

**BANCO INTERAMERICANO DE  
DESARROLLO**

**BLOCKCHAIN**

**y la Tecnología de Registro Distribuida**

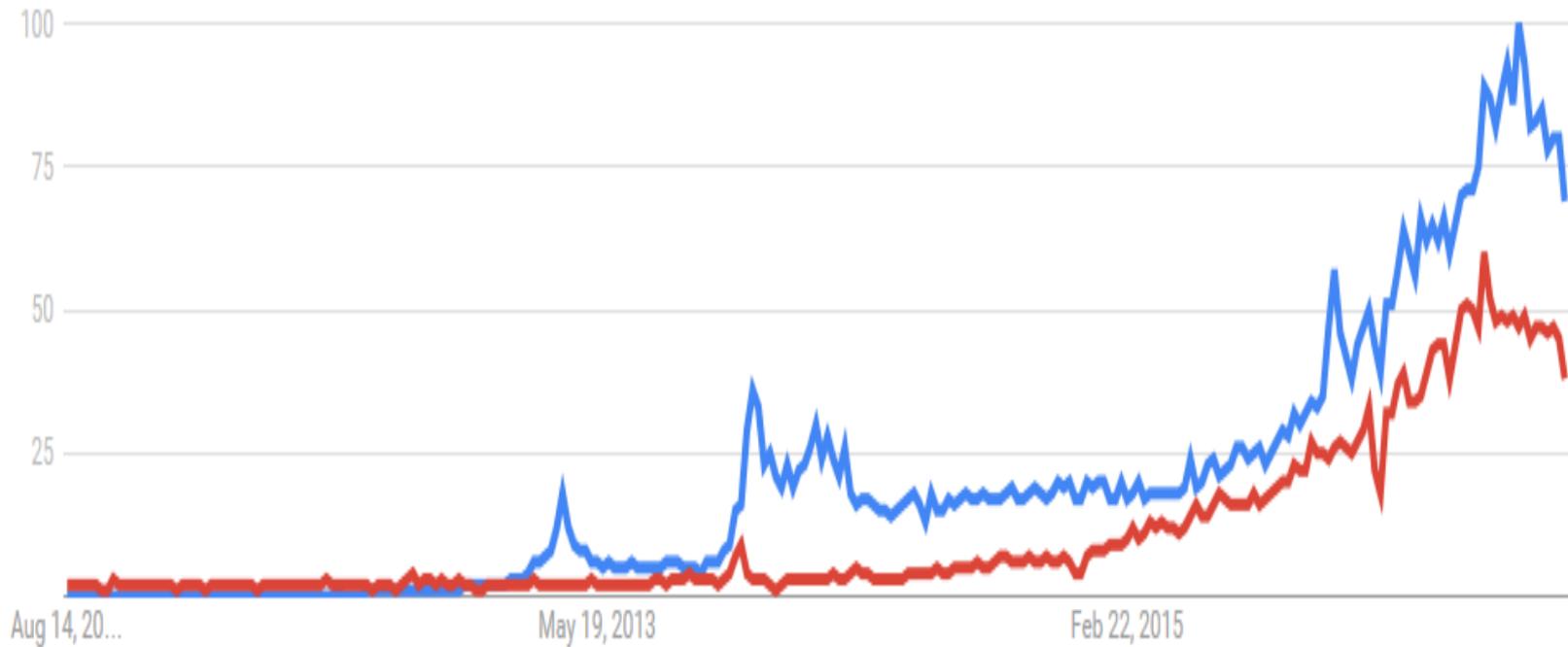


# **CAPÍTULO**

- 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

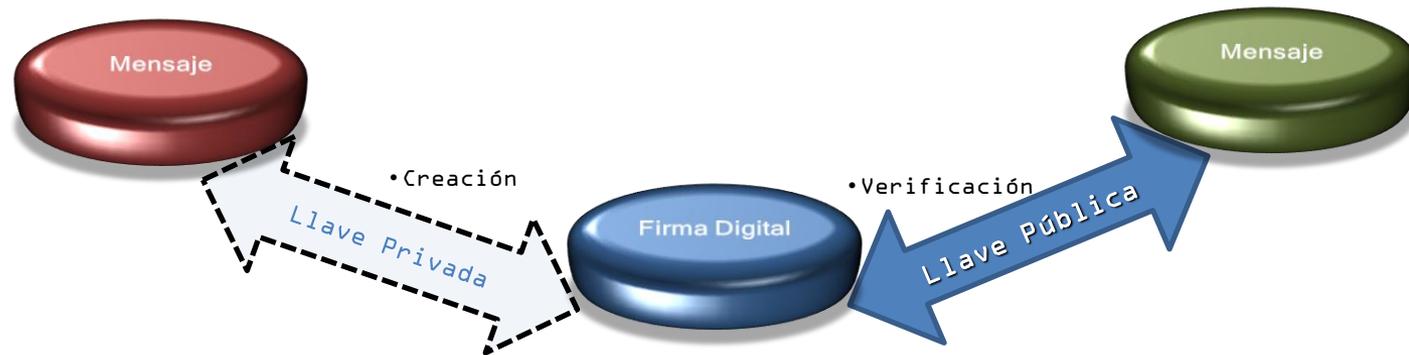
Proof of Work  
(Algoritmo de  
Consenso)

