El futuro digital es de todos

MinTIC

Blockchain & analítica de datos

para industrias digitales

etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business

Agenda

- Actividad Mecanismos de consenso: las reglas de juego de la descentralización (PoS / BFT / PoET).
- Contexto de las billeteras (wallets) almacenamiento de criptomonedas. Recomendaciones y técnicas de seguridad

El futuro digital es de todos

MinTIC

Forbes BLOCKCHAIN 50 2021

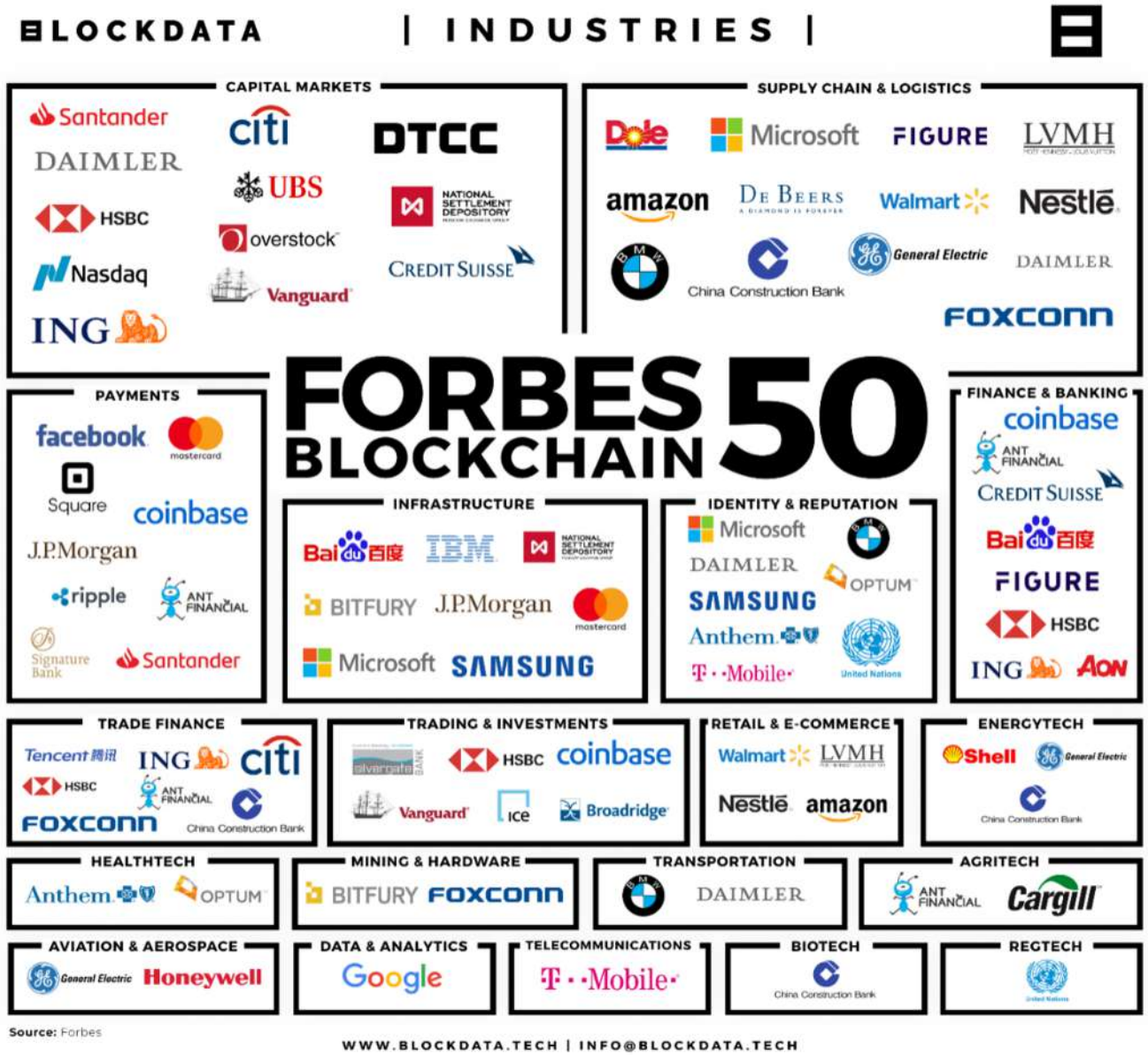
etraining
Diseñamos nuevas formas de aprender

