BANCO INTERAMERICANO DE DESARROLLO

BLOCKCHAIN

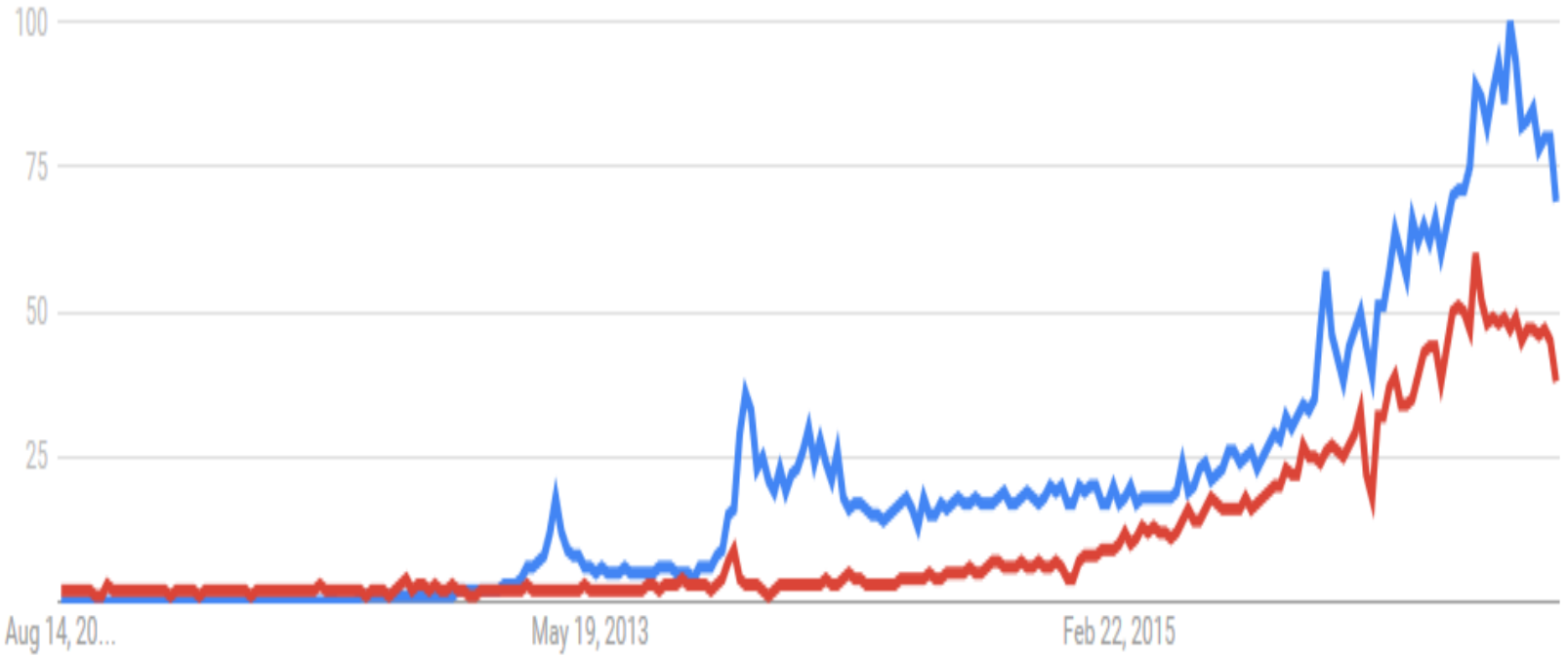
y la Tecnología de Registro Distribuida

CAPÍTULO

1. Antecedentes
2. Elementos, Funcionamiento y Tipología
3. Aplicaciones
4. Estado de la industria y perspectivas

1. Antecedentes

El interés en Blockchain se ha incrementado…



Fuente Google

1. Antecedentes

…..pero entenderlo puede ser confuso

"A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly"

Oxford Dictionary

"It's a distributed ledger shared via a peer-to-peer network that maintains an ever-expanding list of data records"

IBM

"Consists of blocks that hold timestamped batches of valid transactions. Each block includes the hash of the prior block in the blockchain, linking the two. The linked blocks form a chain, with only one (successor) block allowed to link to one other (predecessor) block, thus giving the database type its name"