- 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

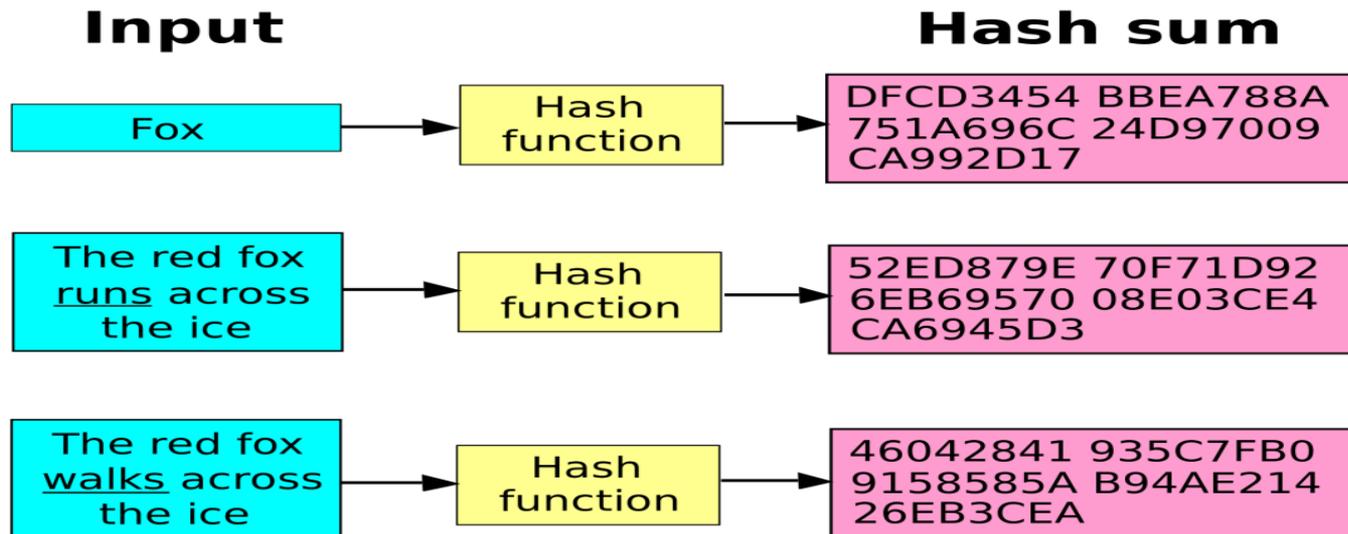


- Imposible para otros replicar la firma
- Provee privacidad y seguridad
- Si la llave privada es robada o perdida, el recipiente del mensaje puede recibir pero no enviar. El mensaje no es recuperable

