

BAJO LA LUPA

BLOCKCHAIN, CRIPTO, DeFi & MÁS

BLOCKCHAIN

Un “*blockchain*”, o cadena de bloques, es un sistema digital por el que se pueden realizar transacciones seguras sin necesidad de intermediario. El historial de datos y transacciones nunca podrá ser borrado ni modificado, por lo que esta tecnología presenta un registro inmutable y está disponible de forma permanente para todo el mundo.

Dentro de los participantes del sistema, se encuentran:

Los **bloques**, en donde cada uno representa una transacción que se enlaza y asegura usando criptografía. La **criptografía** es un proceso de encriptación de texto para generar un cifrado que es ilegible salvo para quien posea la clave de descifrado específica. Con esta ciencia se puede proteger la información y convertir la red más segura; donde el nivel de cifrado dependerá del grado de protección que requieran los datos.

Los **mineros**, que son los encargados de validar, confirmar y procesar todas las transacciones para posteriormente distribuirla a los nodos que forman la red.

Los **nodos**, se dedican a almacenar y distribuir una copia actualizada de la cadena de bloques, permitiendo que cada bloque nuevo que se confirma se añada a la red y a la copia que cada nodo almacena.

Características de la tecnología Blockchain

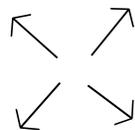
Verificación consensuada

Los participantes en la red comparten la misma documentación, que únicamente puede actualizarse con consenso.



Descentralizada

Una red distribuida optimiza la transparencia, quita intermediarios, reduce costos y optimiza tiempos.



Inalterable

La contabilidad y trazabilidad de los activos es única y dura por toda la vida del activo. A su vez, una vez cerrado un bloque no se puede modificar.



Segura

La verificación consensuada, la descentralización y la inmutabilidad forman un obstáculo para quienes quieran actuar de mala fe.



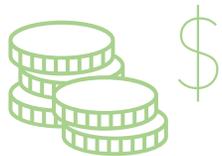
CÓMO FUNCIONA BLOCKCHAIN

Blockchain, a diferencia de otra base de datos que utilizan tablas como fuente principal, estructura la información en bloques vinculados. Cada bloque almacena un conjunto de datos que al rellenarse se vincula al bloque previo para formar una cadena. Cuando un bloque es rellenado no puede alterarse, y la información que se almacena en la red dependerá del propósito para el que fue creada.

Existen tres segmentos de adopción dependiendo en la disrupción de redes de transferencia:

Sistemas Financieros

Disrupción de la transferencia de valor desde sus formas más puras (ejemplo Bitcoin) hasta redes financieras más establecidas como los seguros, préstamos y financiación de consumo.



TRANSFERENCIA DE VALOR

Transacciones más rápidas y seguras que en finanzas tradicionales, menor coste, mayor accesibilidad y simplificación operativa.

Blockchain Corporativo

Impacto de la cadena de bloques en la transferencia de bienes y servicios, tanto físicos como digitales.

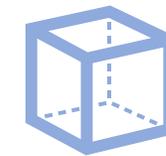


TRANSFERENCIA DE BIENES, SERVICIOS Y DATOS

Optimiza los procesos del negocio y el manejo de datos, mejora la seguridad y minimiza o elimina los intermediarios en la empresa.

Activos Tokenizados

Representan la frontera y el próximo paso en el desarrollo del blockchain.



TRANSFERENCIA DE ACTIVOS FÍSICOS

Aumenta la liquidez, transparencia y accesibilidad. Transacciones más rápidas y de menor costo que las tradicionales.

MÉTODOS DE CONSENSO

¿Quién decide qué se escribe en un *blockchain*? ¿quién valida las transacciones en una red *blockchain*?

Cada red de Blockchain elige cómo va a decidir cuáles son las transacciones, utilizando los **métodos de consenso**.

Estos son procesos que buscan lograr un acuerdo entre los distintos participantes de la red, sobre las transacciones que van a escribirse en la cadena.

