Trabajo Final Maestría en Finanzas

Cómo y por qué las Criptomonedas y Blockchain pueden ser una competencia muy fuerte para el sistema financiero tradicional

UNIVERSIDAD DEL CEMA

Tutor: José Pablo Dapena

Alumno: Juan Martín Vergara

Septiembre 2021

Introducción

Las criptomonedas y su tecnología subyacente denominada Blockchain se han convertido en una de las innovaciones financieras más disruptiva del último tiempo debido a que definen un nuevo paradigma en las relaciones de los agentes económicos; la descentralización de la confianza para garantizar la integridad y seguridad de las transacciones financieras de manera electrónica, reemplazando las entidades de control o autoridades centralizadas por la veracidad de pruebas basadas en algoritmos criptográficos de tal manera que la irreversibilidad y veracidad de las operaciones sean garantizadas.

En segundo lugar, las criptomonedas transparentan el registro y la trazabilidad de las transacciones en la Blockchain porque pueden ser copiadas y validadas por cualquier nodo de la red P2P. En esta situación, ninguna transacción es desconocida porque todas las actualizaciones son replicadas a todos los participantes de la red. También es importante destacar que proveen de anonimato y satisfacen las comodidades al usuario común que desea tener discreción con sus ahorros, así como en el movimiento y transferencia de fondos. Por último, las criptomonedas promueven el desarrollo de mercados libres de intermediación basados en la descentralización y la reducción de costos de acceso a productos y servicios. En otras palabras, las criptomonedas están soportadas por plataformas P2P que permiten a los usuarios compartir directamente bienes, servicios e información a un menor costo y con mayor rapidez que los sistemas tradicionales.

De esta manera, tanto las criptomonedas en sí como su tecnología, son capaces de causar profundos cambios en la sociedad y el sistema financiero que conocemos al proporcionar las bases para crear nuevas oportunidades y desarrollar innovadores modelos de negocios. Lógicamente, esto ayuda a disminuir las barreras de entrada al mundo financiero para muchos usuarios y proveedores de aplicaciones, especialmente para aquellos que residen en países con instituciones o marcos legales poco confiables, con altos niveles de inflación y devaluación.

Desde esta perspectiva, el objetivo central de este trabajo es realizar un análisis general de las criptomonedas y la tecnología Blockchain para así luego entender si estas pueden ser una competencia sólida para el sistema financiero tradicional. Para esto voy a realizar una introducción teórica explicando el funcionamiento de estas tecnologías y de las distintas aplicaciones financieras construidas sobre la Blockchain para ver cómo y por qué estas son una competencia para el sistema financiero tradicional. Además, vamos a observar el crecimiento del ecosistema apalancándonos en el Global Crypto Adoption Index elaborado por Chainalysis.

Capitalización de Mercado

En la actualidad existen casi 6000 criptomonedas activas con una capitalización total de mercado de USD 2.222.510.831.544, dato al 2 de Septiembre de 2021 (CoinMarketCap). Se destaca Bitcoin (BTC) con una dominancia de mercado del 41,9% y le sigue Ether (ETH), el token de la Ethereum Network con el 19.98%.

Bitcoin fue la primera en aparecer, proporcionando el camino y el estándar para que luego aparezcan otras que son conocidas como altcoins. Lógicamente, el nombre viene de la frase "monedas alternativas" y sus funciones, diseños, sistemas de emisión y características van variando dependiendo cual es el objetivo que busca su creador o creadores.

Figura 1: Capitalización total del mercado de criptomonedas al 02/09/2021. Fuente: Coinmarketcap.com

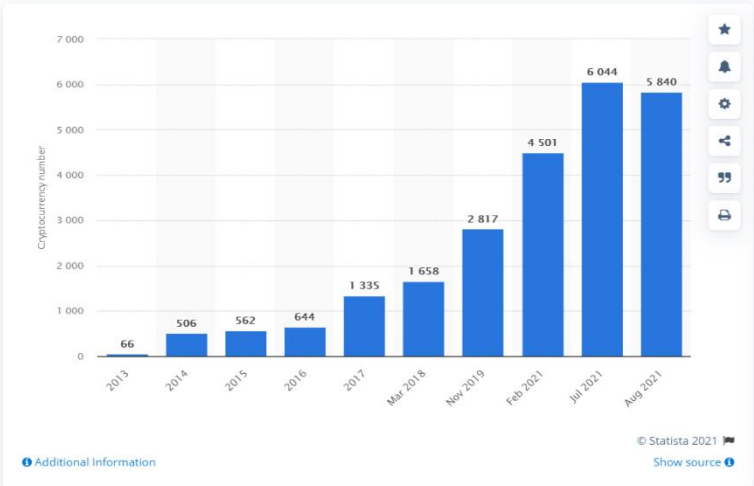


Figura 2: Evolución de la cantidad de criptomonedas disponibles al 02/09/2021. Fuente: Statista