## 2. Elementos, Funcionamiento y Tipología

### Hashing Criptográfico

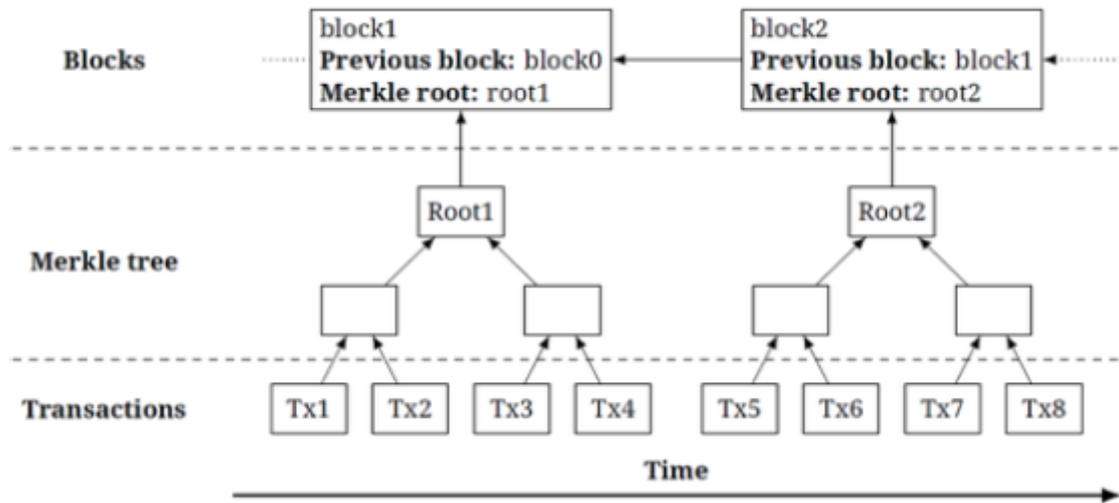
- Convierte datos de cualquier tamaño a una cadena de tamaño fijo



## 2. Elementos, Funcionamiento y Tipología

### Hashing Criptográfico

- Encadena los bloques proveyendo integridad de datos

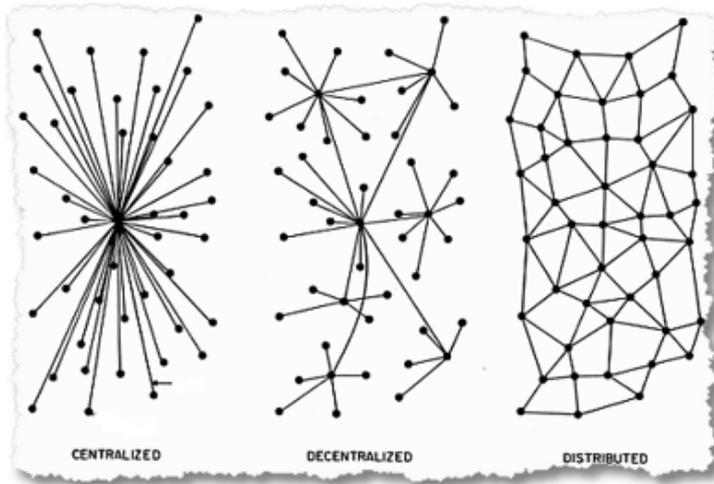


- Las transacciones no pueden ser cambiadas sin cambiar la historia previa.