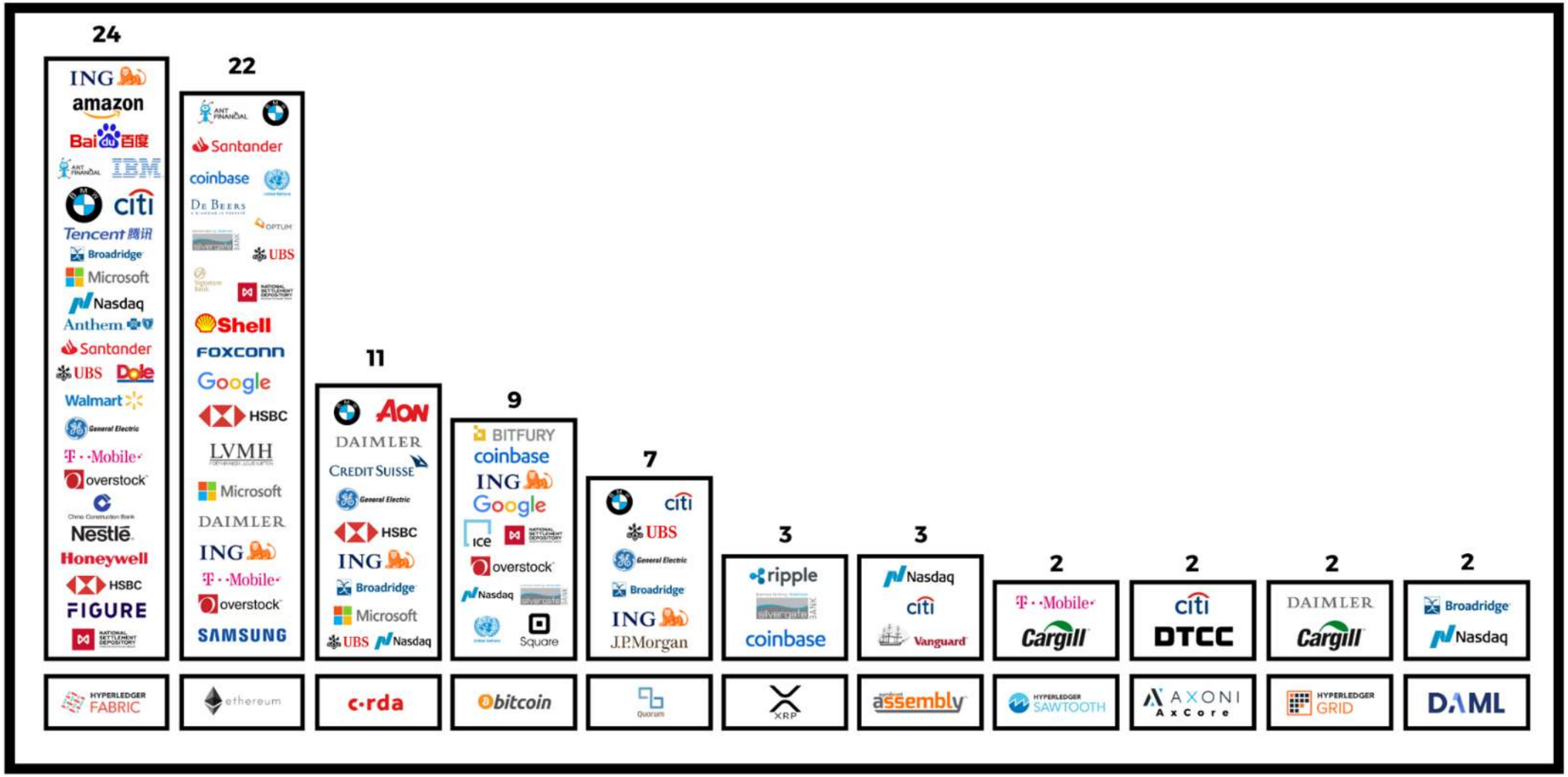
tecnalia Colombia
Inspiring Business

No longer dismissed as a haven for criminals and drug dealers, Bitcoin and blockchain have gone mainstream. Bitcoin's 2020 surge grabbed the attention of C-suite executives worldwide; not only are companies employing the technology underlying Bitcoin to perform tasks such as reconciling invoices and verifying product provenance, but dozens are now holding Bitcoin as a treasury asset. Our third annual Blockchain 50 features companies that lead in employing distributed ledger technology and have revenue or a valuation of at least $1 billion. Twenty-one newcomers—including the world's largest bank, the Industrial and Commercial Bank of China, and four others from Asia—make their debut. They take the spots of such U.S. companies as Facebook, Google, Amazon and Ripple, all of whom are still active in blockchain but kept lower profiles in the space over the past 12 months.