Son los responsables de que todos los bloques de la cadena tengan los mismos datos, para evitar así la manipulación y asegurar la validez de las transacciones. Existen tres mecanismos de consenso:

Proof of Work (PoW): El método consiste en resolver ecuaciones matemáticas criptográficas complejas utilizando potencia informática para validar transacciones. Para empezar, se crea un bloque con cierta información:

- Dirección del bloque anterior
- Transacciones a incluir en el bloque
- Nonce: Es un número arbitrario que solo puede ser utilizado por única vez en una comunicación criptográfica, y es utilizado como protocolo de autenticación. En este campo se introduce un valor aleatorio de forma que con cada valor distinto, el bloque cambia pese a tener las mismas transacciones.

La red permite la creación del próximo bloque al minero que logra encontrar el “*hash*” correcto, por ende, la competencia es alta. El “*hash*” es una función que cumple con las demandas cifradas necesarias para resolver un cálculo de blockchain que sirven para verificar la integridad de los mensajes y autenticar la información. Cualquier computadora usando la red puede validar que el “*hash*” es correcto en una fracción del tiempo que toma “minarlo” (construirlo), así asegurando la validez y recibiendo criptomonedas como recompensa. Este es el método utilizado por Bitcoin y Ethereum.

Proof of Stake (PoS): En este método los mineros disponen parte de su patrimonio como colateral, y mientras más dispongan más chances de ser elegidos para validar la transacción. En este mecanismo hay dos tipos de bloques:

- Regulares: almacenan una copia de la cadena y son a los que se pueden hacer consultas
- Validadores

Los mineros son elegidos al azar para validar los bloques, por ende, quita la competencia que existe en PoW. La recompensa pasa a ser una garantía de la buena fe del validador y se valora según lo ofrecido. Este método lo utilizan **Cardano**, **Solana** y **Tezos**.

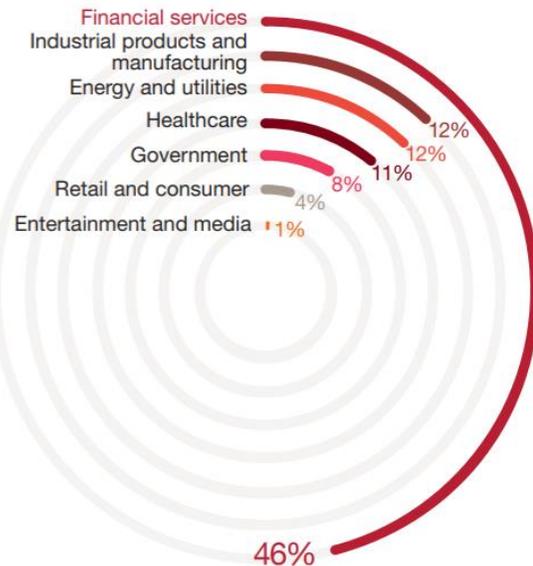
Proof of history (PoH): Este método requiere una cantidad específica de pasos secuenciales para evaluar, pero produce un resultado único que puede verificarse de manera eficiente y pública. Crea un registro histórico con marcas de tiempo exactas de todo lo que sucede en la cadena, desde su origen hasta el momento actual. Tras registrar una transacción, la salida de la operación se convierte en la entrada de la siguiente operación. PoH no es un método de consenso en sí, sino que se combina el método PoS para mejorar el tiempo de confirmación del orden de las transacciones. El método pretende acelerar el proceso de consenso al proporcionar un medio para codificar el tiempo en sí mismo en la cadena de bloques.

TIPOS DE BLOCKCHAIN

PÚBLICO: Es descentralizado y no tiene una entidad sola que controle la red. Cualquiera puede unirse a la red y participar dentro del blockchain.

PRIVADO: Funcionan basados en controles de acceso que restringen a las personas que pueden participar en la red, y solo quienes participen tendrán conocimiento de las transacciones que se realicen.