## 2. Elementos, Funcionamiento y Tipología

### Red Distribuida

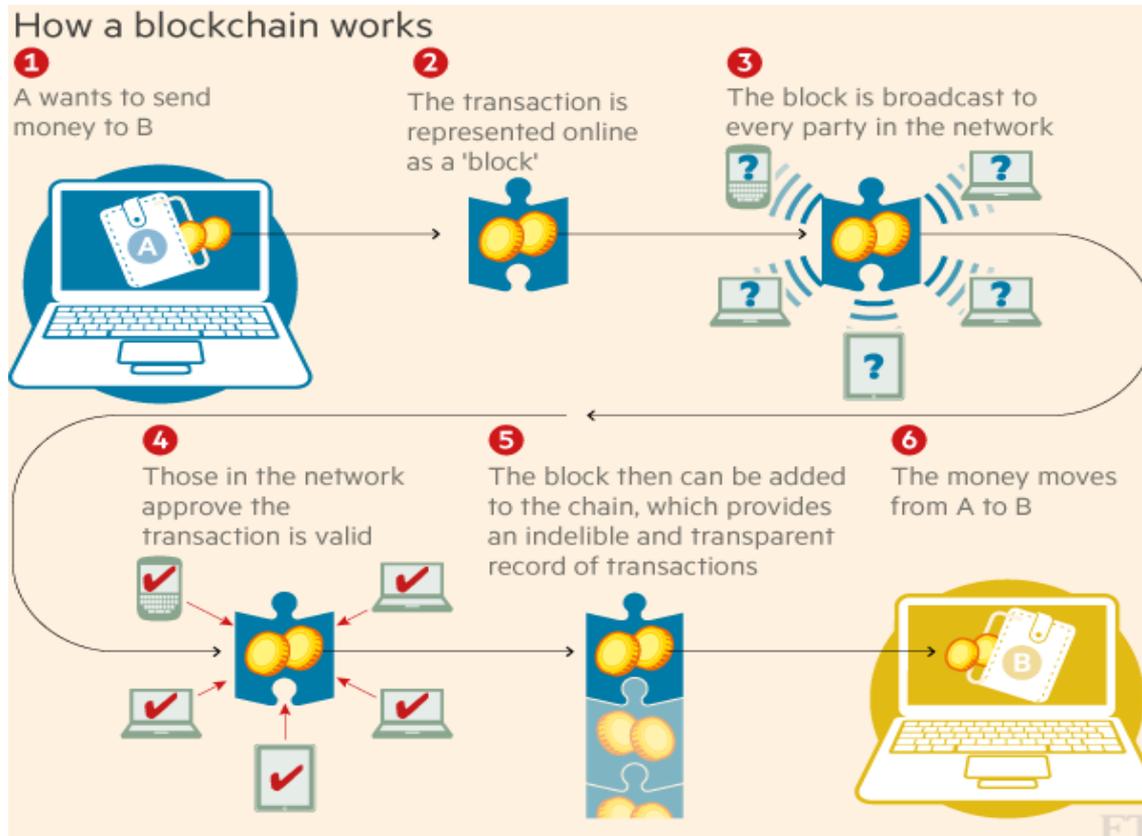
- La información está distribuida en todos los nodos de la red.
- Todos los nodos son iguales
- Provee transparencia y resiliencia



- 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 (Consortio)

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<br>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)