El Bitcoin y la cadena de bloques ya no se consideran un refugio para delincuentes y narcotraficantes, sino que se han convertido en la tendencia principal. El auge de Bitcoin en 2020 atrajo la atención de los directivos de todo el mundo; no solo las empresas emplean la tecnología subyacente a Bitcoin para realizar tareas como la conciliación de facturas y la verificación de la procedencia de los productos, sino que docenas de ellas tienen ahora Bitcoin como activo de tesorería. Nuestro tercer Blockchain 50 anual presenta a las empresas que lideran el empleo de la tecnología del libro mayor distribuido y tienen ingresos o una valoración de al menos 1.000 millones de dólares. Veintiún recién llegados -entre ellos el mayor banco del mundo, el Banco Industrial y Comercial de China, y otros cuatro de Asia- hacen su debut. Ocupan los puestos de empresas estadounidenses como Facebook, Google, Amazon y Ripple, todas ellas activas en el ámbito de la cadena de bloques, pero con un perfil más bajo en los últimos 12 meses.

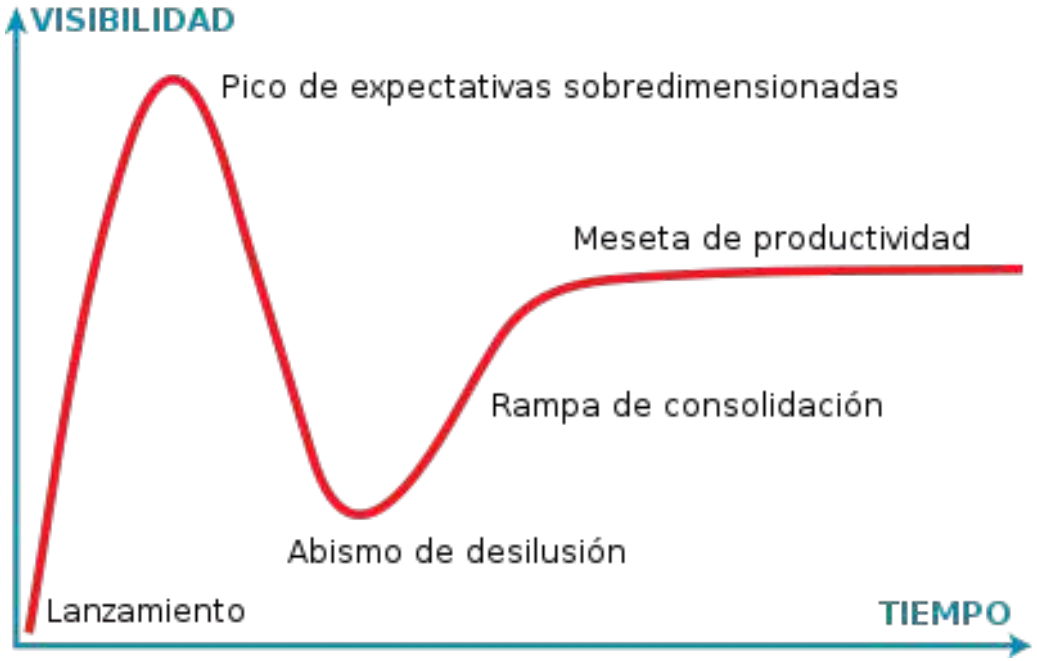
El futuro digital es de todos





Source: Forbes

Gartner Hype Cycle



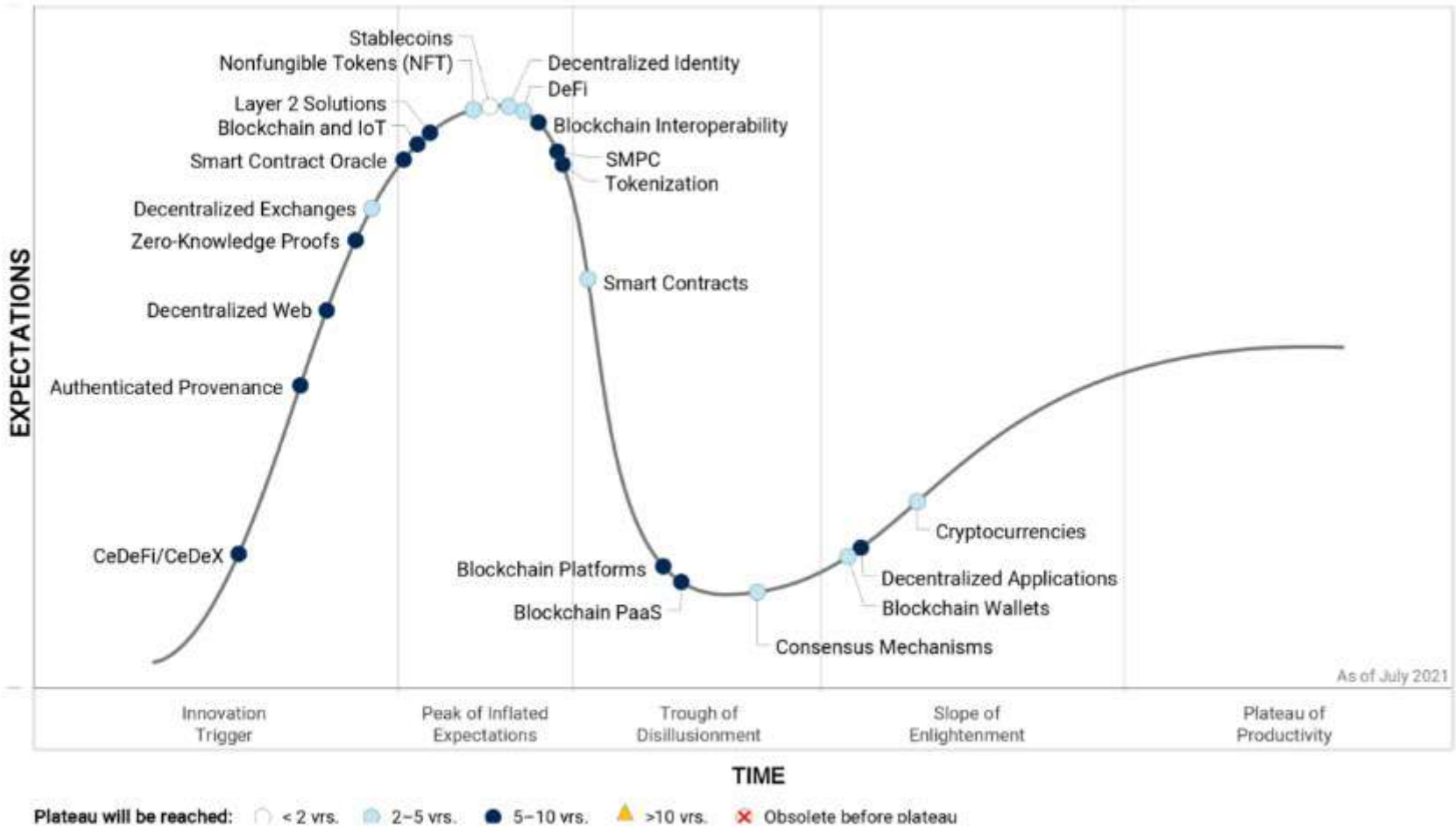
Ciclo de sobre expectación

Es una representación gráfica de la madurez y la adopción de tecnologías y aplicaciones, y cómo son potencialmente relevantes para resolver problemas comerciales reales y explotar nuevas oportunidades.

La metodología Gartner Hype Cycle le brinda una visión de cómo evolucionará una tecnología o aplicación con el tiempo, proporcionando una fuente sólida de información para administrar su implementación dentro del contexto de sus objetivos comerciales específicos.