Industrias que podrían considerarse futuros líderes en Blockchain



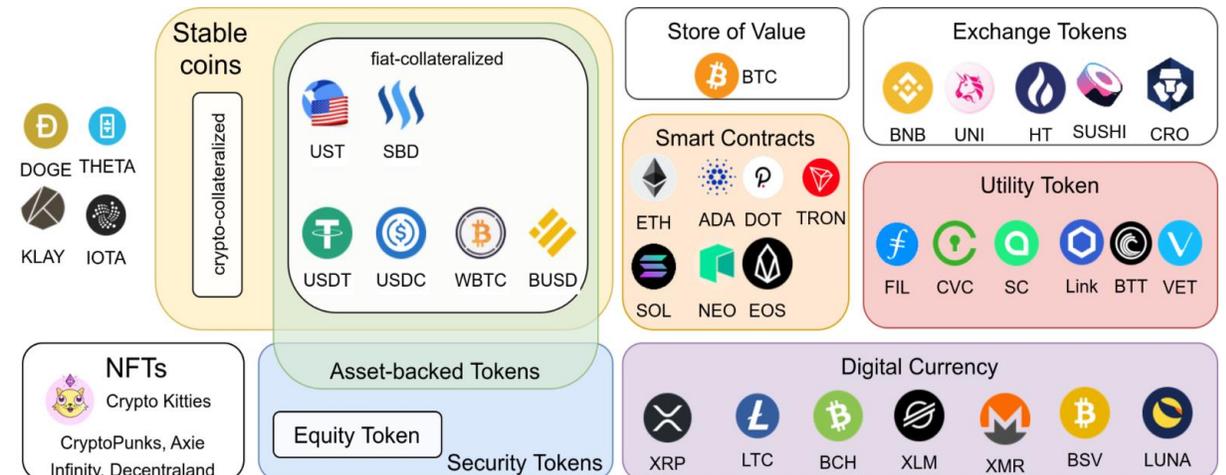
Note: Base: 600.

Q: Which of the following industries are the most advanced in developing blockchain today?

Source: PwC Global Blockchain survey, 2018

PRINCIPALES ACTIVOS FINANCIEROS EN BLOCKCHAIN

- **ACTIVOS DIGITALES:** Recursos no tangibles que se crean, comercializan y almacenan digitalmente.
- **CRIPTOACTIVOS:** Medios digitales que utilizan la criptografía para asegurar las transacciones financieras, entre ellos:
 - Criptomonedas
 - Token digitales
 - Stablecoins



PRINCIPALES CRIPTOACTIVOS EN EL ECOSISTEMA BLOCKCHAIN

- CRIPATOMONEDAS:** Son monedas virtuales que utilizan un cifrado digital para sus operaciones y son el activo nativo de un Blockchain. Con ellas se pueden realizar transacciones económicas sin necesidad de pasar por una institución financiera como intermediara para verificar su autenticidad. Son monedas que no están reguladas ni controladas por ninguna institución, y ese es el principal desafío que presentan.

Necesidad de la existencia de las criptomonedas en una red blockchain

Las criptomonedas fueron creadas como **medio de pago** para los participantes de cada blockchain pública. Su trabajo dentro de cada red de blockchain es remunerado con una criptomoneda específica dependiendo de los intereses de la cadena.

