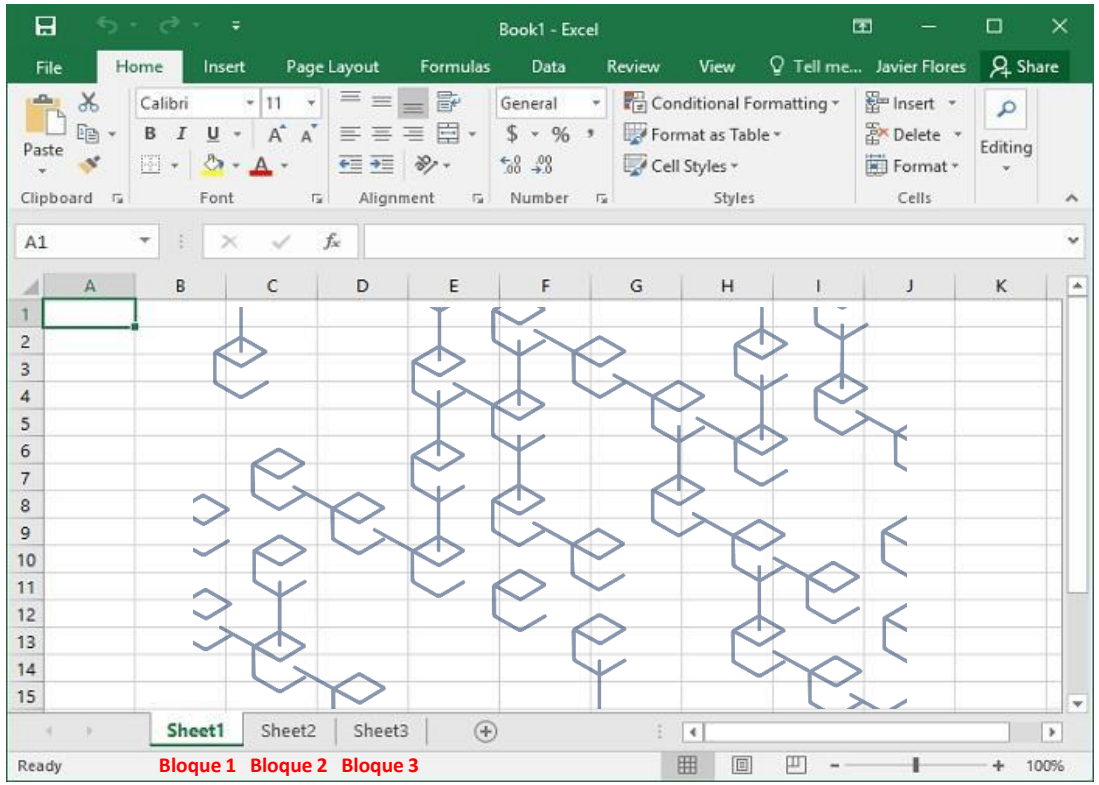
¿QUÉ ES? ¿PARA QUÉ SIRVE?



BLOCKCHAIN ES COMO EXCEL EN LÍNEA

@JoelGomezMX

- Las cadenas de bloques se pueden identificar como un “libro mayor” de contabilidad.
- Estos libros mantienen el registro de transacciones.
- Los “bloques” son grupos de transacciones que han sido procesadas juntas.



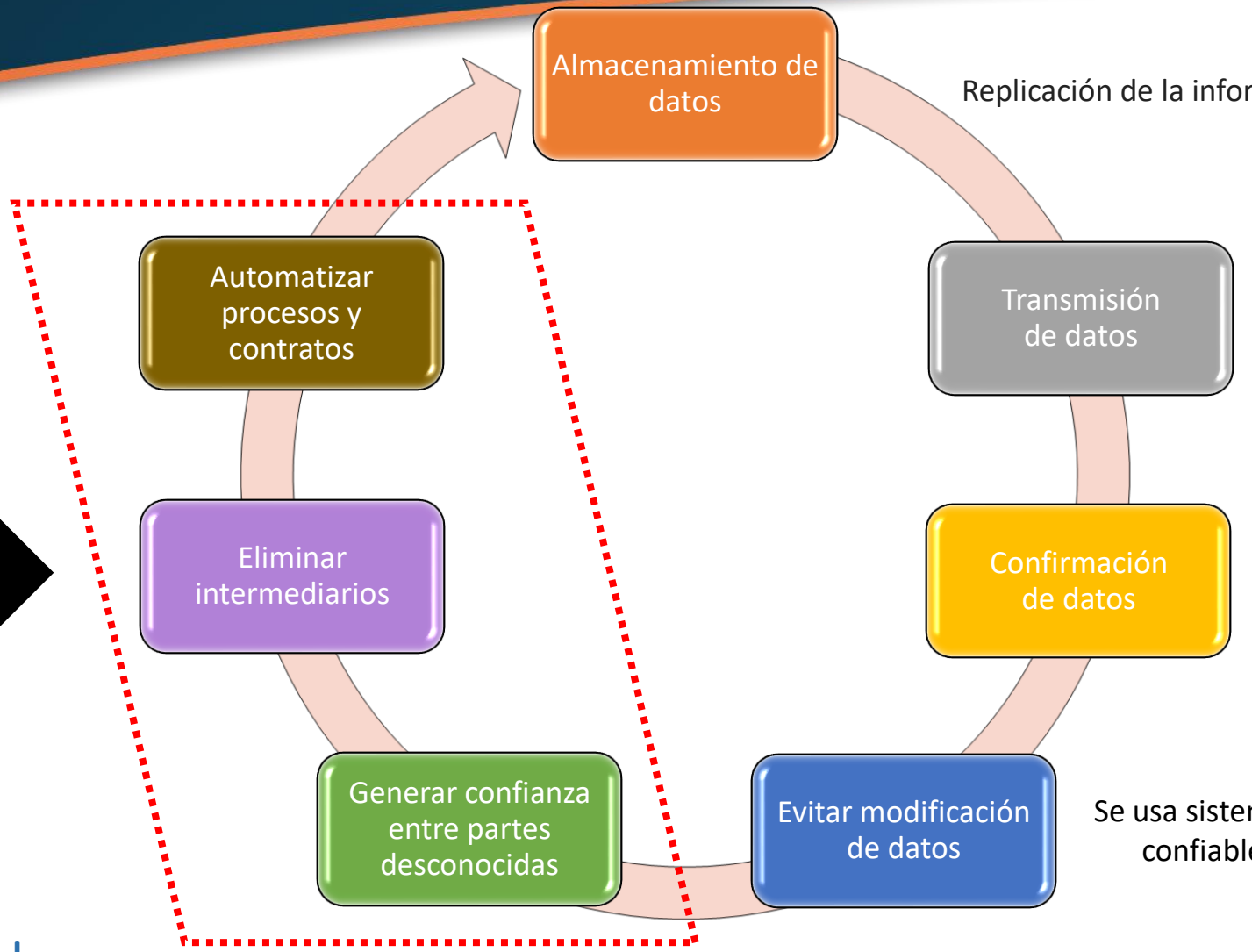
¿QUÉ ES BLOCKCHAIN?

Blockchain es una **base de datos**, descentralizada y distribuida (replicada) globalmente, fomada por cadenas de bloques diseñadas para evitar su modificación, una vez que un dato ha sido publicado.

- Puede contener no solo información, sino de **cualquier cosa que tenga valor** (dinero, acciones, bonos, títulos de propiedad e incluso votos de elecciones).
- No depende de alguien en particular, sino de todos los participantes de la cadena de bloques. **Todo mundo puede ver lo que sucede en tiempo real**.
- Se le ha definido como "**contabilidad colectiva a través de internet**" (tecnología de contabilidad distribuida o "DLT").
- Cada bloque está **firmado digitalmente** y hace mención al bloque previo.
- Los participantes de la red (mineros) **procesan y validan cada transacción**.

FUNCIONES PRINCIPALES DE LA CADENA DE BLOQUES

@JoelGomezMX



Replicación de la información de la cadena de bloques

Redes *peer-to-peer*

Validación mediante proceso de consenso entre los nodos participantes (Minería x algoritmo "prueba de trabajo")

Se usa sistema criptográfico, un sellado de tiempo confiable y enlazando a un bloque anterior

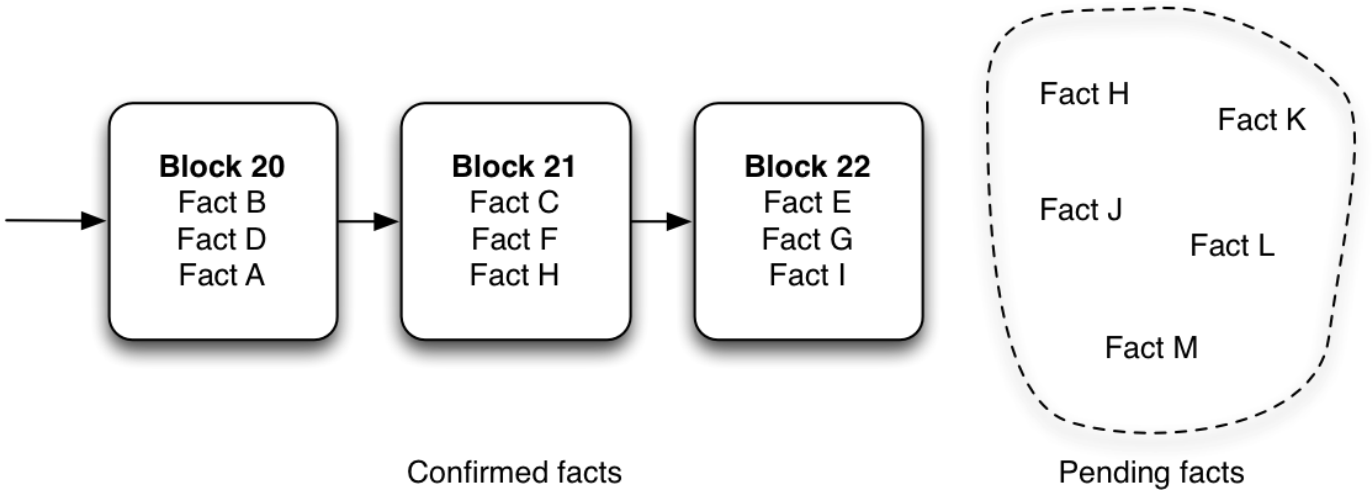
Más que funciones, éstas son consecuencias positivas derivadas de las funciones de Blockchain

LIBRO DE HECHOS

- Un blockchain es un **libro de hechos**, replicado en varias computadoras ensambladas en una red *peer to peer*.
  - Los hechos pueden ser cualquier cosa, desde transacciones monetarias hasta la firma de contenido.
  - Los miembros de la red son personas anónimas llamadas nodos.
  - Toda la comunicación dentro de la red aprovecha la criptografía para identificar de forma segura al emisor y al receptor.
  - Cuando un nodo desea agregar un hecho al libro mayor, se forma un consenso en la red para determinar dónde debe aparecer este hecho en el libro; este consenso se llama bloque.