Wikipedia

2. Elementos, Funcionamiento y Tipología

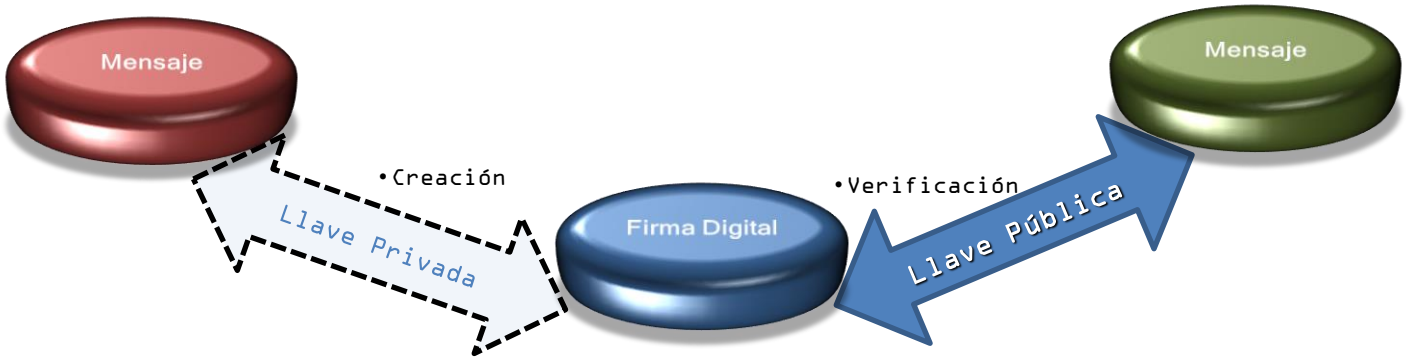
Elementos

Firmas Digitales	• Criptografía de Llave Pública • Provee privacidad y seguridad
Hashing Criptográfico	• Convierte datos de cualquier tamaño a una cadena de caracteres de tamaño fijo • Une los bloques y provee integridad de los datos
Red Distribuida	• Información distribuida a todos los nodos en la Red • Provee transparencia y resiliencia
Proof of Work (Algoritmo de Consenso)	• Requiere un esfuerzo significativo de recursos computacionales de los participantes durante el proceso de validación • Provee irreversibilidad y hace costosos a los ataques