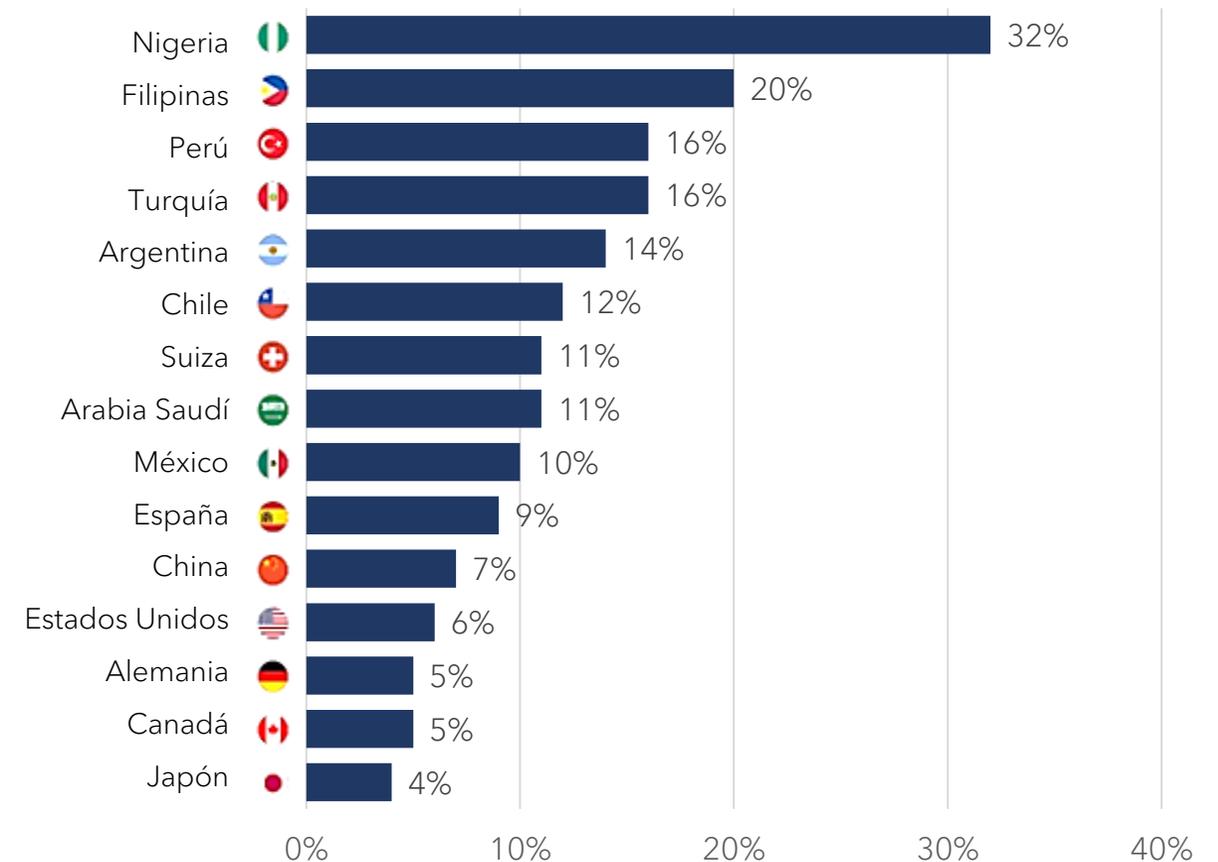
Por ende, las criptomonedas van a existir siempre que exista la tecnología blockchain.

Un Blockchain público no puede existir sin criptomonedas

En un futuro, las criptomonedas podrían aumentar el acceso a los servicios financieros a la población no bancarizada.

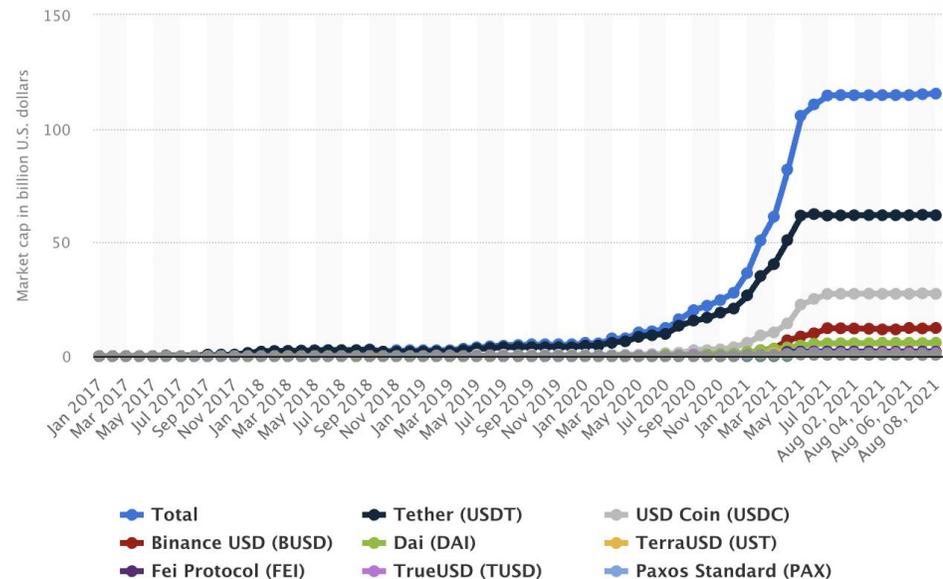
Alrededor del 30% de la población mundial tiene sociedades sub-bancarizadas, por lo que la dinámica de las criptomonedas podría ayudar a cubrir una mayor parte de la población.