El futuro digital es de todos

Hype Cycle for Blockchain, 2021



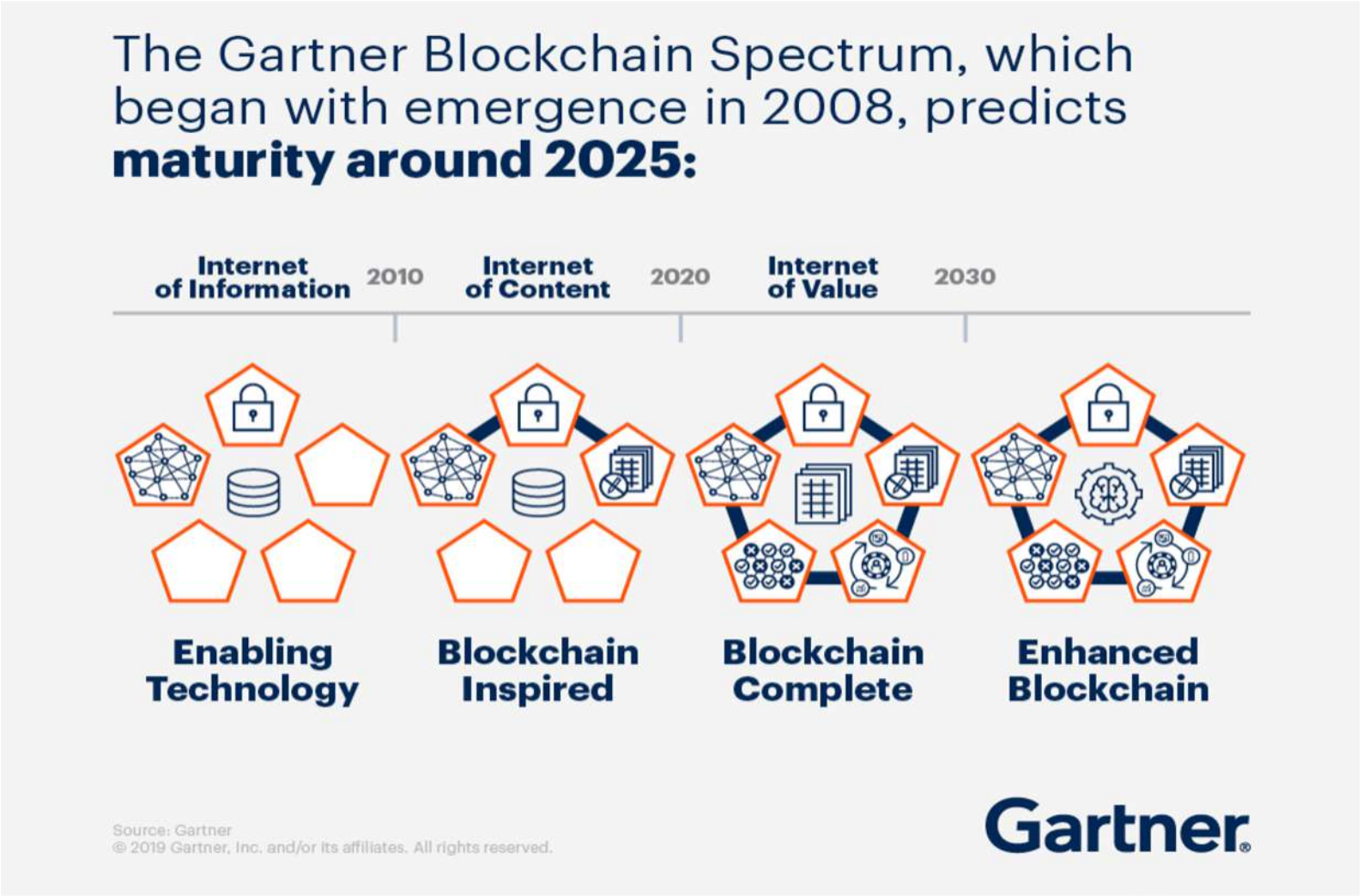
Source: Gartner (July 2021)