Como se ve tanto en la Figura 1 (Capitalización total del mercado de criptomonedas) como en la Figura 2 (Evolución de la cantidad de criptomonedas disponibles), el ecosistema ha crecido a pasos agigantados en los últimos años pero en especial en el último año y medio. Como mencione anteriormente, a lo largo de este trabajo vamos a entender por qué esto ha sucedido y por qué este crecimiento hace que cada vez sea más realista la idea de que esto llegó para quedarse y que puede ser una gran competencia para el sistema financiero tradicional.

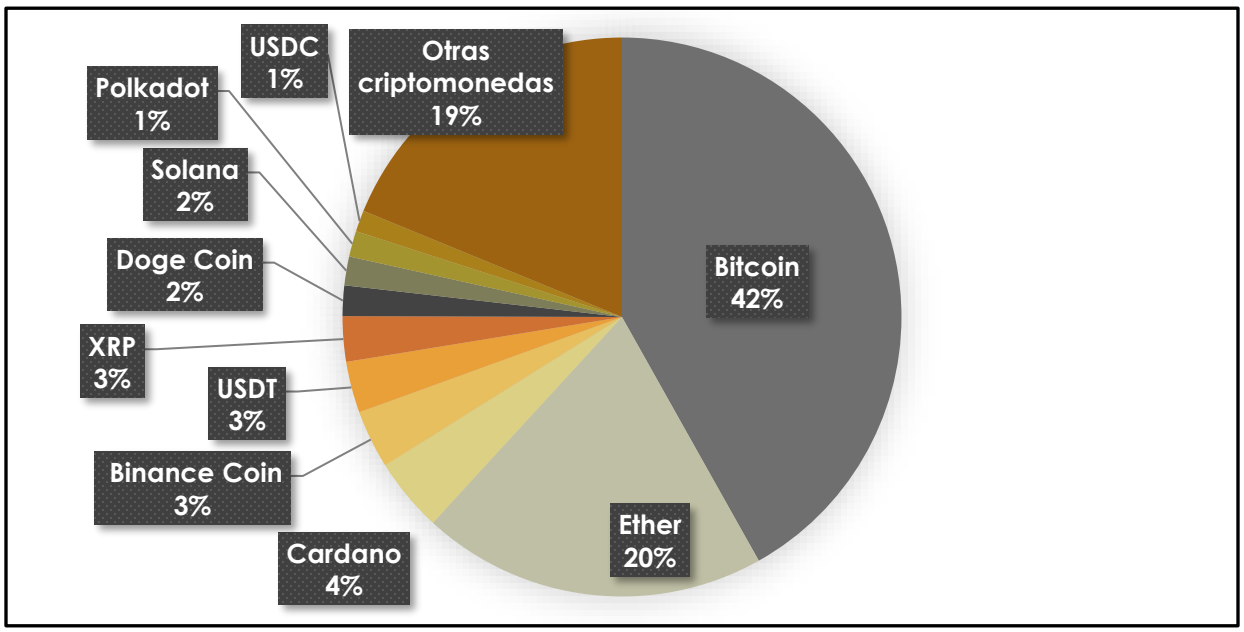


Figura 3: Participación en la capitalización de mercado total al 02/09/2021. Fuente: elaboración propia con datos de Coinmarketcap.com

Conceptos claves y fundamentos técnicos

Para lograr entender cómo es que las criptomonedas y su tecnología Blockchain son una muy fuerte competencia para el sistema financiero tradicional primero es necesario entender los fundamentos teóricos y técnicos de ellas. En esta línea, se realizará un resumen representativo de las principales definiciones y técnicas que las sustentan, incluyendo los mecanismos principales de consenso, emisión y distribución. A su vez, también se mostraran las distintas aplicaciones financieras desarrolladas en este innovador ecosistema, principalmente dentro de lo que es el mundo de los Smart Contracts y DeFi (Decentralized Finance).