LIBRO DE HECHOS

- Un blockchain es un **libro de hechos**…
  - Los hechos se agrupan en bloques, y solo hay una cadena de bloques, replicados en toda la red.
  - Cada bloque hace referencia al bloque anterior.
  - Antes de agregarse a un bloque, los hechos están pendientes, es decir, no confirmados.



marmelab

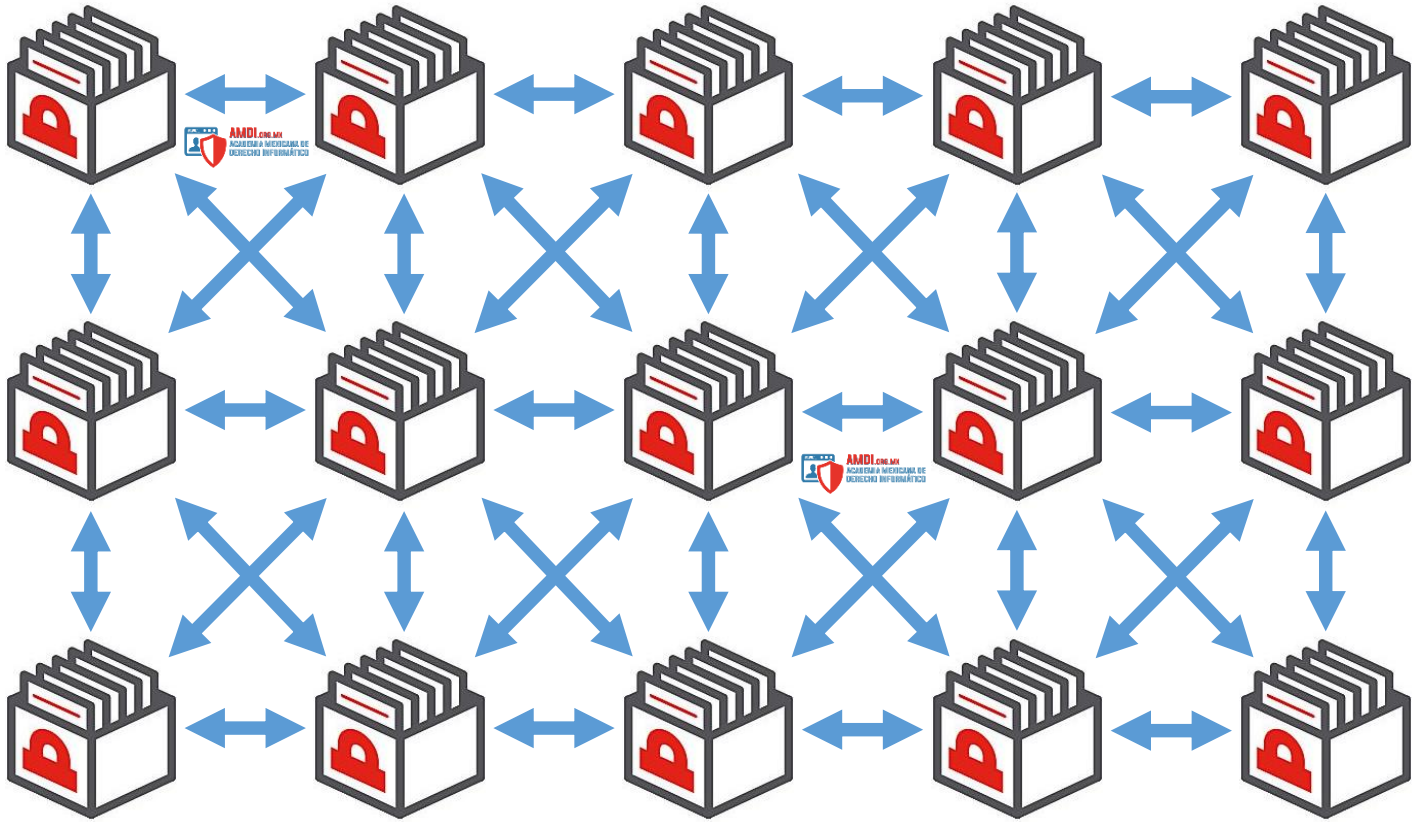
¿POR QUÉ "CADENA DE BLOQUES"?

@JoelGomezMX

Las transacciones se graban de forma cronológica, formando una cadena inmutable.

Fecha + Hora + Participantes + Cantidad

Los bloques se pueden ver y se les puede agregar datos, pero no se pueden borrar, editar ni duplicar.



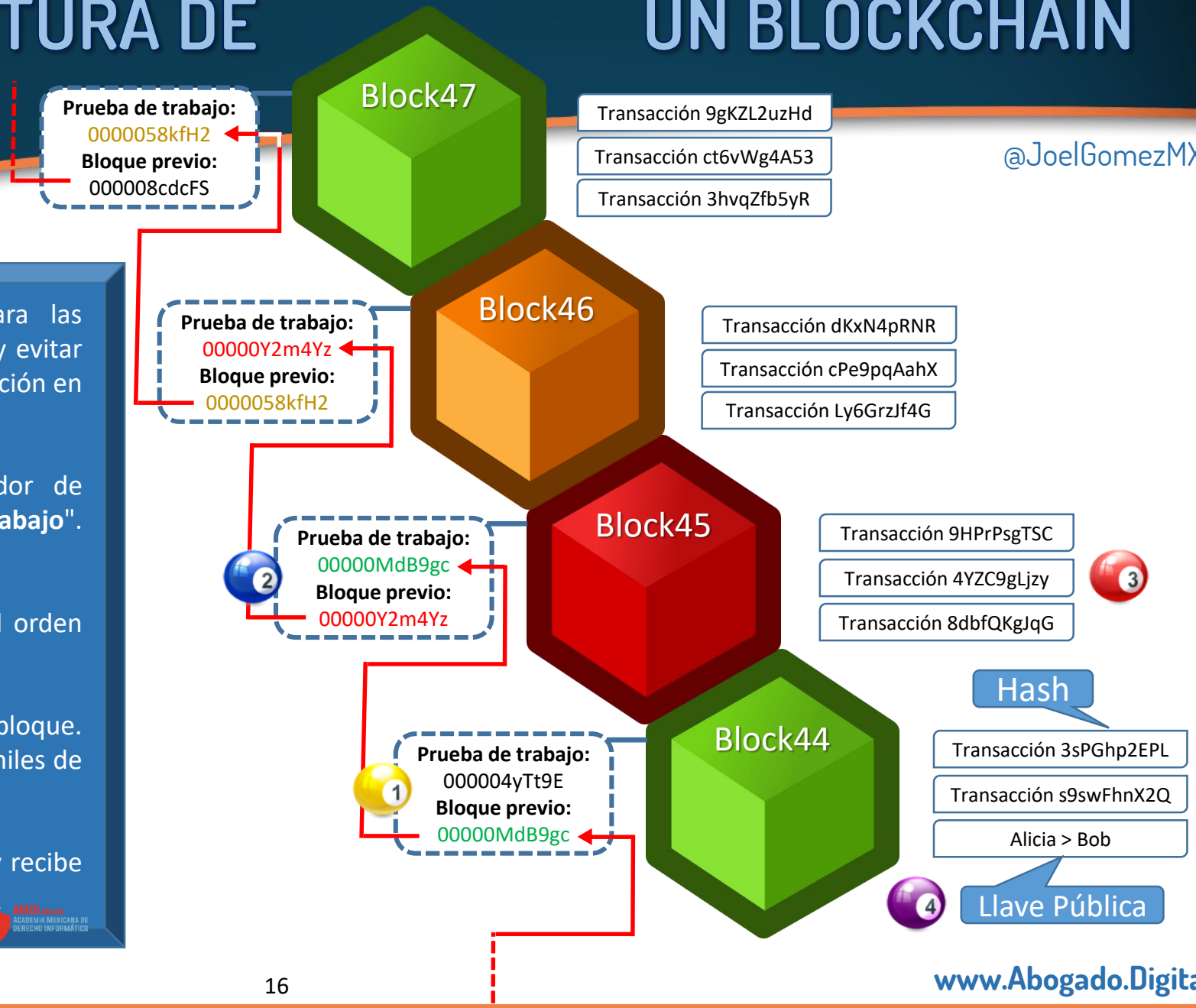
Cada nodo de la red contiene una copia del blockchain completo.

ESTRUCTURA DE UN BLOCKCHAIN

@JoelGomezMX

Blockchain resuelve dos retos principales para las transacciones digitales: controlar la información y evitar duplicaciones. Hay 4 piezas principales de información en un bloque:

1. Una **ID** referida como "**hash**" o identificador de consenso. En el ejemplo se llama "**prueba de trabajo**". Este es un grupo aleatorio de números cifrados.
2. El **número hash del bloque previo**, que fija el orden cronológico en el libro o carpeta.
3. Las **transacciones** que están incluidas en el bloque. Puede ser una, pero también puede contener miles de transacciones.
4. La **llave pública (identidades)** de quien envía y recibe para identificar la transferencia de información.



ESTRUCTURAS DE INCENTIVOS

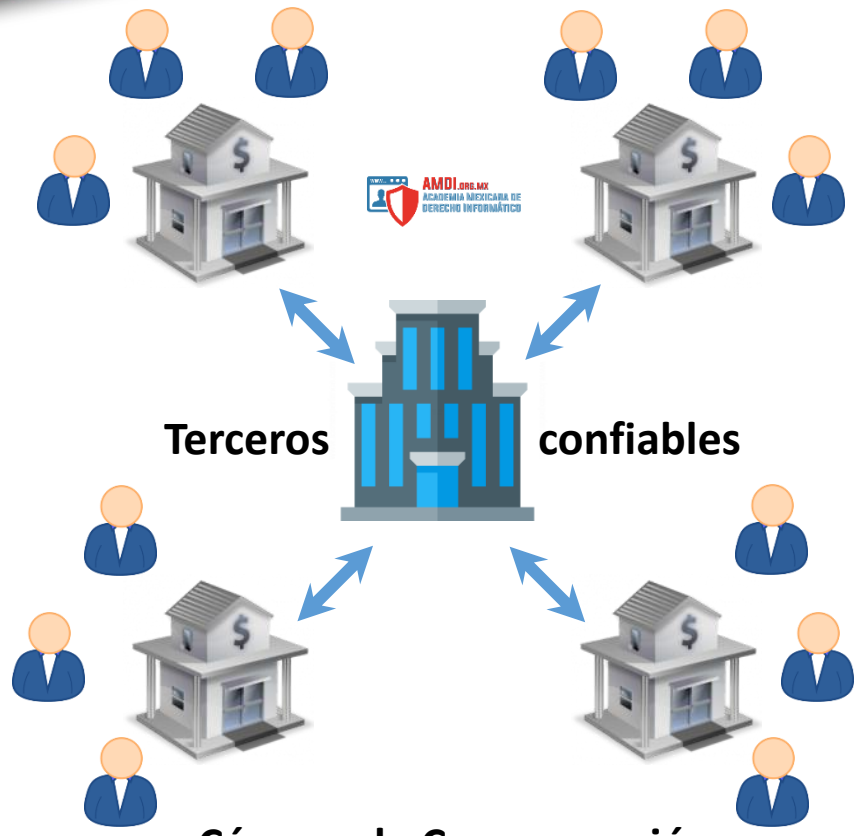
- Los nodos que operan bajo un protocolo son responsables por validar las transacciones y ayudar a otros a mantener el consenso.
- Además de los nodos que propagan transacciones, otros miembros de la red son responsables por crear nuevos bloques que son agregados a la cadena de bloques.

Estas personas son conocidas como “mineros”. El operador de un nodo de minería gasta recursos en términos de poder de cómputo y electricidad. La estructura de incentivos / minería más usada se llama “prueba de trabajo”.

</lexinformatica>
</abogados>

BLOCKCHAIN ELIMINA INTERMEDIARIOS

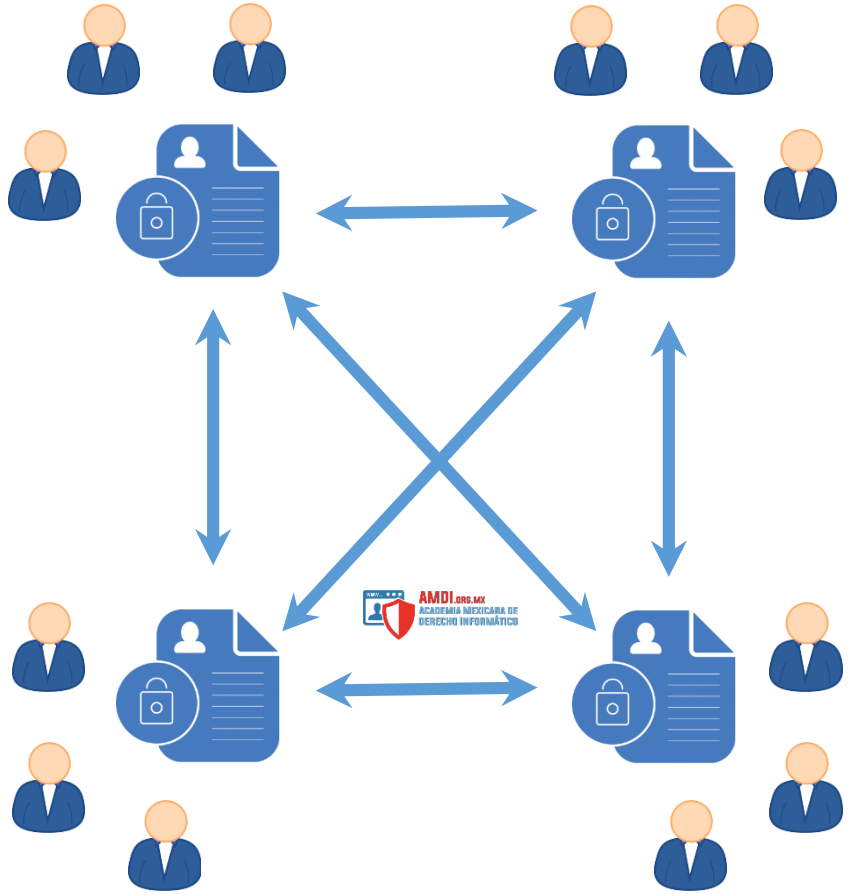
@JoelGomezMX



Cámara de Compensación
(libro contable centralizado)

Requiere **intermediarios** confiables y centralizados. Compensación y liquidación por lotes. **Altas cuotas** e infraestructura cara.