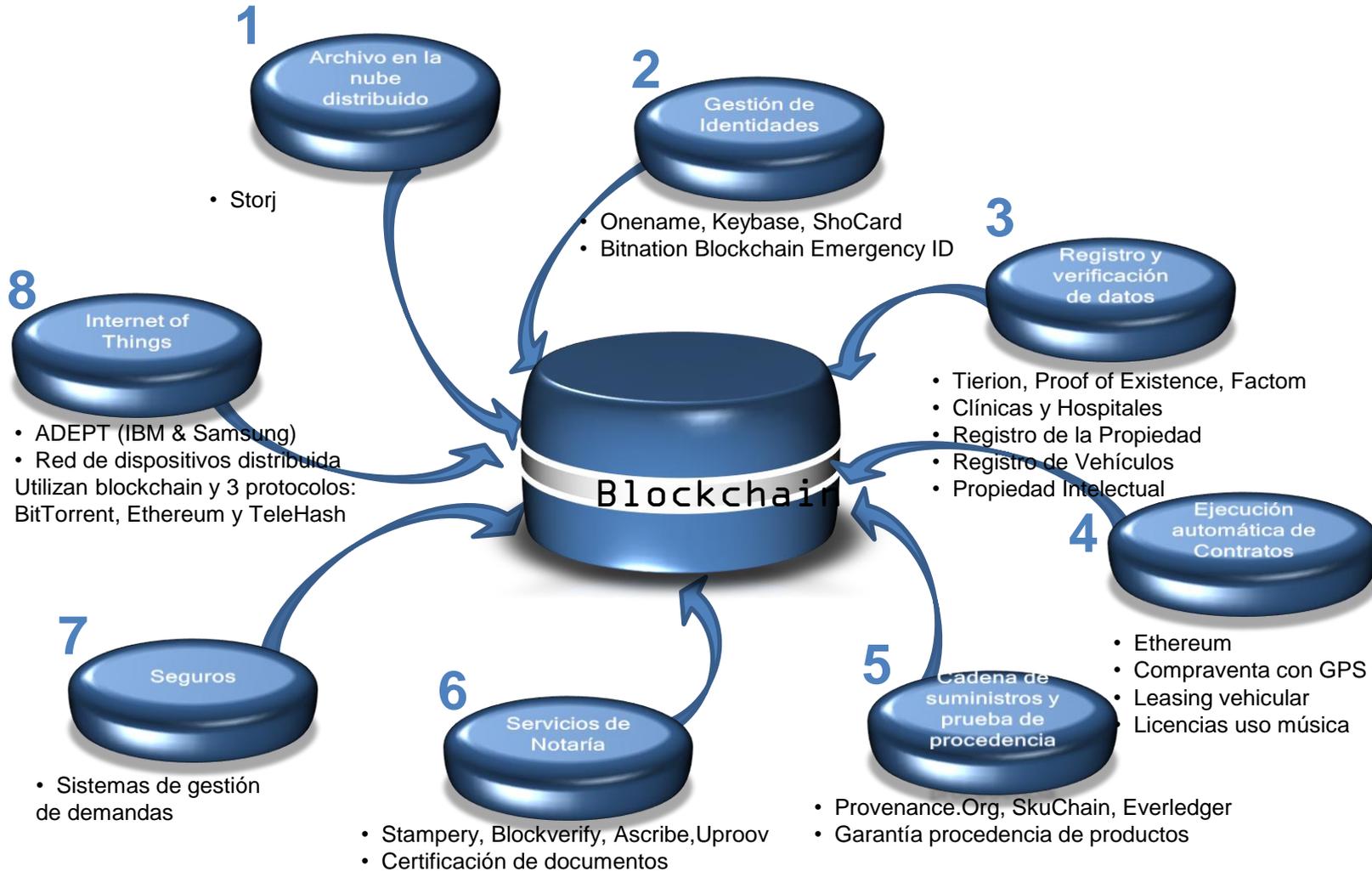
- Son protocolos de computación que facilitan, verifican o instrumentan la negociación y/o realización de un contrato.
- Dinero Programable
- Escrow
- Crowdfunding
- Securities (NASDAQ + Chain.com)

Metodología para prevenir fraude en las transacciones (adicional).