Blockchain

Para entender qué es Blockchain y por qué esta es una herramienta muy útil aplicable a la creación de un nuevo sistema financiero descentralizado, se debe remontar al concepto básico de base de datos. En esencia, las bases de datos son tablas que constan de registros de información y campos de datos. Si nos remitimos a los orígenes, la interacción entre un usuario y estos sistemas era muy limitada, como podía ser un simple llamado telefónico a nuestro banco para consultar nuestros saldos en las cuentas bancarias o saber cuánto tenemos de deuda en una tarjeta de crédito.

Si agregamos un poco más de complejidad, estas bases de datos pueden relacionarse entre sí, compartirse entre miles de usuarios y también ser modificadas. Hoy en día las bases de datos cumplen un rol fundamental en el funcionamiento y desarrollo de casi cualquier actividad e industria. Estas se comparten con los usuarios casi en tiempo real a través de una conexión a Internet. Un ejemplo claro es justamente en el sistema financiero. Los bancos tienen bases de datos que indican la información de los clientes. Esto puede ir desde algo básico como los números de cuenta de cada uno de ellos hasta algo más complejo como el registro de todas las operaciones realizadas con sus respectivos detalles (consultas, transferencias, prestamos, etc.).

En el año 2008, Satoshi Nakamoto (al día de hoy no se conoce quien o quienes son, es un seudónimo) publicó un White Paper en el que aseguraba que había encontrado la manera de crear una red descentralizada en la que podría lograrse el consenso sin el control de una autoridad central. Esto es la Blockchain. Además, esta red proporciona un sistema de intercambio de valor ya que tiene una moneda/activo con una características hasta ahora nunca vista; la escasez digital. Esto es Bitcoin.

La tecnología Blockchain aporta seguridad, integridad y autenticidad a la información contenida en bases de datos distribuidas. Por medio de la criptografía, esta tecnología permite crear bases de datos descentralizadas con protocolos altamente seguros que garantizan la inmutabilidad de la información, y a través de procesos de autenticación, conservan la privacidad en el acceso y disposición de la información según el usuario lo requiera.

Si entramos en un poco más de tecnicismo, la información es segmentada en bloques, los cuales se agregan y validan de forma táctica a partir del consenso generalizado de la mayoría de los nodos que participan de esta red, conformando así una cadena de bloques (de ahí deriva el nombre Blockchain).

El mecanismo de validación funciona utilizando esquemas de incentivos diseñados para compensar la propagación de transacciones legítimas. Toda esta dinámica permite que dos partes, sin la necesidad de conocerse, puedan intercambiar valores y/o información sin una autoridad central o intermediario que otorgue confianza y validez a la operación. La confianza no recae en una contraparte sino en el protocolo que utiliza la Blockchain para funcionar. De esta manera, la Blockchain provee varias de las ventajas de los sistemas centralizados pero sin las implicancias de la participación de intermediarios que usualmente tienen poder de influencia sobre el mercado, capacidad de incumplir sus compromisos y el control de la información de los participantes.

Red P2P

Una red P2P está conformada por nodos geográficamente distribuidos e interconectados entre sí para compartir recursos y servicios. Es decir, una red que carece de una entidad central para monitorear el comportamiento de cada nodo. La detección y prevención de comportamientos no deseados es determinada por la colaboración de los nodos. Cada nodo es autónomo y decide su nivel de contribución a la red. A su vez, otro conjunto de nodos puede encargarse de la validación de transacciones antes de su propagación en la red. En este sentido, la red P2P difunde las transacciones y actualizaciones de la Blockchain. De hecho, el principal reto es lograr que toda la información de los nodos sea replicada y coincida entre sí.