No requiere intermediarios. Rápido procesamiento y administración. **Tarifas bajas** y costo reducido de infraestructura.



Red Financiera
(libro contable descentralizado y distribuido)

NEGOCIOS SIN INTERMEDIARIOS Y DESCENTRALIZADOS (P2P)

Blockchain posibilita nuevos modelos de negocios que buscan eliminar intermediarios e incluso la tenaz presencia del estado.

Blockchain promueve una **economía descentralizada**, un modelo de negocio *peer to peer* (P2P, entre pares), una iteración de la **economía colaborativa**.

América Economía: Alex Preukschat

BLOCKCHAIN ELIMINA INTERMEDIARIOS

@JoelGomezMX

COMERCIO TRADICIONAL

COMERCIO SIN INTERMEDIARIOS

2 REVOLUCIONES: INTERNET Y BLOCKCHAIN

Internet en su momento fue una revolución en el acceso y difusión de la información.

Blockchain nos va a permitir migrar de un internet en el que solo intercambiamos **información** a un internet en el que intercambiamos **valor**.

Blockchain representa una revolución en la transmisión y valor de los datos en Internet.

CADENAS DE BLOQUES PÚBLICAS O PRIVADAS

Las cadenas de bloques públicas y privadas tienen muchas similitudes:

- Son **redes descentralizadas** *peer-to-peer*, en las que **cada participante mantiene una réplica de un libro de contabilidad compartido** al que solo se le pueden agregar transacciones firmadas digitalmente.
- **Mantienen las réplicas sincronizadas** a través de un protocolo denominado **consenso**.
- Proporcionan ciertas **garantías sobre la inmutabilidad del libro mayor**, incluso cuando algunos participantes son defectuosos o malintencionados.

La única distinción entre blockchain público y privado está relacionada con **quién puede participar en la red**, **ejecutar el protocolo de consenso** y **mantener el libro de contabilidad compartido**.

- Una red pública de blockchain está completamente abierta y cualquiera puede unirse y participar en la red.
- La red generalmente tiene un mecanismo incentivador para alentar a más participantes a unirse a la red.
- Bitcoin es una de las cadenas de blockchain públicas más grandes en producción hoy en día.

IBM blog: Praveen Jayachandran

CADENA DE BLOQUES PRIVADA

- **Una red blockchain privada requiere una invitación y debe ser validada** por el iniciador de la red o por un conjunto de reglas establecidas por el iniciador de la red. Las empresas que configuran una cadena de bloques privada generalmente establecerán una red autorizada. Esto impone **restricciones sobre quién puede participar en la red y solo en ciertas transacciones**. Los participantes deben obtener una invitación o permiso para unirse.

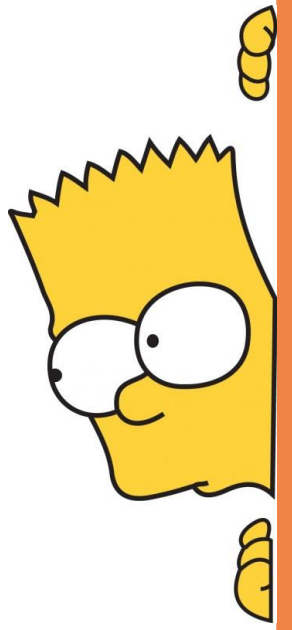
- **El mecanismo de control de acceso podría variar**:
  - los participantes existentes podrían decidir los futuros participantes;
  - una autoridad reguladora podría emitir licencias para la participación;
  - o un consorcio podría tomar las decisiones en su lugar.
- Una vez que una entidad se ha unido a la red, jugará un papel en el mantenimiento de la cadena de bloques de forma descentralizada.

IBM blog: Praveen Jayachandran

4 TIPOS DE CADENAS DE BLOQUES

En un **blockchain de consorcio**, **el proceso de consenso está controlado por un grupo preseleccionado**, por ejemplo, un grupo de empresas. El derecho de leer el blockchain y enviar transacciones a él puede ser público o restringido a los participantes. Las blockchains del consorcio se consideran "blockchains permitidas" y son las más adecuadas para su uso en los negocios.

Los **blockchains semiprivados** **son administrados por una sola compañía que otorga acceso a cualquier usuario que satisfaga los criterios preestablecidos**. Aunque no está verdaderamente descentralizado, este tipo de blockchain permitido es atractivo para casos de uso de empresa a empresa y aplicaciones gubernamentales.



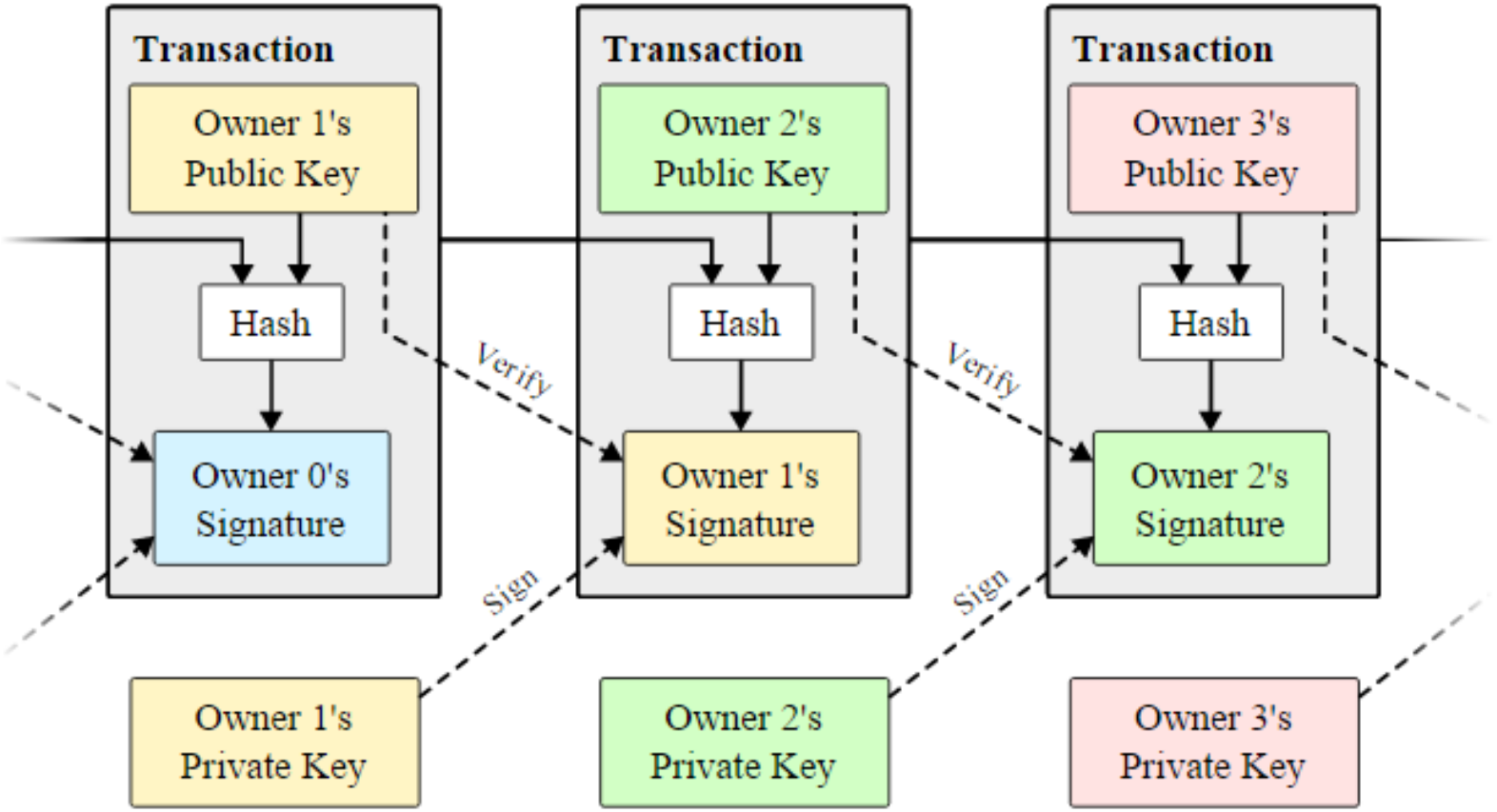
Los **blockchains privados** **están controlados por una sola organización** que determina quién puede leerlo, enviarle transacciones y participar en el proceso de consenso. Dado que son 100% centralizados, las blockchains privadas son útiles como entornos de recinto de seguridad, pero no para la producción real.

Cualquiera puede leer un blockchain público, **enviarle transacciones o participar en el proceso de consenso**. Se consideran cadenas de bloques "sin permiso". Todas las transacciones son públicas y los usuarios pueden permanecer en el anonimato. Bitcoin y Ethereum son ejemplos prominentes de cadenas de bloques públicas.

SEGURIDAD: CRIPTOGRAFÍA + SISTEMAS DISTRIBUIDOS

- Estas cadenas de bloques tienen **dos ingredientes principales**: **criptografía asimétrica** y **sistemas distribuidos**.
- Ello permite crear **archivos ineditables**, **transferir valor** y **automatizar actualizaciones** de los archivos.

FIRMA DIGITAL DE BLOQUES



INTERCAMBIO DE VALOR + CONFIANZA

Donde antes existían **intermediarios**, ahora los podemos substituir con métodos de **seguridad** (cifrado o criptografía) **y consenso**. Todos los participantes de la red acuerdan la validez de una transacción, asegurando que los libros son copias exactas de cada uno.

- Blockchain nos va a permitir **migrar** de un internet en el que solo intercambiamos información a un **internet en el que intercambiamos valor**.
- Dicho valor **se podrá intercambiar de manera directa** entre personas u organizaciones que probablemente no conozcamos, sin intermediarios y con la garantía de que existe plena confianza en la transacción.

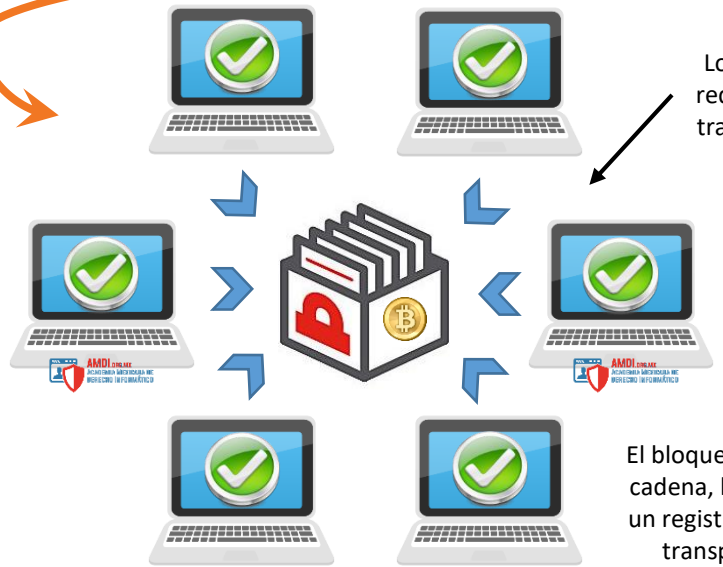
¿CÓMO FUNCIONA UNA TRANSACCIÓN EN BLOCKCHAIN?