¿Qué tan comunes son las criptomonedas en el mundo?

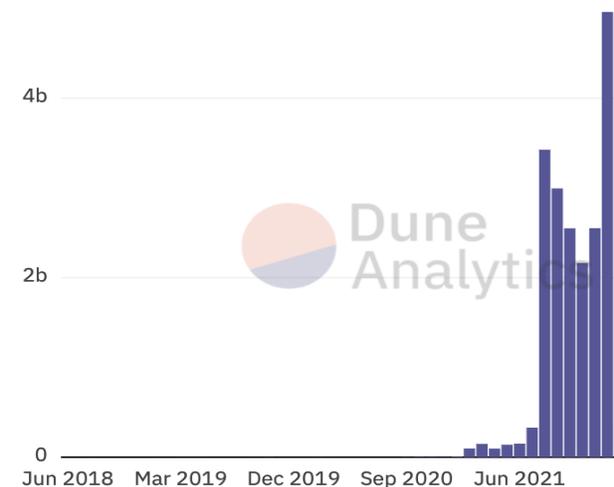


PRINCIPALES CRIPTOACTIVOS EN EL ECOSISTEMA BLOCKCHAIN

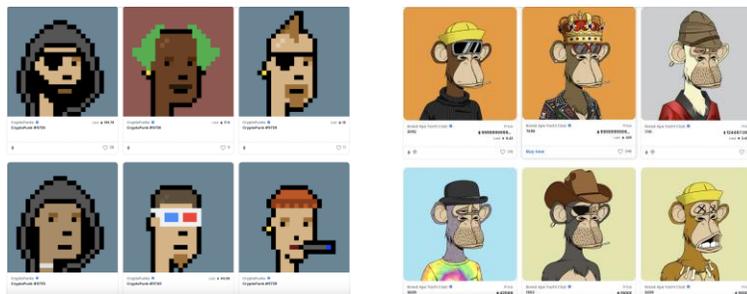
- TOKENS:** Un token es un activo digital que se crea como parte de una plataforma que se construye sobre un blockchain. Son unidades de valor que las organizaciones o proyectos basados en un blockchain desarrollan. La diferencia con las criptomonedas es que los tokens no tienen su propio blockchain y las criptomonedas sí. A su vez, un token puede ser creado para representar cualquier "cosa" del mundo real, una casa, acción de una empresa, un coleccionable.
- NFTs:** Conocidos como tokens no fungibles, son activos digitales que se almacenan en un blockchain. No fungible en este caso significa que es un activo único y que no puede ser reemplazado por otra cosa. Por ejemplo: un dólar es fungible: existen muchos billetes de un dólar y todos representan lo mismo. Mientras que un NFT es como una tarjeta coleccionable, y es única en su tipo. El uso más común hoy es vinculado al arte, pero tienen muchas aplicaciones posibles (derechos intelectuales, derechos comerciales, títulos, etc.).



OpenSea es el principal mercado de NFT y opera en múltiples blockchains
Volumen mensual de OpenSea



Ejemplos de proyectos en NFT
(valorizados en millones de USD por obra)