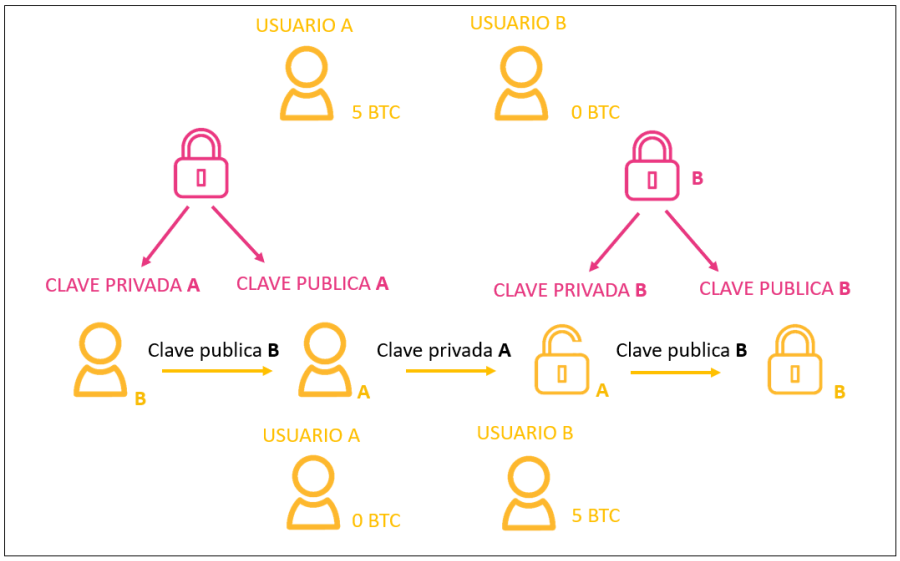
Transacciones y Mecanismos de emisión de moneda

La realización de transacciones está soportada por el uso de claves basadas en métodos criptográficos. Estas claves pueden ser públicas y privadas. Una clave pública es conocida y sirve como dirección de envío/recepción de tokens, algo que se asemeja a lo que sería una clave bancaria uniforme en el sistema bancario tradicional (CBU). Por otro lado, la clave privada es de uso restringido y sirve para demostrar la propiedad y transferencia de fondos. Esta es almacenada en una wallet digital, la cual puede ser instalada en cualquier dispositivo electrónico como un celular, computadora o incluso dispositivos diseñados exclusivamente para este fin como lo son las cold wallets Ledger o Trezor.

Los sistemas de criptomonedas no están respaldados por la confianza y seguridad de una entidad bancaria, en su lugar, se confía en los mecanismos de consenso descentralizados basados en la Blockchain. La emisión de tokens es el resultado de la validación transaccional realizada por esos mecanismos de consenso ejecutados por nodos validadores, conocidos como mineros.

La minería valida y organiza los bloques dentro de la Blockchain. Para lograr esta organización, se necesita del esfuerzo computacional de los mineros que compiten en un sistema descentralizado. Esta competencia consiste en que cada minero construye un bloque candidato y realiza cálculos computacionales para ser el primero en resolver un algoritmo. El minero ganador añade un nuevo bloque a la Blockchain para que las transacciones sean replicadas y actualizadas en cada uno de los nodos. Como resultado de esta competencia se recompensa por su esfuerzo con criptomonedas al nodo minero que logró resolver el problema matemático. Esas criptomonedas provienen de dos fuentes: nuevas monedas creadas y comisiones de todas las transacciones añadidas a un bloque.

La minería puede ser realizada mediante dos mecanismos; Proof of Work y Proof of Stake. En el primer caso se utiliza poder computacional (hardware) y mucha electricidad para resolver el problema matemático mencionado anteriormente. Por el lado del Proof of Stake, este intenta demostrar que la seguridad de un sistema cripto no debe depender de los recursos energéticos y computacionales. Para eso utiliza un algoritmo de consenso diferente donde en lugar de utilizar electricidad para hacer funcionar estas computadoras, utiliza la propiedad de la criptomoneda en sí; lo que se hace es hacer staking con las criptos. El concepto de Stacking se refiera a bloquear tus criptomonedas para respaldar la seguridad y operabilidad de una Blockchain a cambio de recibir una recompensa en la misma criptomoneda. La creencia radica en que un nodo protegerá la integridad de la Blockchain de futuros ataques al poseer una buena cantidad de tokens por lo que no tendría sentido alguno actuar de manera fraudulenta ya que se perjudicará a sí mismo.



En la figura 4, se explica el proceso de realizar una transacción. Fuente: elaboración propia.

En el ejemplo de la Figura 4, el usuario A tiene 5 BTC en su wallet y se los quiere enviar al usuario B. Lo que sucede es que el usuario A crea la transacción especificando la cantidad y la dirección a donde se van a enviar (clave publica del usuario B), la transacción es firmada con la clave privada del usuario A desde un origen (wallet usuario A) a un destino (wallet usuario B). De esta manera el usuario A difunde la transacción a todos los nodos de la red P2P, es decir a los mineros. Estos compiten por resolver el problema matemático complejo acorde a la especificación de la transacción y una vez que este se resuelve, la transacción es confirmada. De esta manera el usuario B recibe los 5 BTC en su wallet pero también esta transacción es difundida a toda la Blockchain y el minero que logro procesarla obtiene la recompensa en criptomonedas, en este caso en BTC.