747513

El futuro digital es de todos

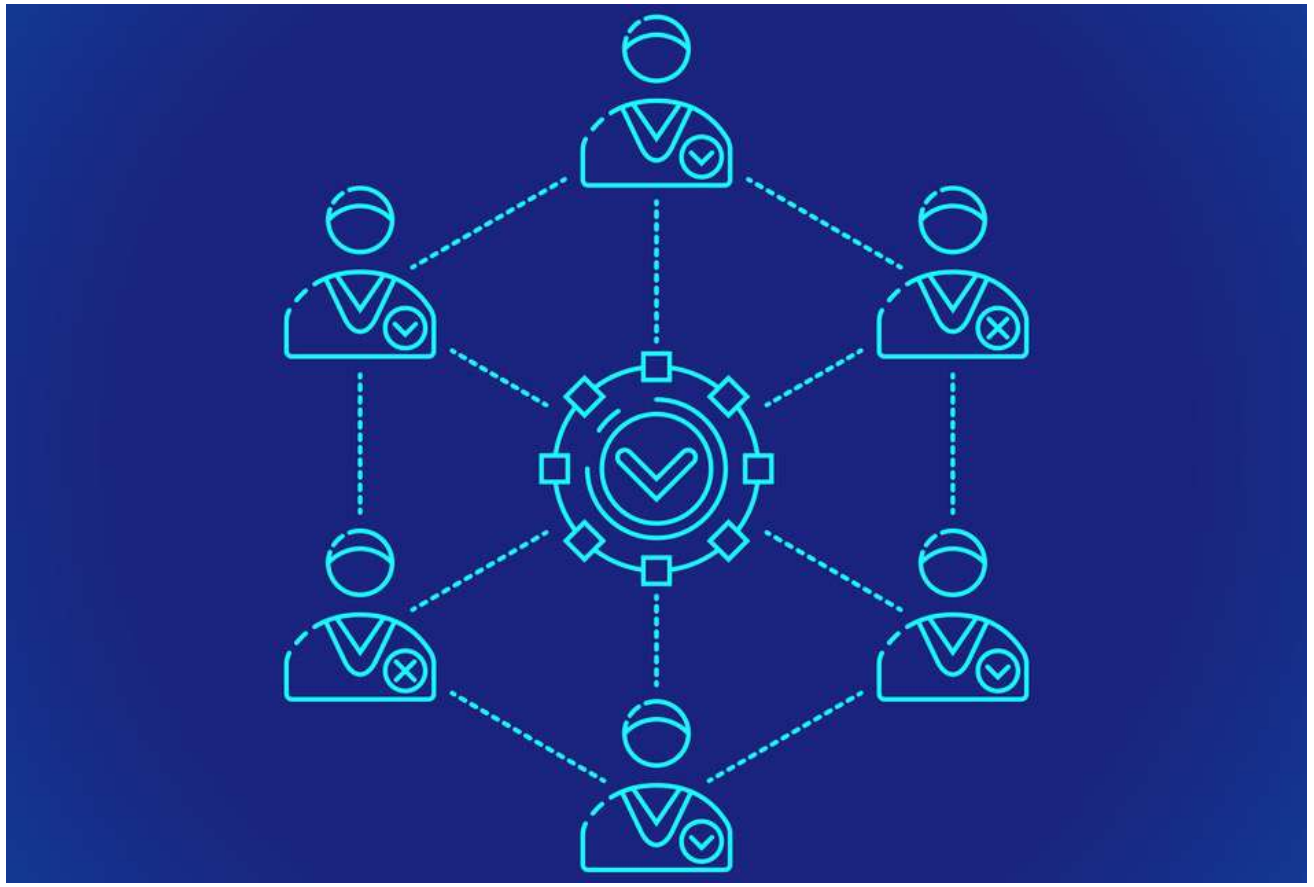
MinTIC

¿QUÉ IMPACTO TENDRÁ Y CUÁNDO?



¿QUÉ ES CONSENSO

El consenso es la aceptación por todos los miembros de la red blockchain de que la información que hay en la misma. De esta forma, todos en la red aceptan que la información no tiene manipulaciones ni datos erróneos o duplicados.



REQUISITOS DE LOS MECANISMOS DE CONSENSO

Hay varios requisitos que deben cumplirse para proporcionar los resultados deseados en un mecanismo de consenso. A continuación se describen estos requisitos:

- **Acuerdo:** Todos los nodos honestos deciden sobre el mismo valor
- **Terminación:** Todos los nodos honestos terminan la ejecución del proceso de consenso y finalmente llegan a una decisión
- **Validez:** El valor acordado por todos los nodos honestos debe ser el mismo que el valor inicial propuesto por al menos uno honesto
- **Tolerante a fallas:** el algoritmo de consenso debería poder ejecutarse en presencia de nodos defectuosos o maliciosos **(nodos bizantinos)**
- **Integridad:** este es un requisito de que ningún nodo puede tomar la decisión más de una vez en un solo ciclo de consenso.

TOLERANCIA A FALTAS BIZANTINAS (BFT)

- Es la propiedad de un sistema que puede resistir la clase de fallas derivadas del problema del dilema de los generales bizantinos.
- Esto significa que un sistema BFT puede continuar funcionando incluso si algunos de los nodos fallan o actúan maliciosamente.

Different Types of Blockchain Consensus Algorithm

1. Proof-of-Stake
2. Proof-of-Work
3. Delegated Proof-of-Stake
4. Proof of Elapsed Time
5. Leased Proof-Of-Stake
6. Simplified Byzantine Fault Tolerance
7. Proof-of-Importance
8. Proof-of-Capacity
9. Practical Byzantine Fault Tolerance
10. Proof-of-Burn
11. Proof-of-Weight
12. Proof-of-Activity
13. Directed Acyclic Graphs
14. Delegated Byzantine Fault Tolerance

Blockchain Council
www.blockchain-council.org

EJERCICIO 1

BLOQUE

METADATA (LA DEFINICION)

PRE HASH (EL CONCEPTO DEL BLOQUE ANTERIOR)

HASH (EL CONCEPTO DEL BLOQUE ACTUAL)

BLOQUE 1

EP DPCGTPDP GYM TXBADFMYFP ÑMYFTOMO OP PYPDRTM BAD BMDFP OP WAE XTYPDAE

PRE HASH (Métodos de consenso)

HASH (Proof of Work)

BLOQUE 2

EDP PWPRTOA ETRGTPYFP NWACGP OPBPYOP OP WM ÑMYFTOMO OP XAYPOME CGP EP FPYRMY PY PW ETEFPXM

PRE HASH (Proof of Work)

HASH (Proof of Stake Pos)

BLOQUE 3

PE GYM ÑAXNTYMÑTAY OP BAI K BAE

PRE HASH (Proof of Stake)