PRINCIPALES CRIPTOACTIVOS EN EL ECOSISTEMA BLOCKCHAIN

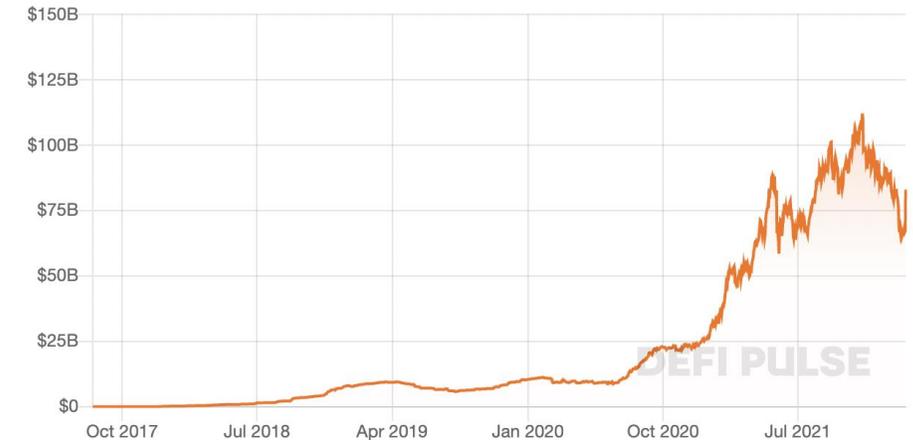
- **DeFi:** es la parte del ecosistema de criptoactivos relacionando a las finanzas descentralizadas. La descentralización es cuando un sistema no tiene una figura central de autoridad. Incluye muchísimos productos y servicios, y es una creciente alternativa a las finanzas tradicionales (TradFi).

Entre ellos hay productos/servicios de pagos, infraestructura, KYC, seguros, exchanges y servicios de custodia.

- **STABLECOINS:** Es un token que está asociado a un activo estable, como por ejemplo al dólar o al oro. Pueden ser centralizadas (emitidas por una entidad que tiene controles sobre ellas) o descentralizadas (manejadas por algoritmos independientes).

Las "stablecoins" pueden ser usadas como método de cambio como cualquier moneda. Además, son utilizadas dentro del ecosistema en momentos de volatilidad como activo de refugio.

Valor total anclado a DeFi
(sobre todos los blockchain existentes)



Estados Unidos y Suiza son los países que más stablecoins tienen



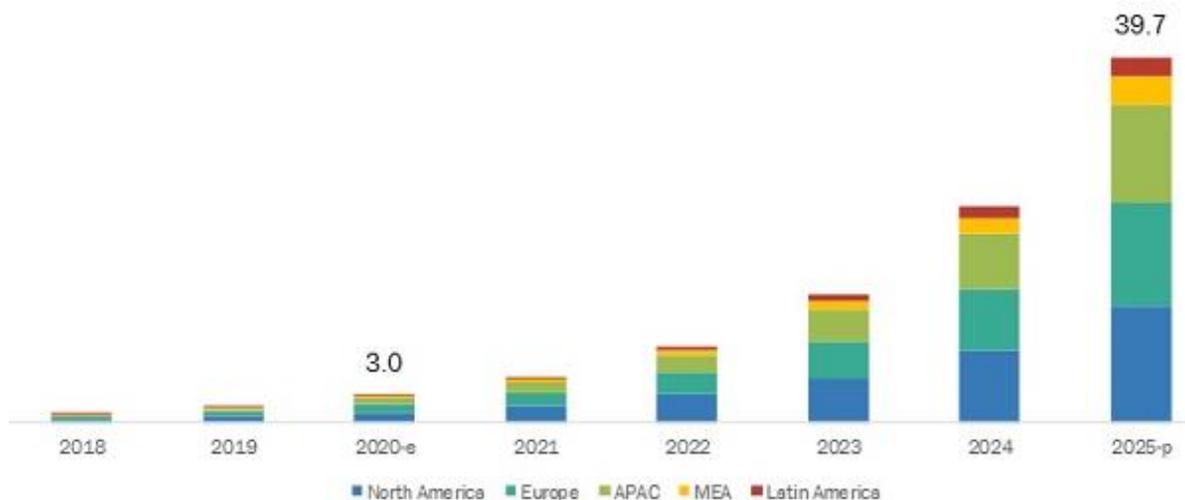
POR QUÉ INVERTIR EN BLOCKCHAIN

- El Blockchain proporcionará una oportunidad de inversión a largo plazo a medida que aumentan sus aplicaciones prácticas y su penetración a lo largo del tiempo.
- El Foro Económico Mundial estima que aproximadamente el 10% del PIB mundial se almacenará en la tecnología Blockchain en 2027.
- Se estima que el valor añadido empresarial de Blockchain será de 176 mil millones de dólares para 2025.