@JoelGomezMX

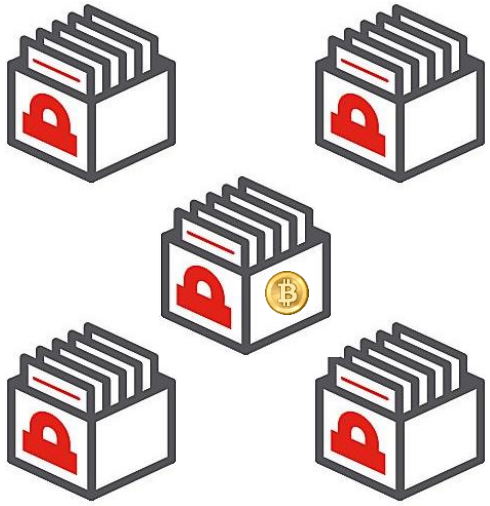
María quiere enviarle dinero a Juan

La transacción se representa en línea como un bloque

El bloque se transmite a todos los miembros de la red



Los miembros de la red confirman que la transacción es válida



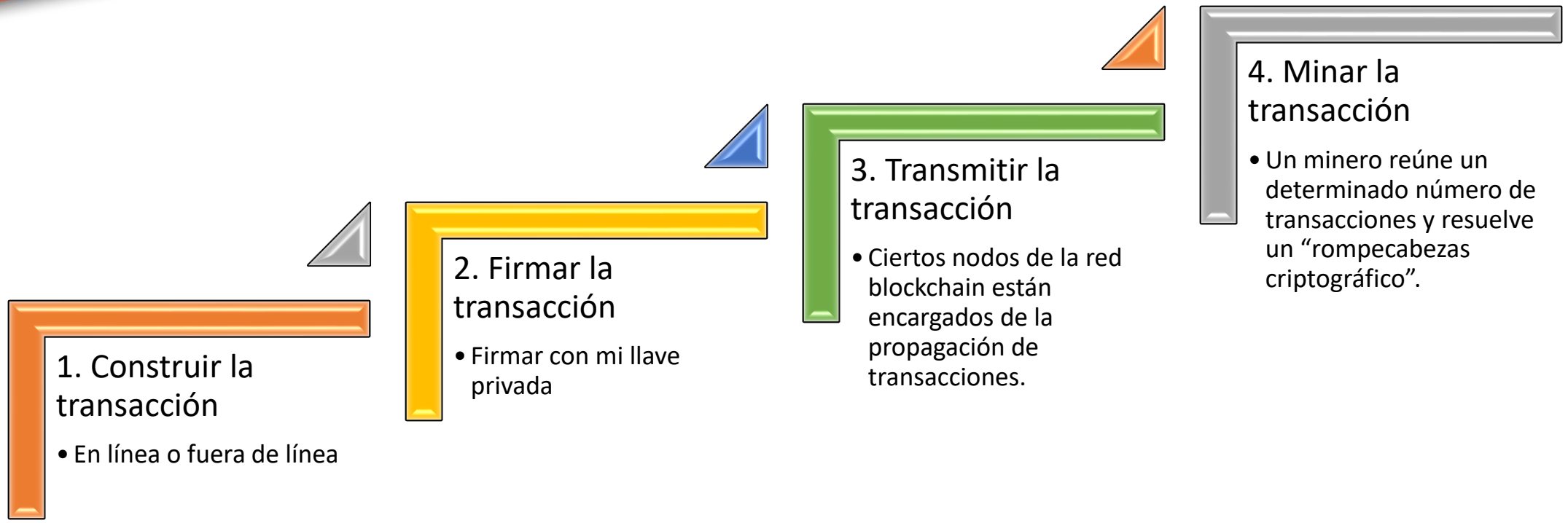
El bloque se añade a la cadena, lo que provee un registro indeleble y transparente de transacciones

Juan recibe su dinero (el bloque de María ahora pertenece a Juan)

</lexinformatica>
</abogados>

PASOS EN UNA TRANSACCIÓN B.CH.

@JoelGomezMX



How a ₿itcoin transaction works

Bob, an online merchant, decides to begin accepting bitcoins as payment. Alice, a buyer, has bitcoins and wants to purchase merchandise from Bob.

WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

An address is a string of letters and numbers, such as 1HULMwZEP kjEPeCh 43BeKJL1yb LCWrfDpN.

CREATING A NEW ADDRESS

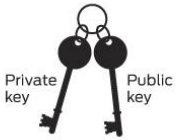
Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of bitcoins.

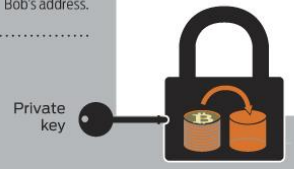
It's tempting to think of addresses as bank accounts, but they work a bit differently. Bitcoin users can create as many addresses as they wish and in fact are encouraged to create a new one for every new transaction to increase privacy. So long as no one knows which addresses are Alice's, her anonymity is protected.

SUBMITTING A PAYMENT

Alice tells her Bitcoin client that she'd like to transfer the purchase amount to Bob's address.



Public Key Cryptography 101
When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.



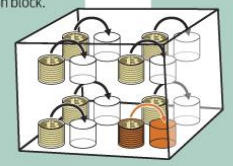
Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring bitcoins from.

Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

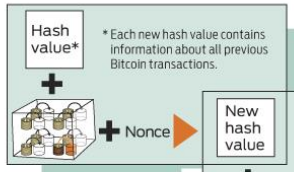
VERIFYING THE TRANSACTION

Gary, Garth, and Glenn are Bitcoin miners.

Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



The miners' computers are set up to calculate cryptographic hash functions.

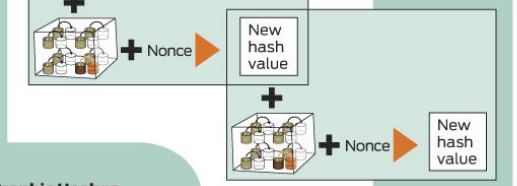


The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

Cryptographic Hashes
Cryptographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.

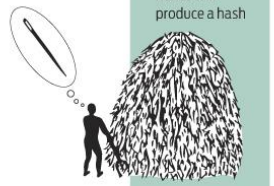
The root of all evil	6d0a 1899 086a... (56 more characters)
The root of all evil	486c 6be4 6dde...
The root of all veil	b8db 7ee9 8392...

Nonces
To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.



The root of all evil ???	0000 0000 0000 ...

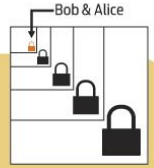
Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form—specifically, it must start with a certain number of zeros.



The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

Each block includes a "coinbase" transaction that pays out 50 bitcoins to the winning miner—in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted bitcoins.

TRANSACTION VERIFIED



As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did—because any changes require a completely different winning nonce—and then redo the work of all the subsequent miners. Such a feat is nearly impossible.

JOSHUA J. ROMERO, BRANDON PALACIO & KARL SSOWALKER INC.

NO CONFUNDIR LA GIMNASIA CON LA MAGNESIA

Incluye labores de minería de bitcoins

Minería profesional
Minería grupal
Minería independiente

ASÍ LUCE UNA BODEGA DE MINERÍA PROFESIONAL DE BITCOINS

Granja de minería de Bitcoins

Granja de minería de Bitcoins

¿CÓMO MINAR BITCOINS?

1. Consigue hardware para minar bitcoins (*ASIC miner*).
2. Encuentra un "grupo minero" (*pooled mining* v. *solo mining*).
3. Consigue software para minar bitcoins.

¿Es legal minar bitcoins en mi país?
¿Es rentable para mi minar bitcoins?

BBVA REALIZA 1ª TRANSACCIÓN BASADA EN BLOCKCHAIN

EL ECONOMISTA

LA OPERACIÓN SE REALIZÓ ENTRE MÉXICO Y ESPAÑA

BBVA realiza primera transacción comercial basada en blockchain

Se logró reducir a 2.5 horas el envío, verificación y autorización del movimiento; normalmente lleva entre siete y 10 días.

Edgar Juárez
27 de noviembre de 2017, 23:18

"Aplicar blockchain a nuestras operaciones de comercio internacional nos permitirá crear un entorno seguro y digital, que será la base de un marketplace global para el Comercio Exterior", concluye Jorge Zebadúa, director de Estrategia y Productos Banca Empresas y Gobierno de BBVA Bancomer.

- **España y México fueron los países entre los que el grupo financiero BBVA realizó la primera transacción basada en tecnología blockchain**.
- Aunque no se trató de una transacción meramente financiera, sí tuvo que ver con comercio internacional, con la presentación electrónica de documentos en una transacción de importación-exportación.
- Gracias a ello, BBVA ha conseguido reducir a 2.5 horas el envío, verificación y autorización de una transacción de comercio exterior que normalmente se prolonga entre siete y 10 días.

BBVA REALIZA 1ª TRANSACCIÓN BASADA EN BLOCKCHAIN

EL ECONOMISTA

- El piloto que hemos realizado supone un **salto en la mejora de la eficiencia de las transacciones de comercio exterior**. La gestión de la documentación se ha reducido a un proceso de pocas horas en el que además todos los involucrados (bancos, importador y exportador) **hemos conocido en todo momento el estado del envío de los documentos**.
- Además, **la operación ha quedado registrada y validada de manera segura**, al mismo tiempo para todas las partes gracias a los registros distribuidos y la inmutabilidad de blockchain.
- El piloto ha incluido la **firma electrónica de los documentos**, la **distribución simultánea de las copias a todas las partes** y la **recepción de la "propiedad"** de la documentación en cada paso de la cadena.
- El piloto se ha centrado exclusivamente en la presentación electrónica de documentos, pero **se podría aplicar al pago final de la carta de crédito**, incluso a los procedimientos previos y a la financiación de las operaciones.
- Aplicar blockchain a nuestras operaciones de comercio internacional **nos permitirá crear un entorno seguro y digital**, que será la base de un marketplace global para el Comercio Exterior.

AMIS + IBM = BLOCKCHAIN

EL ECONOMISTA

- La Asociación Mexicana de Instituciones de Seguros (AMIS) desarrolla, en colaboración con IBM, un **prototipo de base de datos basado en la tecnología blockchain para garantizar que las pólizas de seguro de autos puedan ser verificadas** por las autoridades con mayor facilidad, con el objetivo de **reducir el número de pólizas apócrifas en todo el país**.

- La finalidad de este prototipo es que **cada vez que una compañía aseguradora emita una póliza de seguro para auto, ésta se almacene en el esquema de blockchain**, lo que permite que dicha póliza sea **inalterable** debido a que todas las compañías contarán con una copia de la información de cada seguro de auto que no puede ser alterada sin la autorización de todos los miembros de la asociación.

AMIS + IBM = BLOCKCHAIN

Esta tecnología permite que no sea un tercero el que valide la información contenida dentro de una póliza sino que sea la propia red de empresas de seguros las que garanticen, a través del consenso, que los datos son verídicos.

Save

INCUMBENT BANKS' BLOCKCHAIN INITIATIVES

Institution Name	R3 Member	Hyperledger	Proof of Concept	Investment	Accelerator	Patents
Banco Santander			✓	✓	✓	
Bank of America	✓		✓			✓
Barclays	✓		✓		✓	
BBVA	✓		✓	✓	✓	
BNY Mellon	✓		✓			
Citi	✓		✓	✓		
Commerzbank	✓		✓			
Credit Suisse	✓		✓			
Deutsche Bank	✓		✓			
Goldman Sachs			✓	✓		✓
HSBC	✓		✓			
JPMorgan	✓	✓	✓	✓		
Morgan Stanley	✓		✓			
RBS	✓		✓			
UBS	✓		✓		✓	
Wells Fargo	✓	✓	✓			

BI INTELLIGENCE

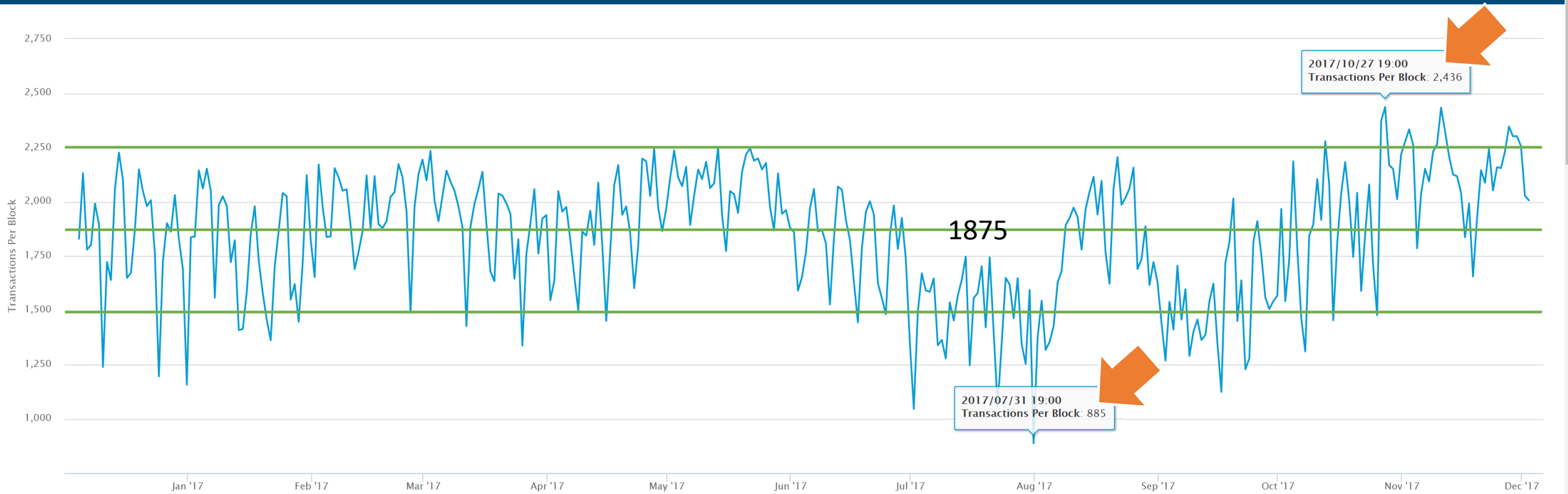
Source: Outlier Ventures

¿CUÁNTAS TRANSACCIONES X BLOQUE?