2. Elementos, Funcionamiento y Tipología

Firma Digital

Se basa en Criptografía de llave pública/privada

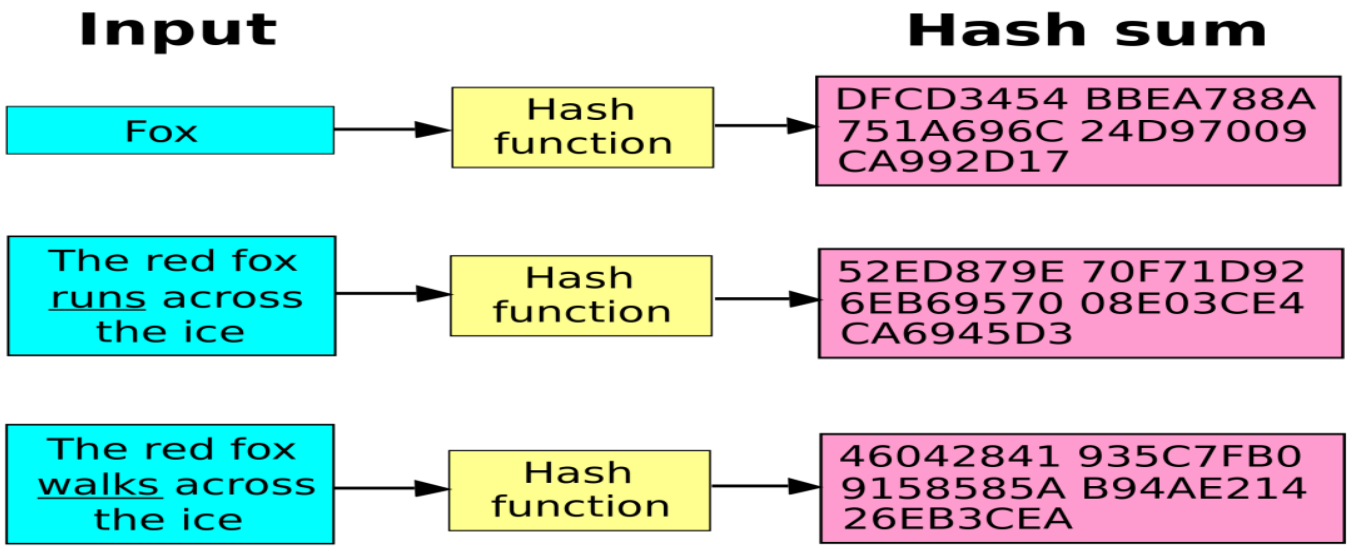


- Imposible para otros replicar la firma
- Provee privacidad y seguridad
- Si la llave privada es robada o perdida, el recipiente del mensaje puede recibir pero no enviar. El mensaje no es recuperable

2. Elementos, Funcionamiento y Tipología

Hashing Criptográfico

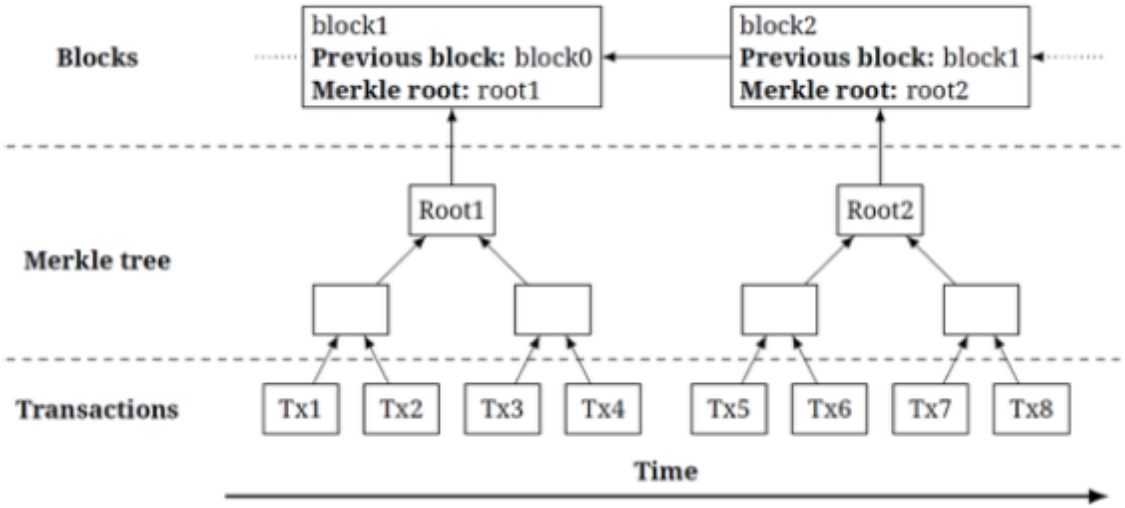
•Convierte datos de cualquier tamaño a una cadena de tamaño fijo



2. Elementos, Funcionamiento y Tipología

Hashing Criptográfico

•Encadena los bloques proveyendo integridad de datos

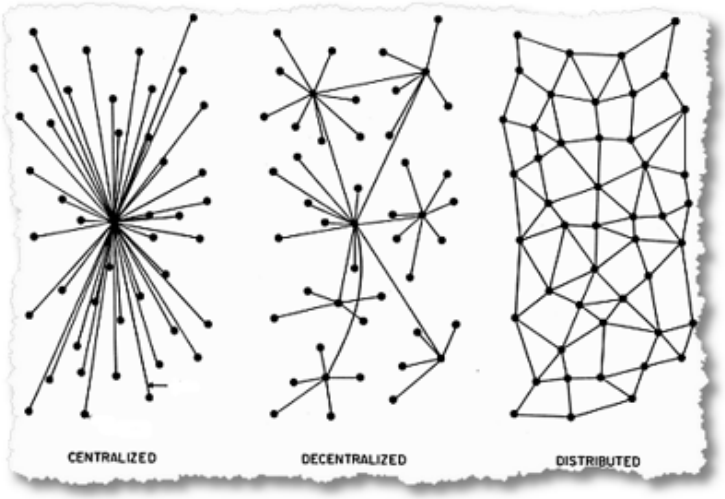


•Las transacciones no pueden ser cambiadas sin cambiar la historia previa.