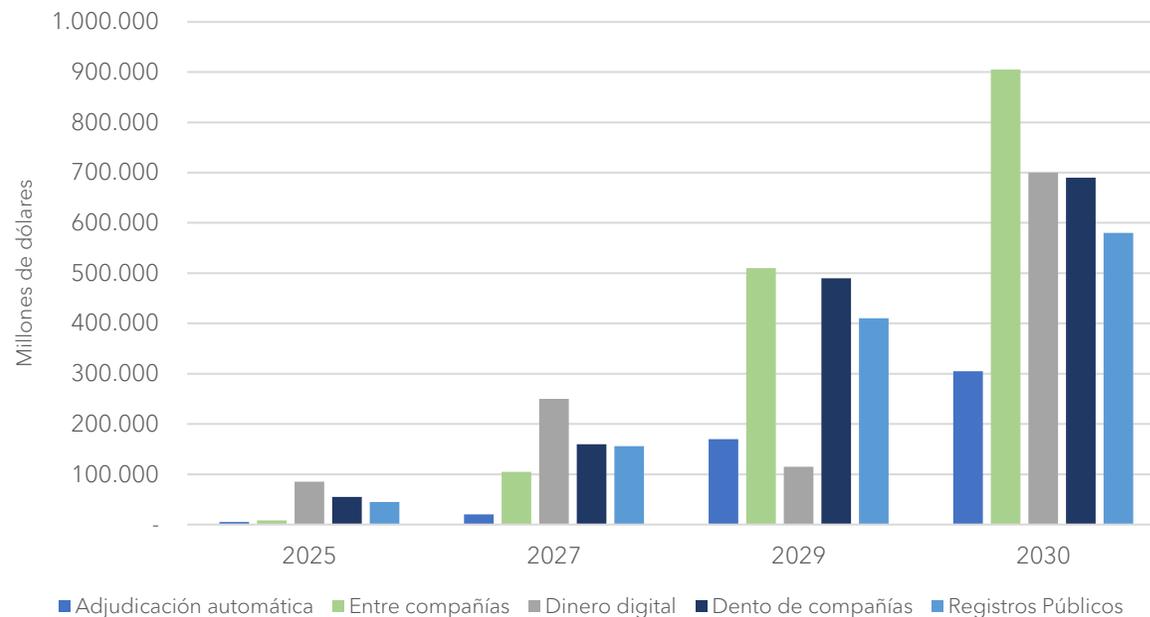
Blockchain aportará 3,1 billones de dólares en valor para 2030

Mercado de Blockchain por región

Mil millones de USD



Valor de mercado de Blockchain



Fuente: Blockchain Business Value, Worldwide, 2017-2030

Fuente: <https://www.iieschool.com/blog/blockchain-cadena-bloques-revoluciona-sector-financiero-finanzas/>

CÓMO ELEGIR DONDE INVERTIR

A grandes rasgos existen distintos proyectos o ecosistemas que brindan la base para el desarrollo de otras aplicaciones.

Cada uno de los proyectos (ETH, SOLANA, etc) funciona como una 'Apple Store' o 'Android Store' en donde cada aplicación se desarrolla, entonces se elige cada uno de los ecosistemas según el atractivo y cantidad de aplicaciones que ofrezca.