@JoelGomezMX

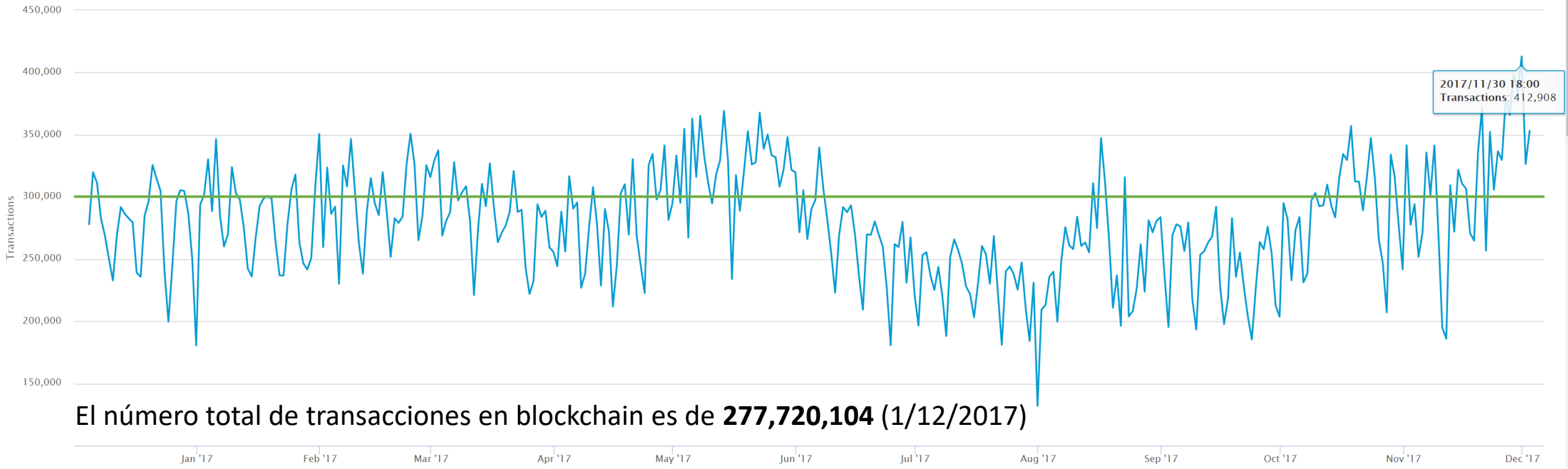
BLOCKCHAIN

En su segmento alto hay 2,250 transacciones por bloque. En el segmento bajo son 1,500 o menos transacciones por bloque.



¿CUÁNTAS TRANSACCIONES X DÍA?

BLOCKCHAIN En promedio aproximado, hay 300,000 transacciones por día. Día con más transacciones: 412,908, Dia con menos transacciones: 131,875.

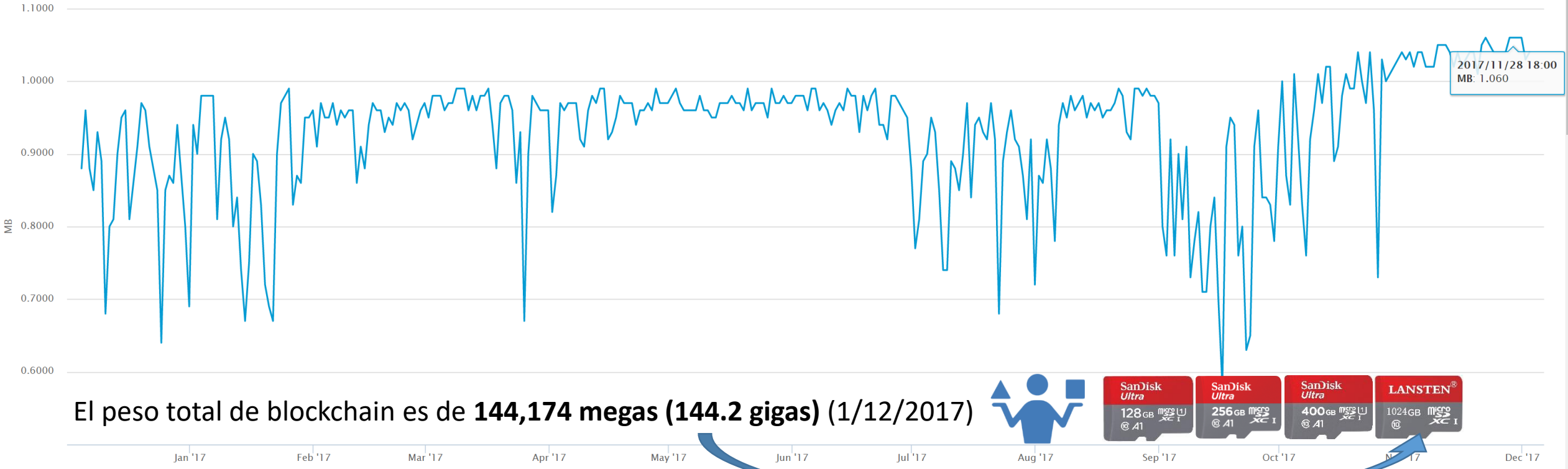


El número total de transacciones en blockchain es de **277,720,104** (1/12/2017)

¿CUÁNTO PESA CADA BLOQUE?

BLOCKCHAIN

En promedio aproximado, cada bloque pesa menos de 1 mega (0.980 megas). El bloque más ligero de 2017 pesa 0.700 megas.



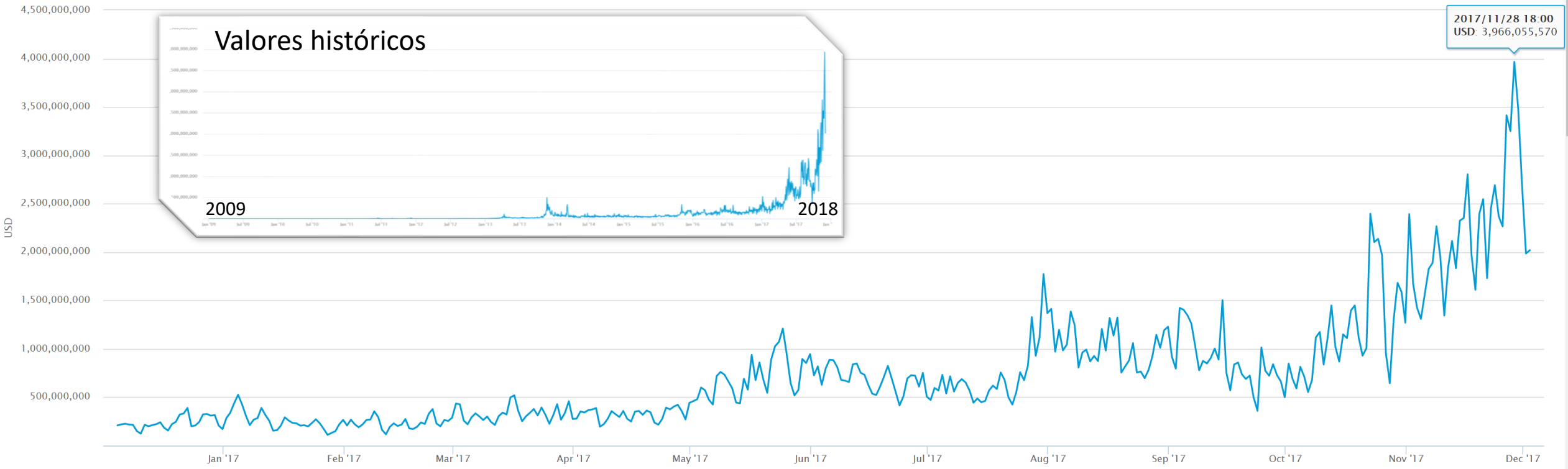
El peso total de blockchain es de **144,174 megas (144.2 gigas)** (1/12/2017)

X 7

VALOR DE TRANSACCIONES EN DLLS. X DÍA

BLOCKCHAIN

Tan solo el 28 de noviembre de 2017 se intercambiaron en blockchain valores (bitcoins) por **$3,966 millones de dólares**.



BLOCKCHAIN EN CRECIMIENTO

- Un estudio realizado por ***IBM Institute for Business Value***, señala que se espera que el mercado de blockchain ascienda a **$2,312 millones de dólares** para 2021 a nivel global.

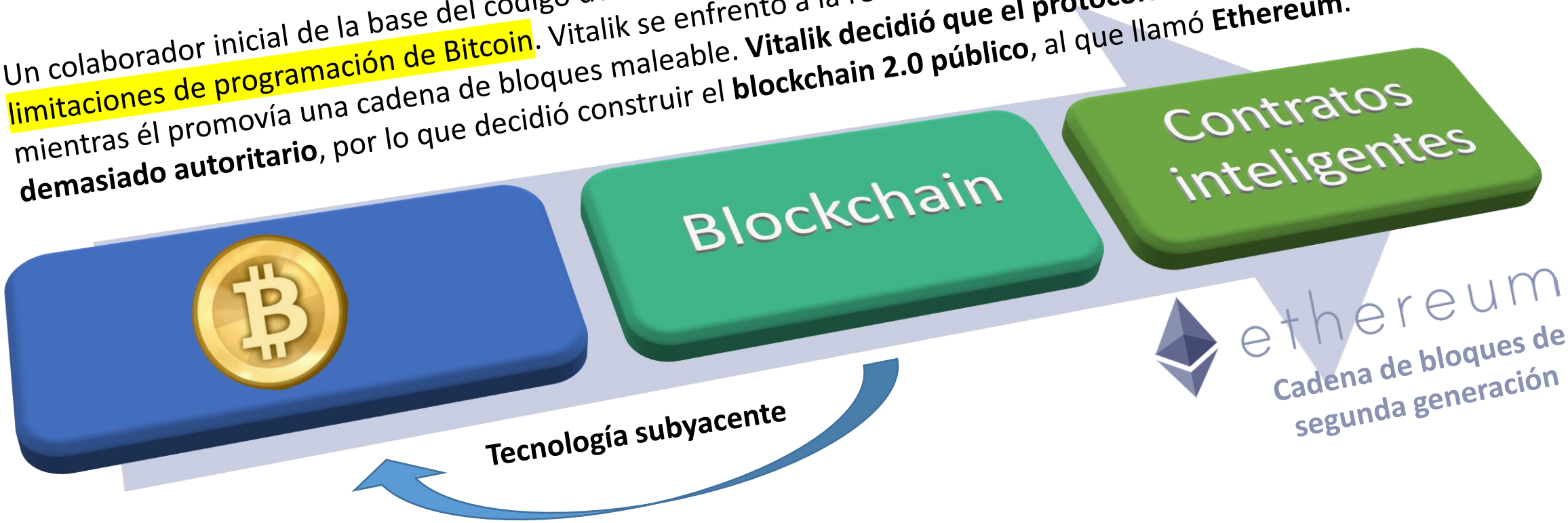
- Con la **tecnología de contabilidad distribuida (DLT)** cualquier bien o servicio podrá ser "tokenizado" (cifrado en lenguaje de programación, para asignarle un valor) y podrá ser pagado de la forma que tu desees.