2. Elementos, Funcionamiento y Tipología

Red Distribuida

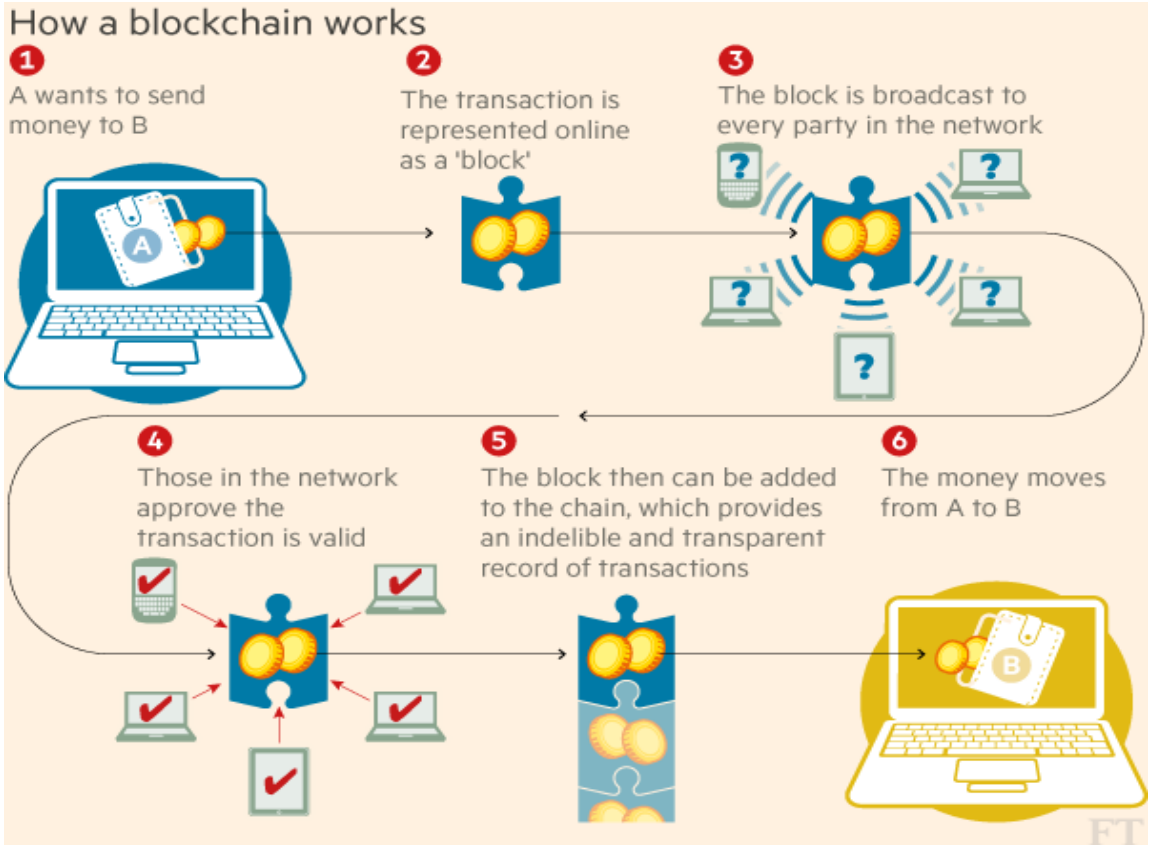
•La información está distribuida en todos los nodos de la red.
•Todos los nodos son iguales
•Provee transparencia y resiliencia



- Todos los nodos tienen una copia del libro de registro
- Para que un ataque tenga lugar, la mayoría de los nodos deberían ser controlados

2. Elementos, Funcionamiento y Tipología

Funcionamiento (Simplificado)



2. Elementos, Funcionamiento y Tipología

Tipología

Estructura

Pública vs. Privada (Consorcio)

Abierta vs. Cerrada

Sin permiso vs. Con permisos

Propósito General vs. Propósito Limitado

Validez de las transacciones

Definida por el protocolo (con o sin permisos)

vs.