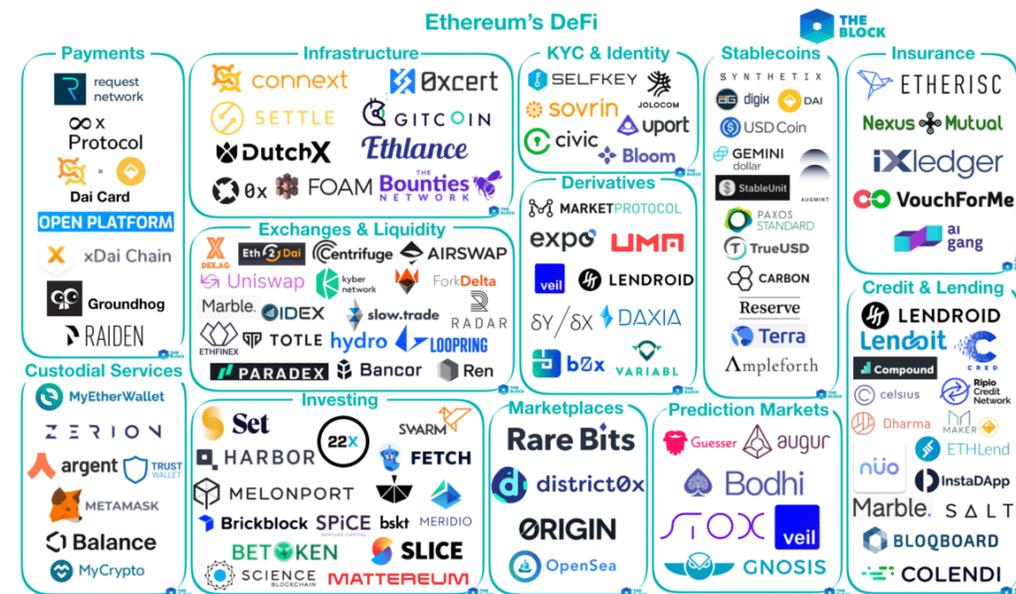
La existencia de una criptomoneda es intrínseca a cada uno de los proyectos dado que es el método de retribución del minero que trabaja para la red. Un ejemplo es el yuan digital el cual se desarrolla sobre el ecosistema de Ethereum, pero es necesario que exista ETH como moneda para pagarle a los mineros.

Esto hace que sea relevante conocer la cantidad de proyectos que se esta desarrollando sobre cada plataforma para conocer el valor de cada una.

Ecosistema Ethereum:

ALTERNATIVAS DE INVERSIÓN

- Se puede invertir en las distintas aplicaciones que se desarrollan sobre el ecosistema. Como por ejemplo, comprar yuan digital si entiendo que va a subir de valor.
- Hoy en día ya existen distintos instrumentos que permiten invertir en varios proyectos de manera simultánea y diversificar el riesgo dentro de esta categoría que forma parte de los activos alternativos del portafolio.



Por ideas de inversión contacte a su Asesor Financiero



info@latinadvisorsuruguay.com

Disclaimer

La información disponible en esta presentación es únicamente con fines informativos. La información, recomendaciones, análisis, conclusiones e ideas de Latin Securities SA Agente de Valores son meramente opiniones de la misma, y en consecuencia, de forma alguna deben interpretarse como asesoramiento de inversión, sugerencias de venta, compra, Inversiones u operaciones de naturaleza alguna. El uso de la información, recomendaciones, análisis e ideas proporcionadas por Latin Securities SA Agente de Valores son de exclusiva responsabilidad de quienes decidan utilizarlas, y por lo tanto Latin Securities SA Agente de Valores no será responsable de forma alguna por los resultados ni Rendimiento económico y/o financiero y/o en especie y/o monto alguno sobre inversiones u operaciones se efectúen utilizando la información, recomendaciones, análisis, conclusiones e ideas suministradas por la Latin Securities SA Agente de Valores. Las valuaciones de los productos pueden tanto subir o bajar como consecuencia de las evoluciones de los mercados. No garantizamos que la información contenida en esta presentación sea precisa, completa u oportuna ya que las mismas solo son precisas a la fecha de su publicación, así como los precios de los productos son meramente indicativos, y no se debe depender de los mismos al asesorar a sus clientes. El desempeño pasado no es un indicador confiable ni una garantía de resultados futuros. Las diferencias en el tamaño de la cuenta, el momento de las transacciones y las condiciones del mercado que prevalecen en el momento de la inversión pueden generar resultados diferentes entre las cuentas. Diferencias en la metodología utilizada para calcular el rendimiento también puede dar lugar a resultados de rendimiento diferentes a los mostrados. El rendimiento compuesto se compara con el de un índice no gestionado, que no genera comisiones de gestión, costes de transacción u otros gastos asociados con una cuenta administrada.



WWW.LATINADVISORS.COM.UY