HASH Delegated proof stake (DPOS)

BLOQUE 4

PW WTOPD PE DPEBAYEMNWP OP HMWTOMD WME FDMYEMÑÑÑTAYPE

PRE HASH Delegated proof stake (DPOS)

HASH Leader Based Concensus (LBC)

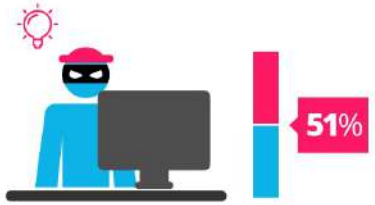

BLOCKCHAIN & CRYPTO 101
WHAT IS
PROOF OF
STAKE
BINANCE
ACADEMY

El futuro digital es de todos

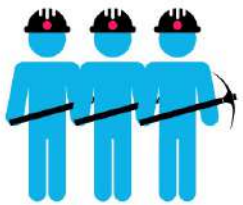
MinTIC

Prueba de Trabajo VS Prueba de Participación

La Prueba de Trabajo es un costos calculo computacional, también llamado minería.



Una recompensa es otorgada al primer minero en resolver el problema de cada bloque.



Los mineros compiten por ser el primero en resolver el problema matemático.

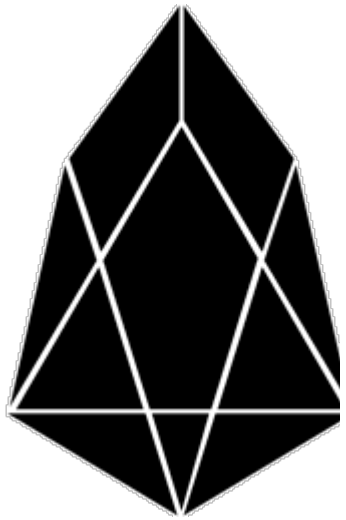
En la Prueba de Participación, la creación de un nuevo bloque es elegida de forma determinística, dependiendo de la riqueza, también definida como stake.

En El sistema PoS no hay recompensa por lo que los mineros se quedan con las comisiones de transacción.

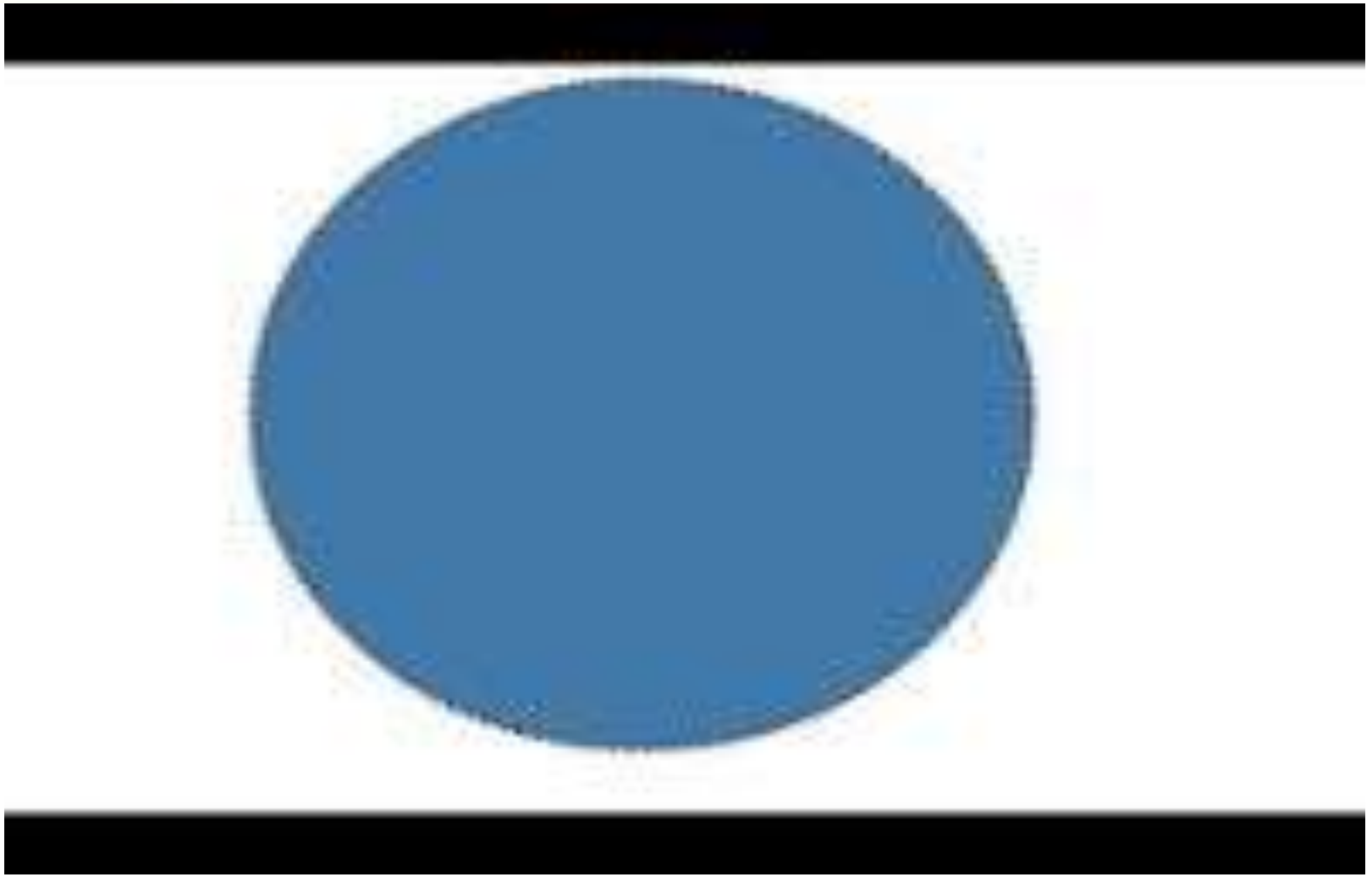
La concurrencia de la Prueba de Participación es mil veces mas económica.