Definida por el protocolo y las decisiones de los procesadores (sólo con permisos)

2. Elementos, Funcionamiento y Tipología

Tipología

Que es verificado y registrado

	Autoridad Central	Grupo de Actores conocidos	Grupo de actores (algunos conocidos)	Nadie (algoritmo matemático)
Propiedad Activos (on-platform)	Bco. Central Bco. Comercial		Ripple (XRP)	Bitcoin
Propiedad Activos (off-platform)	Bco. Custodio	Hyperledger	Ripple (Gateways)	Colored Coins
Derechos y obligaciones surgidos de acuerdos	Clearing House	Eris	Ripple (Codius)	Ethereum

Quien valida y mantiene un registro confiable

3. Aplicaciones

Intercambio de Valor

Registro digital confiable e inmutable

Contratos Inteligentes (Smart Contracts)

3. Aplicaciones

Crea un libro mayor público que sigue (monitorea) el origen, traspaso y propiedad del activo transado.

Intercambio de valor

- Pagos y Transferencias
- Envío de remesas

Registros Digitales

- Títulos de propiedad
- Registros de Salud
- Registros universitarios
- Diamantes
- Armas
- Arte
- Patentes
- Patentes de Autoría o Propiedad de contenidos digitales

3. Aplicaciones

Contratos Inteligentes (Smart Contracts)

- **Son protocolos de computación que facilitan, verifican o instrumentan la negociación y/o realización de un contrato.**

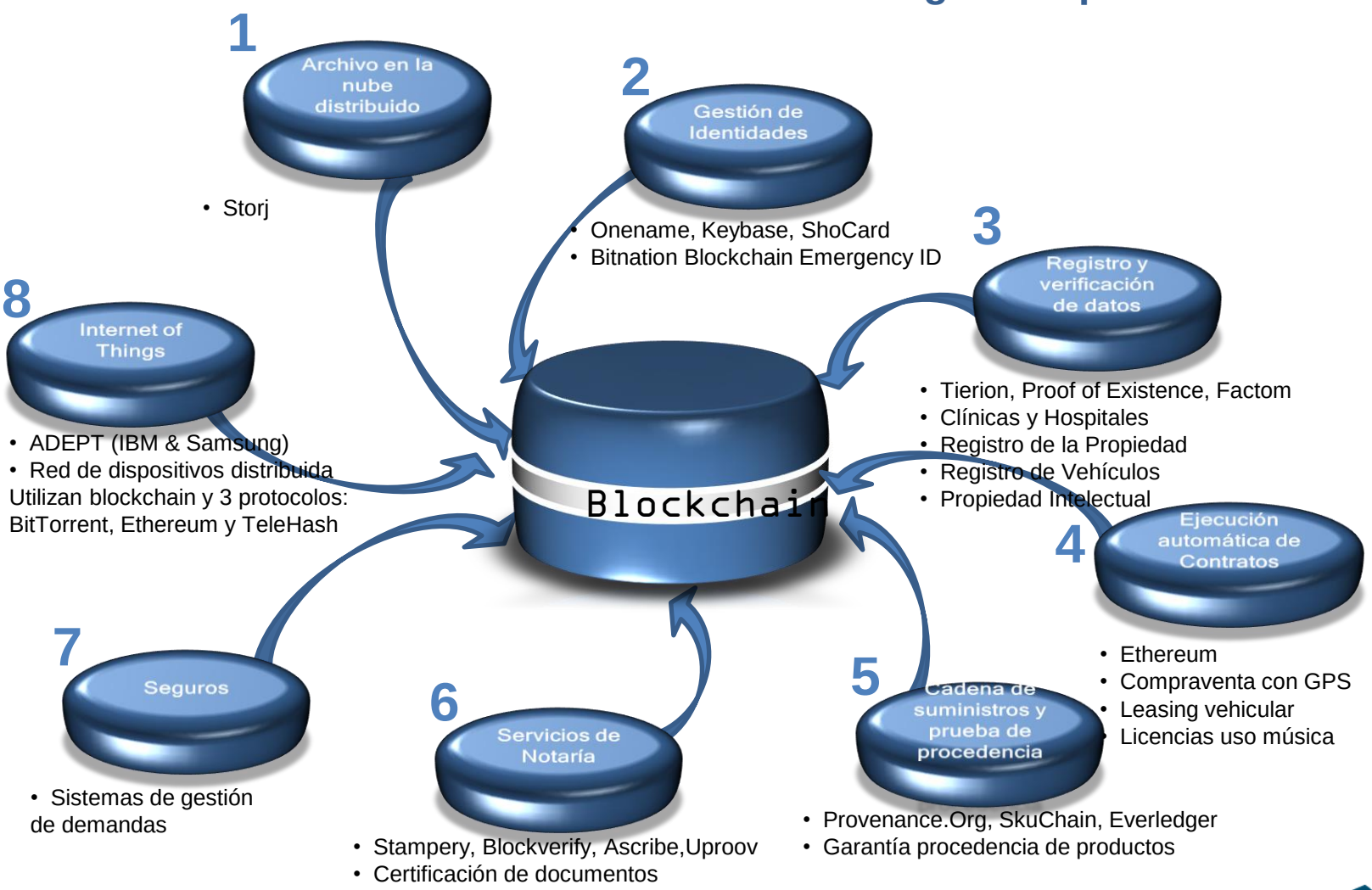
- **Dinero Programable**
- **Escrow**
- **Crowdfunding**
- **Securities (NASDAQ + Chain.com)**