Multisig

# 3. Aplicaciones

## Algunas aplicaciones



# 4. Estado de la industria y perspectivas

## APPLICATIONS & SOLUTIONS

|  |   |  |  |  |
|--|---|--|--|--|
| <b>Brokerage</b><br>Unocoin, BIT Pagos, BTCC, BITFINEX, CIRCLE, COINJAF, QUADRIGACX, bitFlyer, safello, volabit, coinFloor, coins.ph                       | <b>Exchanges</b><br>BTER.com, coinbase, KRaken, HUOBI.com, BITSTAMP, POLONIEX, bitcoin.de, BTC, GEMINI, mexbt, CAMP BX, BITSO, Coinffeine, BitOasis, PAYMIUM, CEXIO, SHAPE SHIFT, BTC EXPRESS, coinsecure, coinsetter | <b>Soft Wallets</b><br>BLOCKCHAIN, airBitz, ARMORY, xapo, bread wallet, Coinkite, Mycelium, MultiBit HD, coinprism   | <b>Hard Wallets</b><br>TREZOR, Ledger Wallet, keep key, COSE   | <b>Investments</b><br>Grayscale, magnr, loanbase, string, Yuanbao, KOIBANK, Bitbond, WeiFund, WEALTHCOIN, lighthouse, BSAVE.IO, dangpu.com, BTCjam, CHROMA.FUND  |
| <b>Merchants</b><br>bitpay, Bitnet, Coinkite, PEY, CoinPayments, coinsnap, coinbase, CoinSimple, BIT Pagos   | <b>Compliance</b><br>ELLIPTIC, third key solutions, PROTUS, CHAINALYSIS, Sig, BLACKSEER, CryptaCorp, IdentityMind, U, VOGOGO, COINALYTICS, BLOCKVERIFY, Merkle Tree   | <b>Trading Platforms</b><br>COINIGY, HEDGY, OrderBook, tradewave, COINUT, AltOptions, COINIGY, MAKER, BITNOMIAL, TERA EXCHANGE, BITMEX, Mirror, CRYEX, 1 Broker, TABTRADER, dxmarkets, AlphaPoint, NOBLE MARKETS, HitFin | <b>Capital Markets</b><br>Chain, symbiont, NASDAQ Private Market, Digital Asset Holdings, clearmatics, itBit, TradeBlock, t0, R, epiphyte                                  | <b>Money Services</b><br>CRYPTO PAY, cashila, ABRA, Fuzo, tether, Bitwala, coins.ph, BITX, Simplex, ATLAS, coinx, R<BIT, uphold, BITEXO, CoinPip, DUO MONEY, LocalBitcoins.com, BitPesa, BlinkTrade, COINAPULT, MELOTIC, Glidera, bridge21 |
| <b>Financial Data</b><br>bitcoinity, CoinMarketCap, CryptoCoin, BRAVENEW.COIN, BlockJockey, CRYPTO TRADER, BitcoinWisdom, TradeBlock, CoinGecko, Coinhills | <b>Payments</b><br>Align Commerce, About Payments, COIN, BLADE, GAZEBO.IO, GemPay, cuber, SETL.io, safe cash  | <b>Payroll &amp; Insurance</b><br>paybits, bitWAGE, DYNAMIS  | <b>ATMs</b><br>LocalBitcoins.com, Robocoin, bitxatm, bitaccess, Project Skyhook, btcpoint, SERV, LAMASSU BITCOIN VENTURES, GB, genesiscoin, COINOUTLET, Modenero Concierge | <b>Banks</b><br>BBVA, UBS, LHV, London Stock Exchange, secco, BNY MELLON, BARCLAYS, fidor BANK, citibank, moni   |
| <b>Trade Finance</b><br>GAZEBO.IO, everledger, CHRONICLED, WAVE, thingchain, PROVENANCE  | <b>Trade Finance</b><br>GAZEBO.IO, everledger, CHRONICLED, WAVE, thingchain, PROVENANCE   | <b>Trade Finance</b><br>GAZEBO.IO, everledger, CHRONICLED, WAVE, thingchain, PROVENANCE  | <b>Trade Finance</b><br>GAZEBO.IO, everledger, CHRONICLED, WAVE, thingchain, PROVENANCE  | <b>Trade Finance</b><br>GAZEBO.IO, everledger, CHRONICLED, WAVE, thingchain, PROVENANCE  |

## MIDDLEWARE & SERVICES

|   |   |   |  |   |   |
|---|---|---|--|---|---|
| <b>Services</b><br>CRYPTONOMEX, B9, CONSENSYS, SolidX, appliedblockchain, RUBIX | <b>Software Development</b><br>chainscript, HydraChain, Blockstack.io, PEERNOVA, CREDITS, eris, Manifold, Blockstream | <b>General APIs</b><br>BitGo, neuroware, coinbase, bitcore, Coinkite, BLOCKCYPHER | <b>Special APIs</b><br>TIERION, Open Assets, bitbind.io, factom, chromaWay | <b>Platforms</b><br>Counterparty, Monetas, blockstack, HYPERLEDGER, BLDHAPPS, appliedblockchain, Tendermint | <b>Smart Contracts</b><br>SmartContract, CoinSpark, ROOTSTOCK, bitShares, Tembusu Systems |
|---|---|---|--|---|---|