Bitcoin

Como vimos al principio del trabajo, Bitcoin es la criptomoneda más popular y de mayor capitalización en el mercado. Fue la primera en ser creada y es básicamente una red descentralizada de pago P2P compuesta por nodos. Provee los conceptos básicos para el surgimiento de otras que utilizan similares principios criptográficos como es el caso de Ether que ya lo veremos más adelante.

Dentro del ecosistema Bitcoin se define a una transacción como una estructura de datos que codifica la transferencia de valor entre los participantes en un sistema de pago. Esta estructura está formada por salidas y entradas, las cuales registran el flujo transaccional entre los participantes. De esta manera, la integridad del flujo transaccional es garantizada a través de la implementación de scripts, tanto en las salidas como las entradas. El script vinculado a una salida se llama script de bloqueo y especifica las condiciones que se deben cumplir para que una salida (fondos) pueda ser gastada. Un script de bloqueo es llamado "scriptPubKey" porque usualmente contiene una clave pública (dirección del destinatario). El script vinculado a una entrada se llama script de desbloqueo y resuelve o satisface las condiciones de un script de bloqueo, permitiendo que una salida sea gastada. Un script de desbloqueo es llamado "scriptSign", porque usualmente contiene una firma digital. Si el script de desbloqueo satisface las condiciones del script de bloqueo, el resultado de su ejecución será verdadera y la firma es una autorización válida.

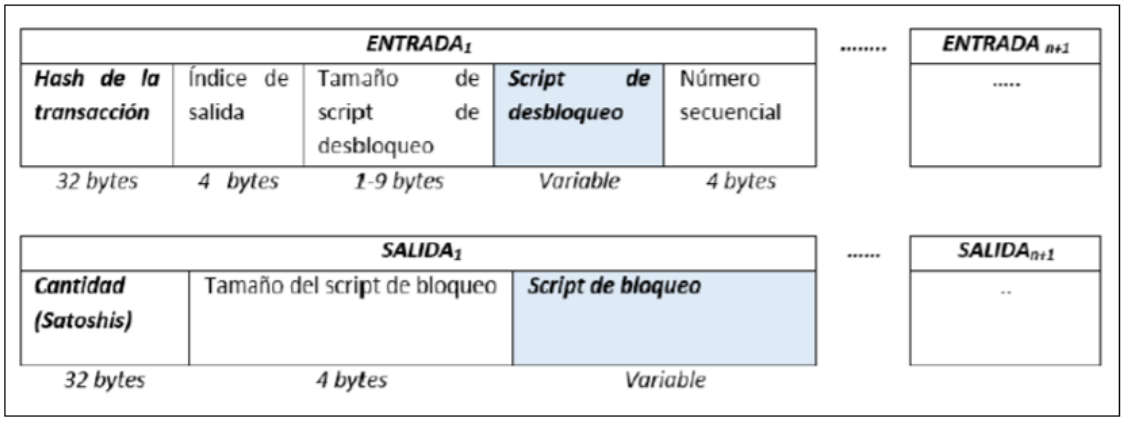


Figura 5: Estructura de una transacción. Fuente: Mastering Bitcoin, Andreas Antonopoulos, 2015.

Estructura de la Blockchain de Bitcoin

Blockchain en Bitcoin es una estructura compuesta por una lista de bloques que incluyen transacciones. Cada bloque es identificado con un hash, generado por el algoritmo criptográfico (SHA-256). El bloque generado en el inicio de la Blockchain se llama génesis. Cada bloque creado sirve como base para la generación del siguiente bloque ya que cada bloque posterior es vinculado secuencialmente con un bloque anterior. A partir de este esquema es que se denomina altura al número de bloques añadidos después del bloque génesis.

Transacción On-Chain

Como ya vimos**,** una transacción es una transferencia de valor de un token en particular, cuyos detalles son grabados en bloques adecuados en la Blockchain, y los mismos son transmitidos a toda la red de la criptomoneda después de una verificación adecuada.

Las transacciones dentro de la cadena (on-chain) son aquellas transacciones que ocurren dentro del Blockchain y permanecen dependientes del estado ella para su validez. Todas estas transacciones dentro de la cadena se producen y se consideran válidas solo cuando la Blockchain se modifica para reflejar estas transacciones en los registros del libro público. Dependiendo del protocolo de red, una vez que una transacción obtiene suficientes confirmaciones de los participantes de la red, esta se vuelve irreversible. Solo se puede revertir si la mayoría de los participantes de la Blockchain llega a un consenso para revertir la transacción.