- Samir Goel, emprendedor en criptomonedas -

CADENA DE INNOVACIONES

@JoelGomezMX

Un colaborador inicial de la base del código de Bitcoin, **Vitalik Buterin** se sintió frustrado en 2013 por las limitaciones de programación de Bitcoin. Vitalik se enfrentó a la resistencia de la comunidad Bitcoin mientras él promovía una cadena de bloques maleable. **Vitalik decidió que el protocolo de Bitcoin era demasiado autoritario**, por lo que decidió construir el **blockchain 2.0 público**, al que llamó **Ethereum**.



ANTECEDENTES BLOCKCHAIN 2.0

Cameron McLain, The Mission:

- **Vitalik** creó un lenguaje de programación para **Ethereum** que es más maleable que el de **Bitcoin**.
- A diferencia de la cadena de bloques de Bitcoin, que solo permite el registro de Bitcoins, **la cadena de bloques de Ethereum permite la transferencia y el registro de otros activos**, como préstamos o contratos.
- Este sistema blockchain de segunda generación **lanzado en 2015** se puede utilizar para construir "**contratos inteligentes**".
- **Ethereum** también se ha utilizado como plataforma de crowdfunding para ***Initial Coin Offerings (ICOS)***.

ETHEREUM

Wikipedia:

- **Ethereum** usa como divisa interna el **ether**, la criptomoneda descentralizada subyacente al mismo que sirve para ejecutar los contratos del mismo. A este respecto, Ethereum no es como la mayoría de las criptodivisas existentes, ya que **no es solamente una red para reflejar las transacciones de valor monetario, sino que es una red para la alimentación de los contratos basados en Ethereum**. Estos contratos de código abierto pueden ser usados para ejecutar de forma segura una amplia variedad de servicios, entre los que se incluyen: sistemas de votación, intercambios financieros, plataformas de *crowdfunding*, propiedad intelectual y organizaciones descentralizadas autónomas.

¿QUÉ ES UN ICO?

Cameron McLain, The Mission:

- **Un ICO es un evento de recaudación de fondos** en el que un grupo de tecnólogos o empresarios recaudan dinero creando y vendiendo sus propios "tokens" a través de un evento de crowdfunding en un blockchain, generalmente Ethereum.
- Un token es una especie de “acción” en una empresa, pero sin muchas de las características y protecciones.
- **El dinero recaudado con los tokens se usa para construir nuevos proyectos relacionados con la cadena de bloques y los titulares de los tokens tienen una participación en estos proyectos**. A medida que la tecnología blockchain se expande mucho más allá de Bitcoin para impulsar las redes emergentes, las empresas y las actividades, las personas adquieren los tokens para participar en esta innovación.

¿QUÉ ES UNA DAO O UNA DAC?

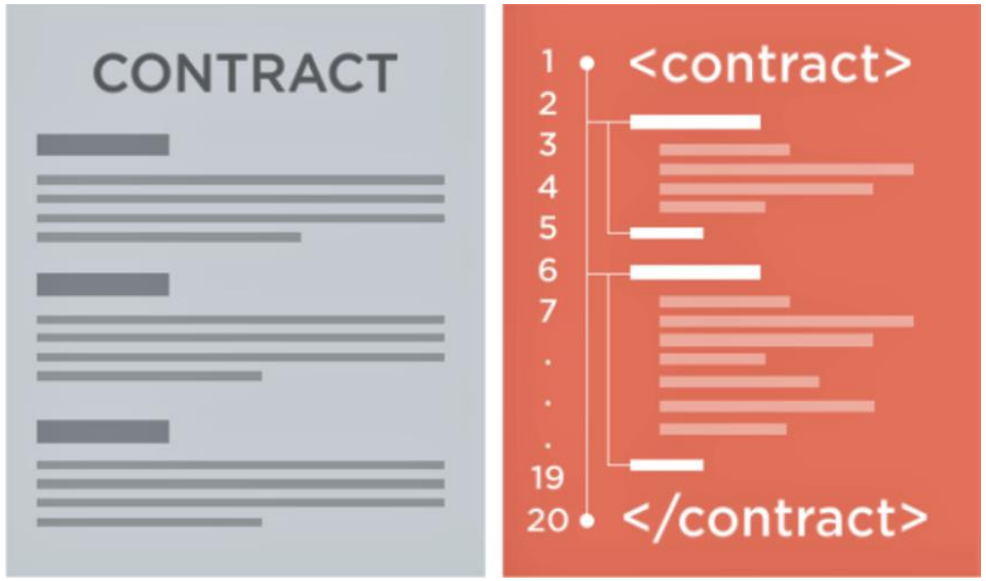
Wikipedia:

- Una **Organización Autónoma Descentralizada** (*Decentralized Autonomous Organization*) o DAO, también llamada **Empresa Autónoma Descentralizada** (*Decentralized Autonomous Corporation*) o DAC, es una organización que está dirigida a través de reglas codificadas en programas de computadora llamados contratos inteligentes. Un registro de transacción financiera de una DAO así como dichas reglas están gestionadas a través de un blockchain.
- Los datos incluidos en el blockchain podrían, siempre y cuando las organizaciones reguladoras lo permitieran, reemplazar documentos públicos como acciones y títulos.
- Una vez que **una DAO** se ponga en marcha, **puede ser autónoma** en el sentido de que pueda **funcionar sin necesidad de supervisión humana**, siempre que los contratos inteligentes sean apoyados por una plataforma como *Ethereum*.

CONTRATOS INTELIGENTES

¿Qué son?
¿Cómo funcionan?
¿Cuáles son sus características?

¿QUÉ ES UN CONTRATO INTELIGENTE?



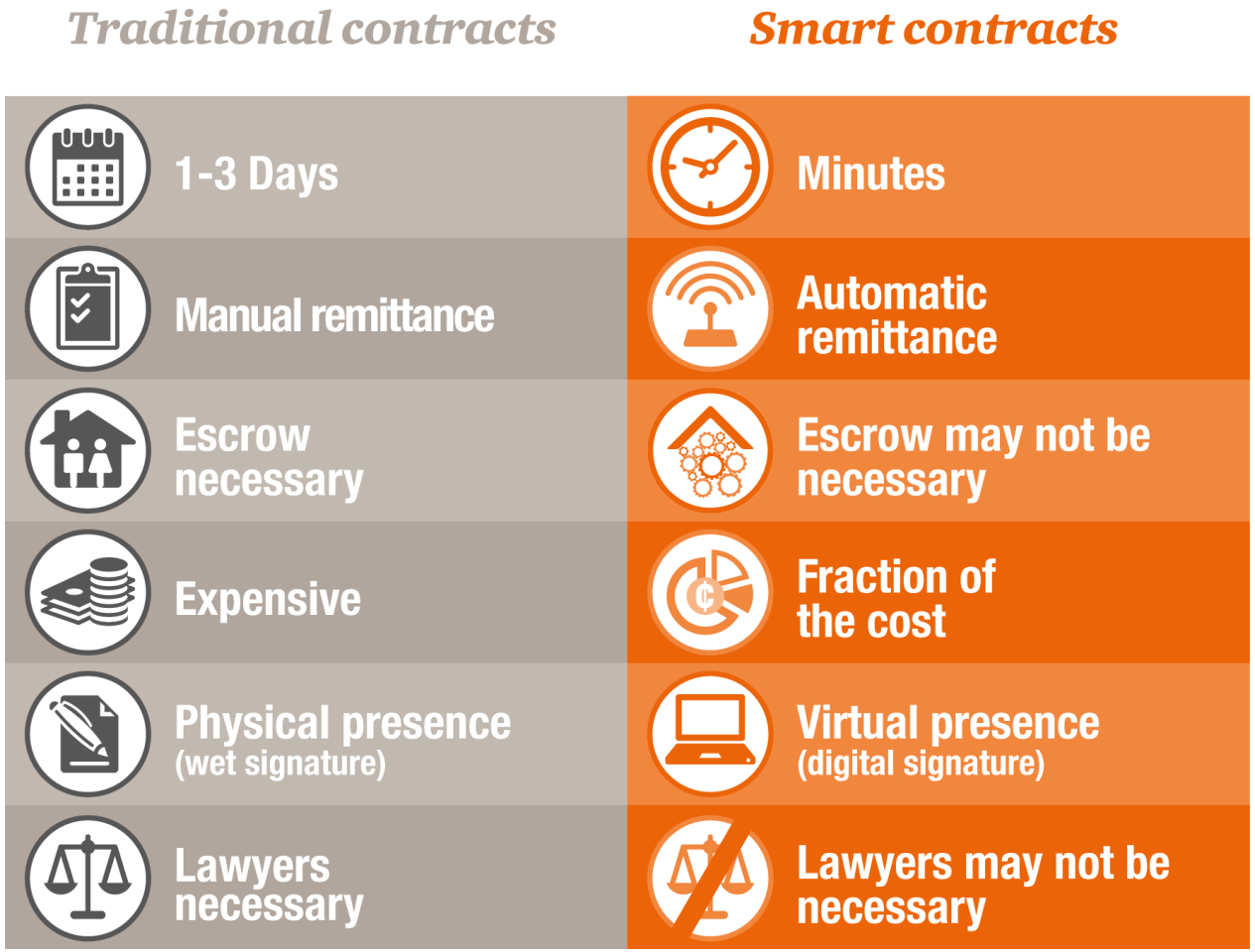
El concepto lo definió en **1994** el criptógrafo **Nick Szabo**, pero no se pudo materializar porque la infraestructura tecnológica necesaria para crearlos aún no existía.

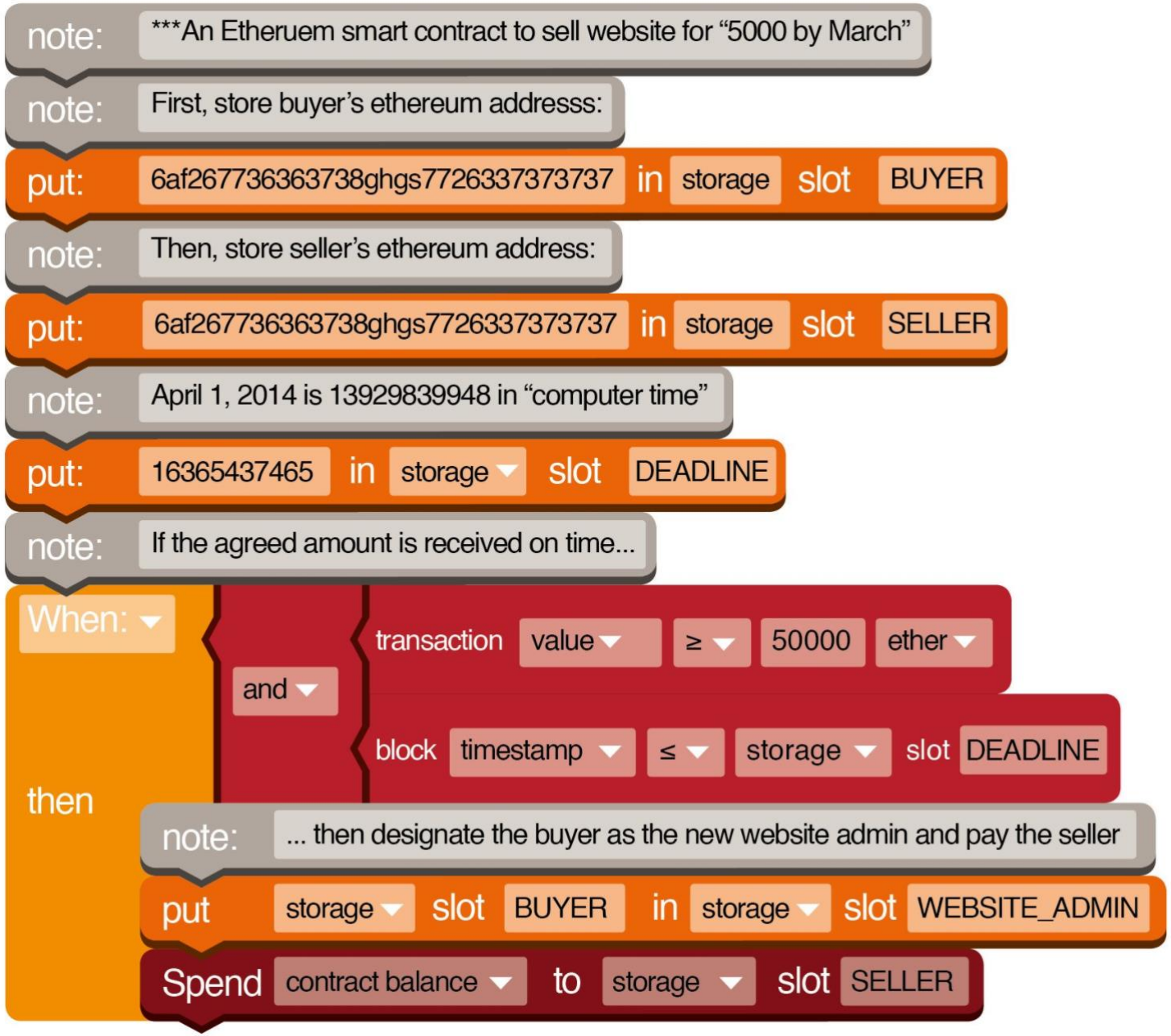
- Un contrato inteligente es un **código de computadora** que se ejecuta en la parte superior de una cadena de bloque que contiene un conjunto de reglas bajo las cuales las partes de ese contrato inteligente acuerdan interactuar entre sí. **Si se cumplen las reglas predefinidas, el acuerdo se aplica automáticamente**.
- El código de contrato inteligente **facilita, verifica** y **hace cumplir** la negociación o ejecución de un acuerdo o transacción.