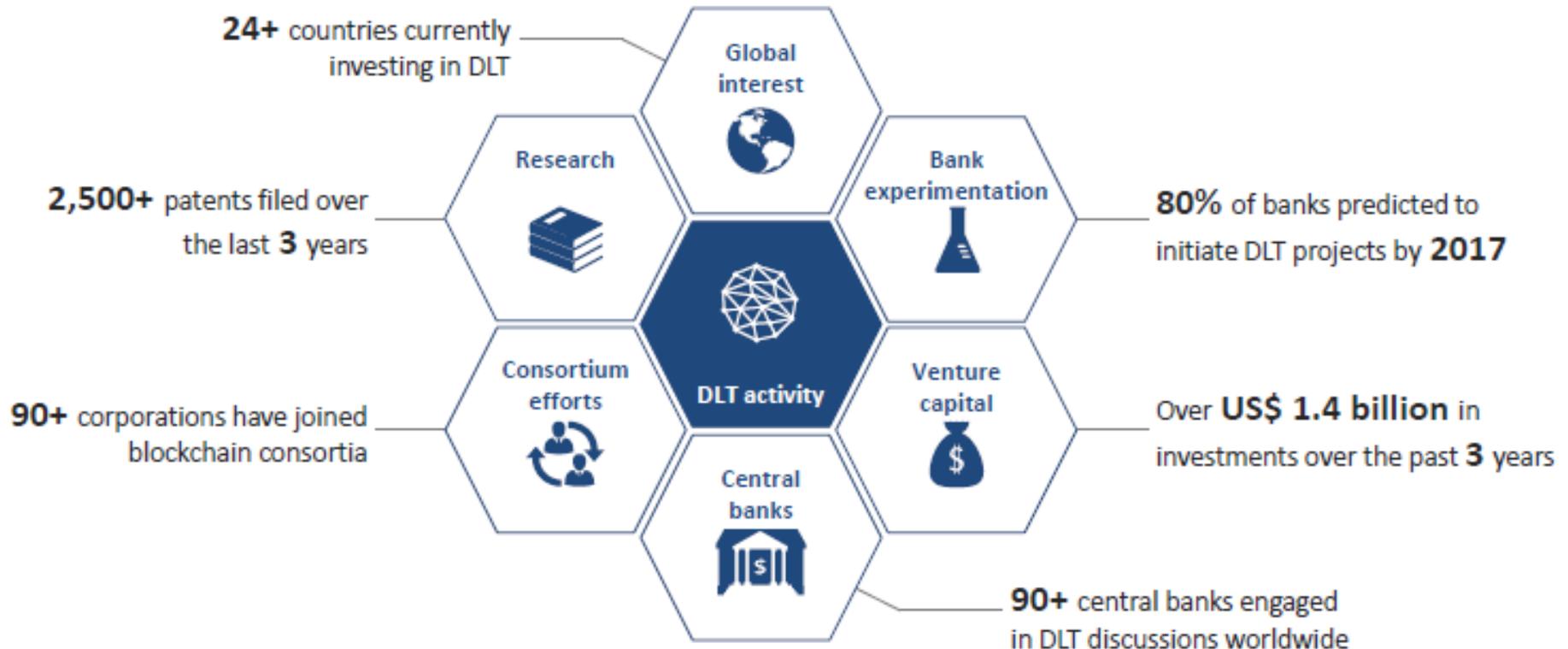
## INFRASTRUCTURE & BASE PROTOCOLS

|  |                                   |   |   |
|--|-----------------------------------|---|---|
| <b>Public</b><br>bitcoin, btshares, ethereum | <b>Special</b><br>ripple, stellar | <b>Payment</b><br>Lightning Network, MONERO | <b>Miners</b><br>ANTPOOL, BitFury, 21 INC, BTCC, BITCOIN CZ |
|--|-----------------------------------|---|---|