Metodología para prevenir fraude en las transacciones (adicional).

Multisig

3. Aplicaciones

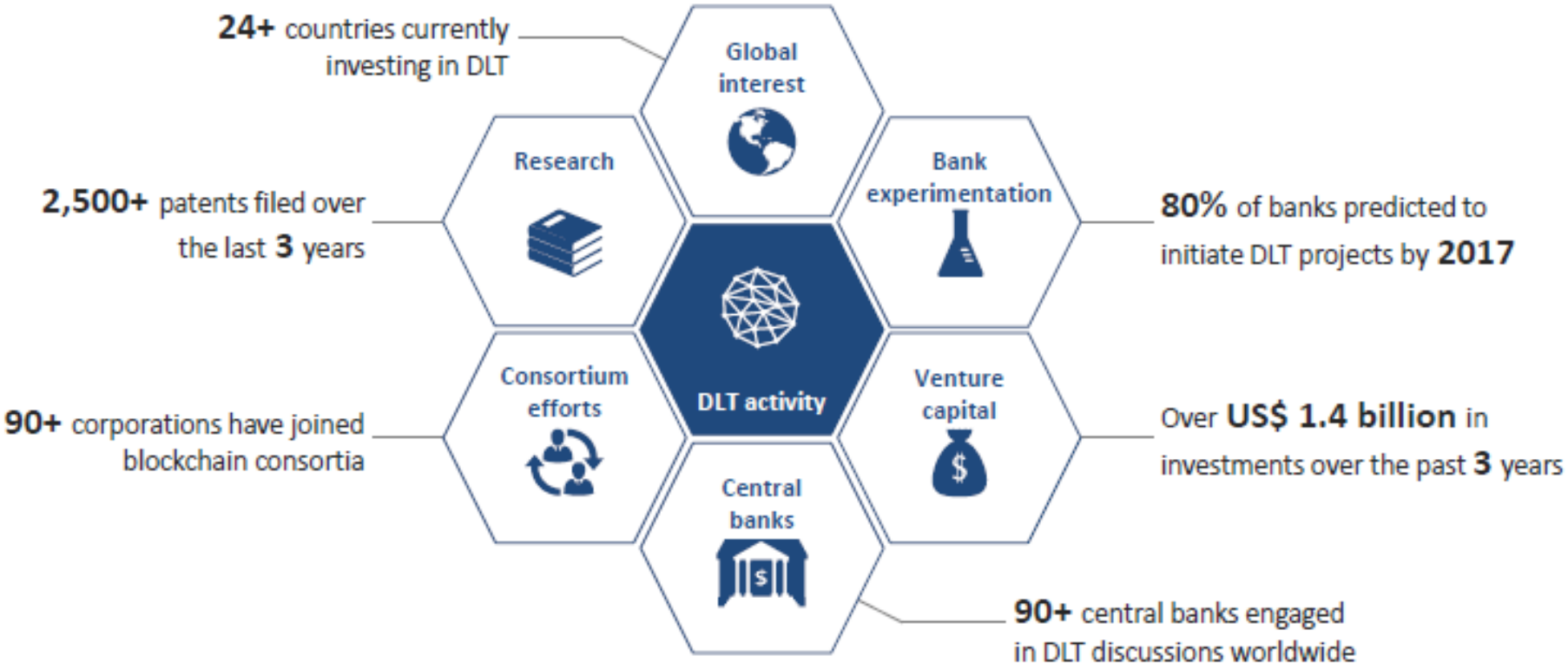
Algunas aplicaciones



4. Estado de la industria y perspectivas

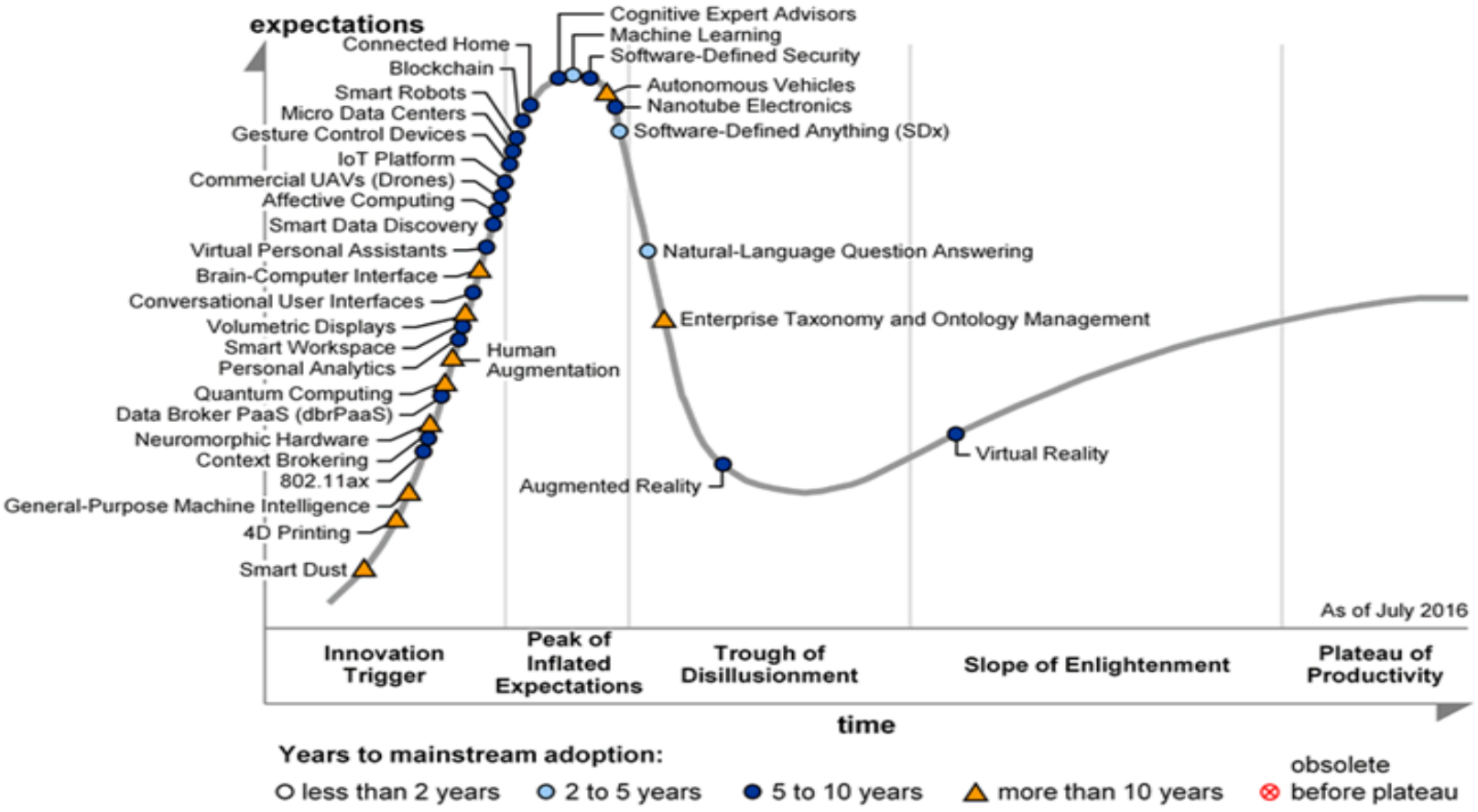
4. Estado de la industria y perspectivas

Nivel de actividad y compromiso



4. Estado de la industria y perspectivas

Perspectivas: Adopción en 5-10 años



Fuente: Hype Cicly for Emerging Technologies. Gartner (2015)

MUCHAS GRACIAS!