¿QUÉ ES UN CONTRATO INTELIGENTE?

- Contrato inteligente es un término usado para describir un **código de programa de computadora** que es capaz de **facilitar**, **ejecutar** y **hacer cumplir** la negociación o **ejecución de un contrato** usando la tecnología de bloque de bloques.
- Todo el proceso es automatizado puede actuar como complemento o sustituto de los contratos legales, donde **los términos del contrato inteligente se registran en un lenguaje informático como un conjunto de instrucciones**.

INTELIGENTES VS... ¿TONTOS?



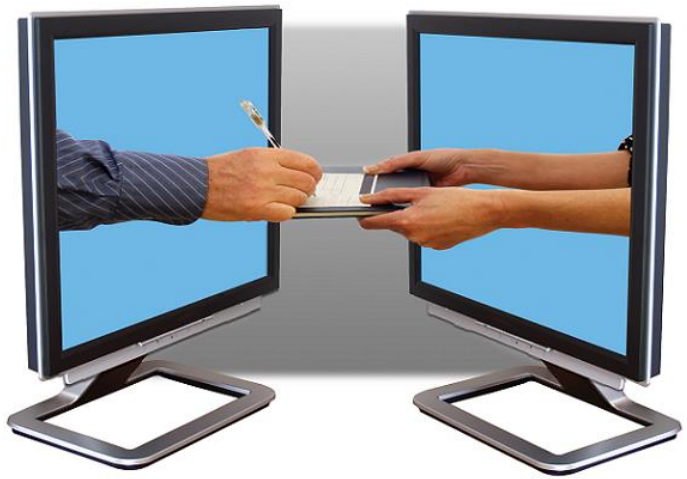


ASÍ SE VERÍA EL “CÓDIGO” DE UN CONTRATO INTELIGENTE

OBJETIVO DE UN CONTRATO INTELIGENTE

El **objetivo principal** de un **contrato inteligente** es permitir a dos partes anónimas comerciar y hacer negocios entre sí, por lo general a través de Internet, **sin la necesidad de un intermediario**.

BlockchainTechnologies.com



3 ELEMENTOS DEL CONTRATO INTELIGENTE

1. La transacción debe **implicar más que la mera transferencia** de una moneda virtual de una persona a otra (por ejemplo, una transferencia de un pago);
2. La transacción **involucra a dos o más partes**, y
3. La **ejecución del contrato no requiere ninguna participación humana directa** después de que el contrato inteligente se haya hecho parte de la cadena de bloques.
   - Es este último elemento el que hace que estos contratos sean "inteligentes“.

POSIBILIDADES...

Los contratos inteligentes son:
• Auto-verificables • Autoejecutable • Resistentes a la manipulación (a prueba de modificaciones)

Los contratos inteligentes pueden:
• Convertir las obligaciones legales en procesos automatizados. • Garantizar un mayor grado de seguridad. • Disminuir la confianza en los intermediarios de confianza. • Disminuir los costos de la transacción.

BENEFICIOS CLAVE

- El beneficio clave de los contratos inteligentes reside en el corazón de su característica más crítica y codiciada: la automatización.
  - Dado que los contratos inteligentes requieren poca o ninguna intervención humana, son generalmente mucho más baratos, rápidos y menos ambiguos en su ejecución y casi no dejan espacio para errores humanos.
- Los documentos legales basados en código tendrán la capacidad de depurarse ellos mismos. Es decir, los contratos inteligentes podrán detectar errores e inconsistencias dentro de un documento legal mediante la lógica de la máquina.

TIPOS DE "SMART CONTRACT"

- En el contexto de desarrollo de aplicaciones blockchain, el término "smart contract" no tiene nada que ver con la noción tradicional de contrato.
- Un "smart contract" se refiere a un pedazo de código de programación que se ejecuta sobre el blockchain en su mayoría de una manera automatizada.
- Un tipo de contrato inteligente se refiere al código que es ejecutado sobre el blockchain (*code based smart contract*), el otro tipo de contrato inteligente se refiere a la implementación de un "*contrato legal*" sobre el blockchain.
- Hyperledger usa el término "*chaincode*" para describir el código que busca ser ejecutado sobre una cadena de bloques.

BITCOIN VS. ETHEREUM (TURING-COMPLETE)

- Mientras que el protocolo Bitcoin contiene un lenguaje básico (limitado) de *scripting* que le permite alguna funcionalidad de programación, no es cercanamente tan robusto como la Máquina Virtual de Ethereum que está incorporada al Protocolo de Ethereum, u otros **protocolos similares con "capacidades - Turing" de programación completas**.

- El efecto de esto es **agregar una computadora completamente funcional a blockchain**. Con ello no solo podemos almacenar criptomonedas en blockchain, sino también **podemos almacenar e implementar programas de cómputo en un blockchain**, que una vez que sean llamados correrán en cada nodo conectado a la red.
- Este tipo de *smart contracts* permiten la creación de **DAO**s.

MÁS NO SIEMPRE ES MEJOR

- Mayores funcionalidades también puede ser algo problemático. Ello implica más código, lo cual resulta en mayores probabilidades de errores. Mientras muchos consideran el scripting de Bitcoin como algo muy limitado, otros lo ven como una ventaja pues provee las funciones y capacidades que son necesarias para cumplir su propósito.
- Mientras que la tecnología blockchain (salvo Bitcoin) es todavía joven y sujeta a mucho desarrollo, ya **existen preocupaciones sobre la falta de estándares e interoperabilidad** entre diferentes cadenas de bloques.

REGLAS Y CONSECUENCIAS ESTRICTAS

"El programa (de los contratos inteligentes) puede definir reglas y consecuencias estrictas del mismo modo que lo haría un documento legal tradicional, pero **a diferencia de los contratos tradicionales, también puede tomar información como *input*, procesarla según las reglas establecidas en el contrato** y adoptar cualquier medida que se requiera como resultado de ello".

Javier Sebastián, responsable de Regulación Digital de DLT de BBVA Research.

EJEMPLOS DE USO EN SERVICIOS FINANCIEROS

Depto. BBVA Research:

- **Préstamos:** podrían almacenarse como *smart contracts* en el *blockchain*, junto con la información de las garantías de la propiedad. Si el deudor no efectúa un pago, el *smart contract* podría revocar automáticamente las claves digitales que le dan acceso a las garantías.
- **Depósito en garantía (¿*smart escrow*?):** los *smart contracts* se pueden configurar fácilmente como cuentas de depósito en garantía que hacen un seguimiento del intercambio entre dos partes. El comprador de bienes o servicios transferiría el pago a la cuenta del contrato. El contrato supervisaría los servicios externos (p. ej. localización vía GPS) y, una vez transferida la propiedad del vendedor al comprador, el contrato liberaría automáticamente los fondos al vendedor.

EJEMPLOS DE USO EN SERVICIOS FINANCIEROS

Depto. BBVA Research:

- **Herencias:** podrían automatizarse estableciendo la asignación de activos tras el fallecimiento. Podría ser tan sencillo como mover un control deslizante que determina quién obtiene cuánto. Una vez que el *smart contract* puede verificar la condición de activación, en este caso el fallecimiento, el contrato entra en vigor y los activos se reparten.
- **Mercados de capitales:** los valores basados en pagos y derechos que se ejecutan según unas reglas predefinidas se pueden escribir como *smart contracts*. Ya hay experimentos para la emisión de *bonos inteligentes* y para la gestión de mercados de valores privados. Los contratos que supervisan el rendimiento de activos digitales o no digitales también se pueden utilizar como futuros, forwards, swaps y opciones.

¿QUIÉN RESUELVE CONFLICTOS?

Jueces: 1150–1025 AC

Árbitros:
1795 / 1899

Blockchain: 2017

VALOR ASEGURADO

Con **contratos inteligentes el 100% del valor de la operación está asegurado en la cadena de bloques**, la cual técnicamente actúa como un "intermediario" reteniendo el dinero o valor de la transacción, mismo que será automáticamente liberado o depositado a la "criptobilletera" del vendedor una vez que las condiciones del contrato sea hayan cumplido.

LOS CONTRATOS INTELIGENTES REDUCEN RIESGOS EN TRANSACCIONES

@JoelGomezMX

Los contratos inteligentes están codificados, y el código de computadora es siempre binario, por lo que no hay áreas grises o ambigüedades.

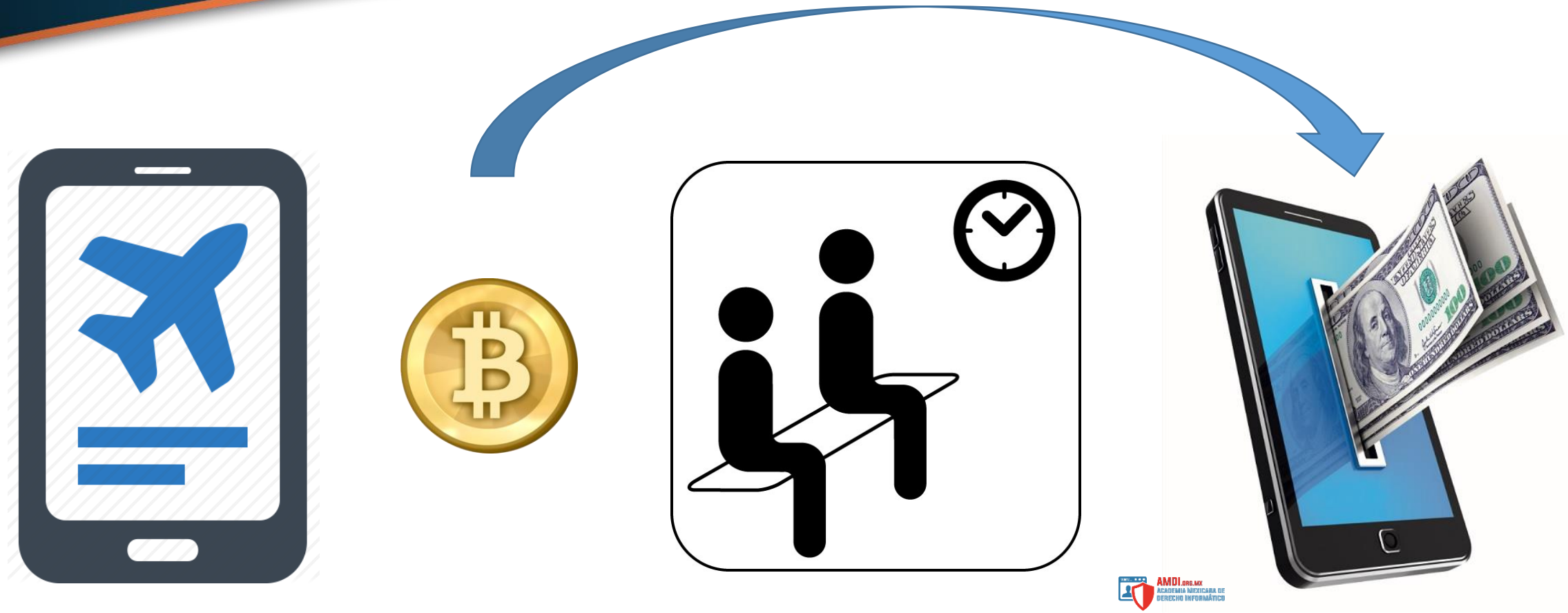
El estado actual de las cosas enlazadas digitalmente a la cadena de bloques -sea esa cosa una casa o una cartera bitcoin- **es verificable**.

Son auto-ejecutables, lo que significa que **las partes en el contrato no pueden negarse a cumplirlo**, nadie puede decidir no llevar a cabo una determinada tarea.