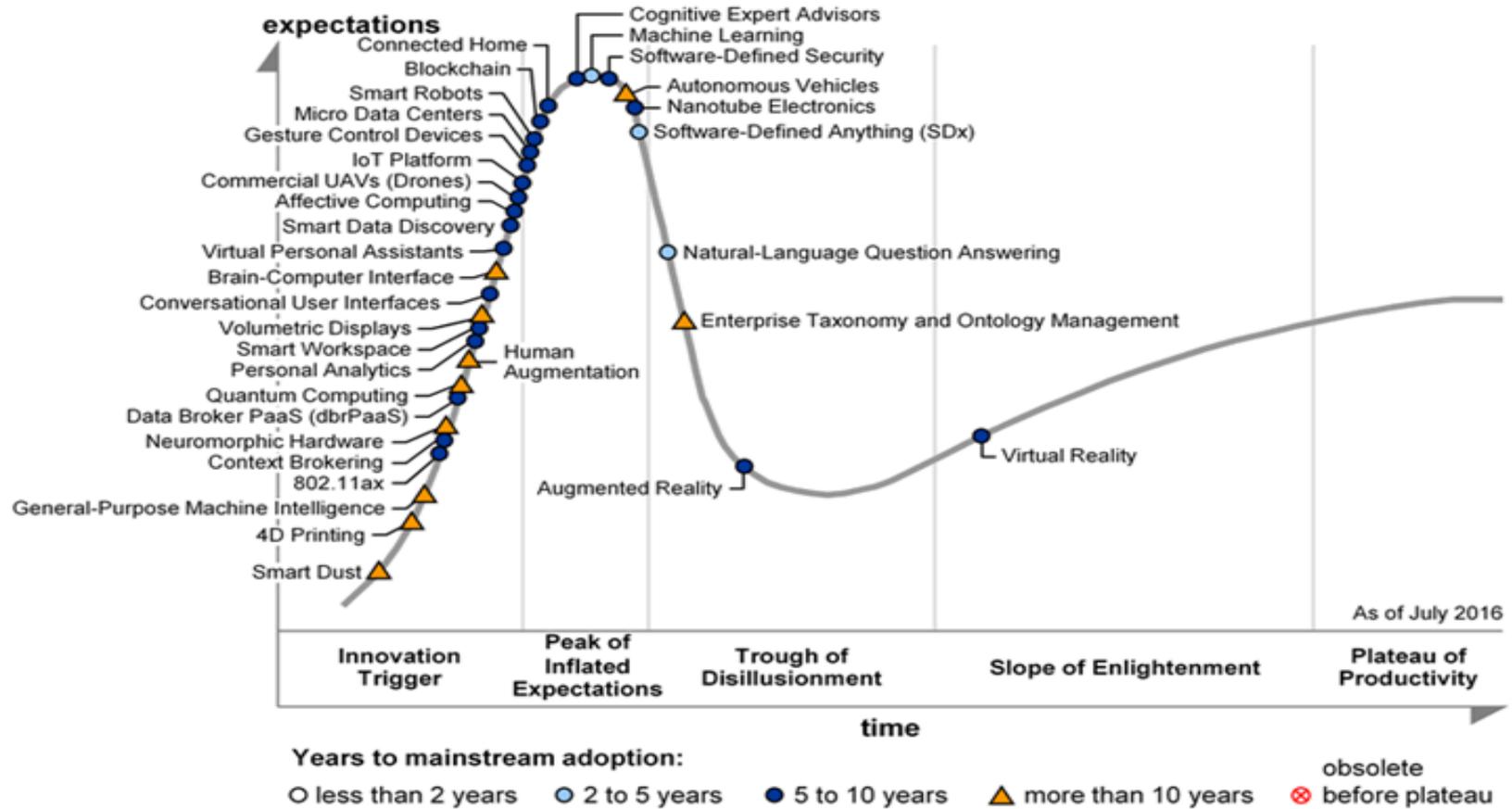
## 4. Estado de la industria y perspectivas

### Nivel de actividad y compromiso



## 4. Estado de la industria y perspectivas

### Perspectivas: Adopción en 5-10 años



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

**MUCHAS GRACIAS!**