DPOS

- Los delegados definen una rotación de líderes. Esto significa que cada delegado, tiene un turno dentro de la rotación para producir un bloque. Gracias a esta acción, dicho delegado puede generar un bloque y cobrar una recompensa por ello. Si el delegado no está disponible cuando llega su turno, debe esperar a uno nuevo.
- El poder de voto de cada participante de la red es proporcional a su participación en la misma. Esta característica, es parte de su relación con el protocolo de consenso de Prueba de Participación. Para favorecer la descentralización, es habitual que las redes basadas en DPoS sometan a votación decisiones relacionadas con su funcionamiento. Temas como las recompensas, la cantidad de delegados el comportamiento ante bifurcaciones de la red y otras. Además de que permiten penalizar a los delegados si no se comportan de acuerdo a lo esperado.



Lisk



¿QUÉ ES UNA BILLETERA?

El término wallet hace referencia a una cartera, billetera o monedero virtual en el que podemos gestionar nuestros activos criptográficos. Es un software o hardware diseñado exclusivamente para almacenar y gestionar las claves públicas y claves privadas de nuestras criptomonedas.

TIPO BILLETERAS

Cold Wallet

Hot Wallet

TIPO BILLETERAS

- **Desktop Wallet:** Solo nos permite el acceso desde un Pc, lugar donde debemos descargarla e instalarla. Te permite crear y almacenar tu clave privada y dirección pública para administrar tus criptomonedas. Tiene un nivel de seguridad mayor al de otros tipos de carteras ya que puedes conectarla o desconectarla de la red.
- **Mobile Wallet:** Cómo su nombre indica, estos wallets solo pueden ejecutarse con un smartphone. Están basadas en aplicaciones, comparten el mismo sistema de interfaz de usuarios y son creadas para ser soportadas por sistemas operativos Android o IOS. Tiene la ventaja de que ofrece una mayor movilidad, ya que puedes llevarla siempre contigo y utilizarlas desde cualquier ubicación en la que te

- **Web Wallet:** Wallet o cartera de criptomoneda almacenada en la nube. Se basa en aplicaciones web, lo que te permite acceder desde cualquier dispositivo con conexión. Es un tipo de cartera más vulnerable al estar almacenada en la nube, ya que se encuentra en conexión a la red, e implica el control por parte de terceros que gestionan el servidor.
- **Paper Wallet:** Pertenece a las Wallets en frío y ofrecen una mayor seguridad. Se trata de una billetera impresa en papel que contiene las claves y direcciones para administrar tus criptomonedas. Funcionan mediante la generación de códigos QR y su creación es muy sencilla. A través de software o plataforma online.
- **Hardware wallet:** Son las carteras frías que comentamos anteriormente. Normalmente tienen forma de USB y guarda las claves para acceder a tus criptomonedas de la forma más segura, al no tener conexión a la red. Podemos encontrar diferentes tipos de billeteras digitales según su tipo de conexión, capacidad de almacenamiento o capacidad de transacción.

El futuro digital es de todos

MinTIC

Gracias

etraining
Diseñamos nuevas formas de aprender

tecnalia Colombia
Inspiring Business