Joe Dewey y Shawn Amuial

EJEMPLO 1 DE CONTRATO INTELIGENTE

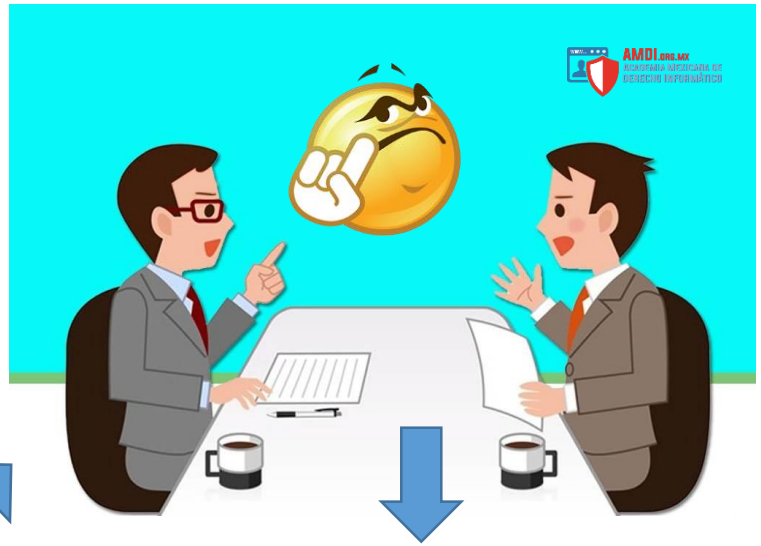
@JoelGomezMX



EJEMPLO 2 DE CONTRATO TRADICIONAL

1ª escenario

@JoelGomezMX

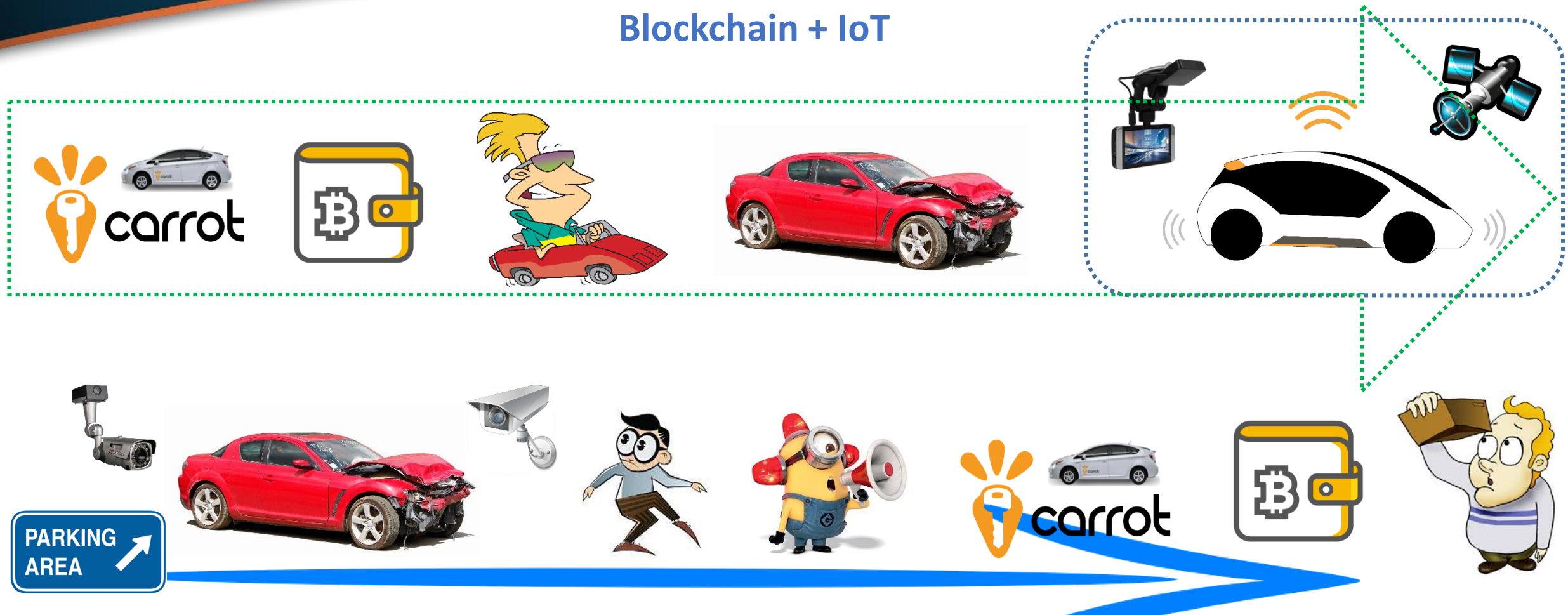


EJEMPLO 2 DE CONTRATO INTELIGENTE

2° escenario

@JoelGomezMX

Blockchain + IoT



USOS ACTUALES DEL BLOCKCHAIN

@JoelGomezMX

- Prueba de titularidad de módulos en el desarrollo de una app.
- Prueba de titularidad para almacenamiento y entrega de contenidos digitales.
- Transferencia de valores basada en puntos para apps de transporte compartido.
- Comercio de seguridad digital: titularidad y transferencia.
- Digitalización de documentos / contratos y prueba de titularidad para transferencias.
- Almacenamiento descentralizado usando una red de computadoras sobre blockchain.
- Internet de las cosas descentralizado.
- Provee identidad digital que protege la privacidad del consumidor.
- Servicios de custodia (escrow).
- Portal de tecnologías de información de contratos inteligentes para ejecutar el procesamiento de órdenes en comercio electrónico y manufactura.
- Administración descentralizada de archivos de historial clínico de pacientes.
- Digitalización de activos: mejora medidas anti-pirateo.
- Permite autenticidad de comentarios de consumidores (reviews).
- Descentralización de recursos informáticos y de internet para cada casa y negocio.
- Digitalización de constitución de sociedades, transferencia de capital social / titularidad y gobernanza.

USOS DE BLOCKCHAIN X SECTORES

Blockchain en Banca y Finanzas	Blockchain en Negocios	Blockchain en Gobierno	Blockchain en Otras Industrias
• Seguros • Pagos Internacionales • Mercados de capitales • Financiamiento del comercio • Protección contra lavado de dinero • Transacciones punto a punto	• Gestión de la cadena de suministro • Cuidado de la salud • Bienes raíces • Medios de comunicación • Energía	• Gestión de registros • Gestión de identidad • Votación • Impuestos • Agencias sin fines de lucro • Legislación / Cumplimiento / Supervisión regulatoria	• Gestión Financiera / Contabilidad • Voto de accionistas • Gestión de registros • La seguridad cibernética • Big Data • Almacenamiento de datos • Internet de las cosas (IoT)

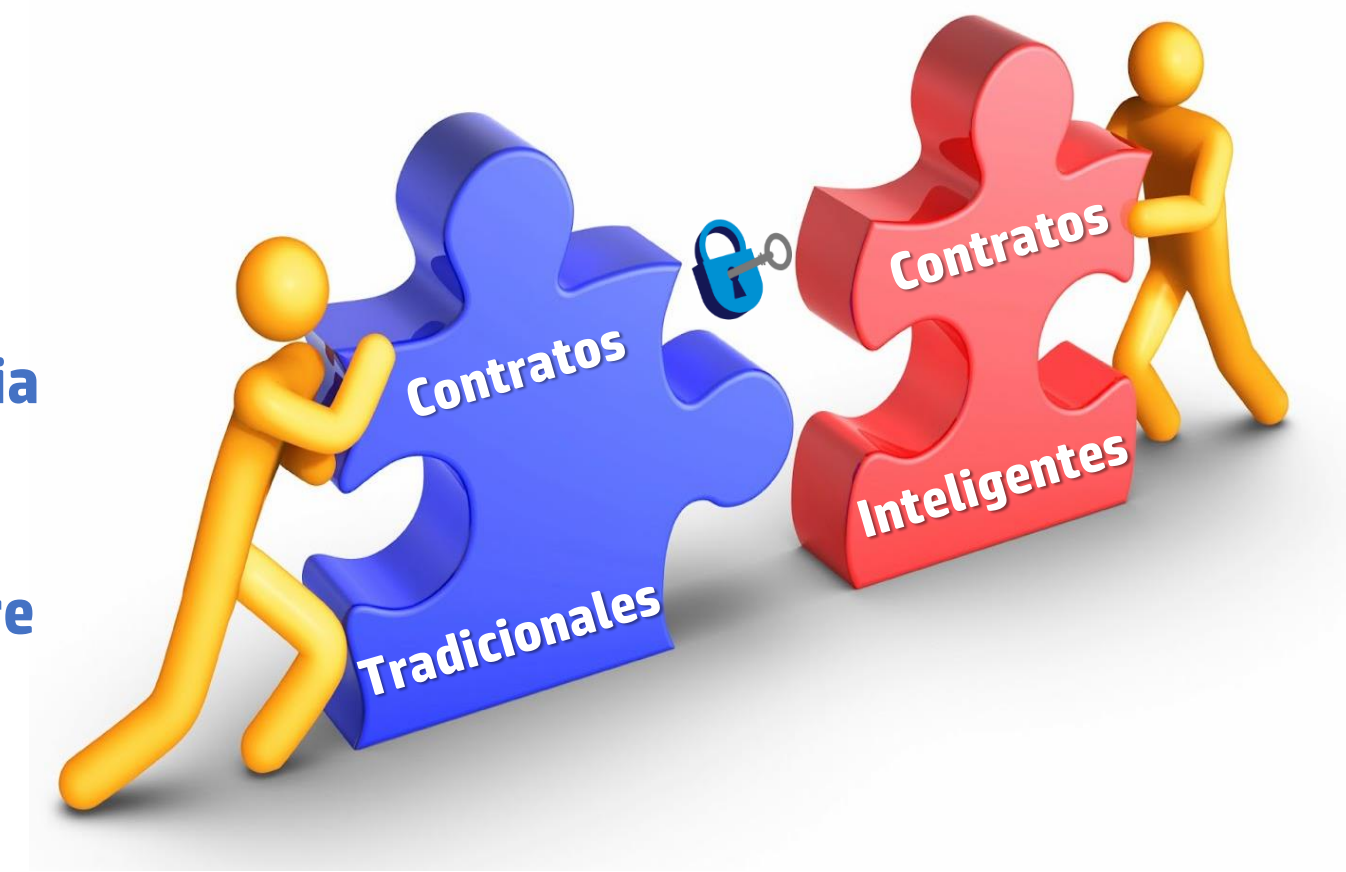
RETOS:

Consolidar su validez jurídica

Lograr su estandarización en la industria

Convertir el lenguaje legal al mundo informático

Fortalecer su seguridad y ejecución libre de errores



</lexinformatica>
</abogados>

GRACIAS

@JoelGomezMX

Joel A. Gómez Treviño

Lex Informática Abogados, S.C.

Academia Mexicana de Derecho Informático, A.C.

- www.LexInformatica.com
- www.JoelGomez.Abogado
- www.amdi.org.mx
- www.AbogadoDigital.tv
- www.Abogado.Digital

Boulevard Anillo Periférico Adolfo López Mateos No.4293, Piso 3, Int. 300.
Col. Jardines de la Montaña. C.P. 14210.
Ciudad de México.

Conmutador.- (55) 4774-0597

joelgomez@lexinformatica.com

abogado@joelgomez.com

SOBRE EL AUTOR

Joel Gómez Treviño

- Es Abogado egresado del Tecnológico de Monterrey y tiene una Maestría en Derecho Internacional por la Universidad de Arizona. Es Doctor Honoris Causa. Cuenta con 24 de años de trayectoria como especialista en derecho de las tecnologías de la información, privacidad y propiedad intelectual.
- Es Presidente fundador de la Academia Mexicana de Derecho Informático y Coordinador del Comité de Derecho de las TIC y Datos Personales de la Asociación Nacional de Abogados de Empresa, Colegio de Abogados (ANADE).
- Ha recibido 18 reconocimientos (nacionales e internacionales) debido a su desempeño profesional y su contribución al crecimiento de la industria de Internet en México.
- Ha sido invitado a impartir más de 450 conferencias y cursos en programas profesionales y académicos de Brasil, Canadá, Colombia, Costa Rica, Ecuador, España, Estados Unidos, Guatemala, Italia, Panamá, México y Asia.
- Es profesor del ITESM, Universidad Panamericana, INFOTEC y UDLAP.