Transacción Off-Chain

Las transacciones fuera de la cadena (off-chain) son aquellas que ocurren en la red de una criptomoneda que mueve el valor fuera de la Blockchain. Debido a su costo muy bajo, las transacciones off-chain están ganando popularidad, especialmente entre los grandes participantes.

Este tipo de transacciones pueden ser ejecutadas usando múltiples métodos. En primer lugar, puede producirse un acuerdo de transferencia entre las partes que realizan la transacción. En segundo lugar, las transacciones off-chain pueden involucrar a un tercero, como un garante, que se encargue del cumplimiento de la transacción (procesadores de pagos actuales como PayPal funcionan de esta forma). Otro método para realizar este tipo de transacciones es utilizar un mecanismo de pago basado en cupones. Un participante compra cupones a cambio de tokens y entrega el código a otra persona para que esta los canjee. El reembolso es posible en la misma criptomoneda o en diferentes criptomonedas, dependiendo del proveedor de servicios del cupón. De la manera más sencilla, dos partes pueden incluso intercambiar sus claves privadas involucrando una cantidad fija de criptomonedas y así los tokens nunca salen de la wallet.

Ethereum Network y Ether

Una vez que la gente se empezó a dar cuenta del poder de Bitcoin y Blockchain, se empezó a intentar llevar esas características a otros ámbitos. ¿Qué otros aspectos de nuestra vida cotidiana pueden ser descentralizados también? Ethereum es creado para responder esa pregunta.

Ahora, para que un sistema sea verdaderamente descentralizado, se necesita una gran cantidad de computadoras que corran ese sistema. Antes del surgimiento de Ethereum, la única red de este estilo era la de Bitcoin que por cierto es bastante limitada ya que está escrita bajo lo que se conoce como un lenguaje Turing incomplete. Esto significa que solamente puede entender y procesar una cantidad de ordenes pequeñas como por ejemplo quien le manda dinero a quien. Si queres un sistema más complejo que te permita más operaciones y de mayor complejidad necesitas un lenguaje de programación diferente, lo que a su vez implica una red de computadoras distinta. Con esta idea aparece Ethereum Network.

Ethereum Network fue introducida por Vitalik Buterin a fines del 2013. En primera instancia él propuso un cambio en la red de Bitcoin para poder expandir las posibilidades de los programadores para que estos puedan incluir otros casos de uso dentro de la red y no solo la transferencia de dinero. Esta propuesta no fue aceptada por la comunidad de Bitcoin por lo que en 2013 publicó un

White Paper donde proponía una Blockchain de propósito general, es decir, una Blockchain que tiene un lenguaje de programación que es Turing completo, que permite hacer muchas más operaciones. De este modo, esta red se iba a poder adaptar a nuevos y distintos casos de uso en comparación a Bitcoin. Como vamos a ver a continuación, lo innovador de esta red es la posibilidad de crear Smart Contracts, los cuales son el pilar para que las criptomonedas sean una competencia muy fuerte para el sistema financiero tradicional.

En resumen, Ethereum es una plataforma de código abierto, basada obviamente en la tecnología Blockchain, que permite crear aplicaciones descentralizadas. En Bitcoin, el intercambio de valor se hace a través de Bitcoin y en la red de Ethereum se hace a través de Ether. La diferencia es que en Ethereum, además de intercambiar valor, es posible ejecutar programas informáticos. Cualquier programador del mundo puede escribir código y ejecutarlo en este plataforma para crear una app descentralizada. Entonces Ethereum es una red que proporciona infraestructura para ejecutar las Dapps (decentralized applications) y los Smart Contracts de una manera descentralizada.

Smart Contracts

La expresión “Code is Law” se utiliza para decir que la tecnología es la que pone las reglas, es decir, que el código te dice lo que podes y lo que no podes hacer de una manera automatizada. Con el reciente desarrollo de lo que son los Smart Contracts, este escenario futurista puede llegar a estar más cercano de lo que muchos creen.

El lenguaje de programación de Ethereum (Solidity) es utilizado para programar estos contratos inteligentes, los cuales son el motor a través del cual funcionan las aplicaciones descentralizadas. En la vida tradicional, un contrato es un conjunto de “IF” & “THEN”, es decir, un conjunto de condiciones que una vez cumplidas generan una determinada acción. Por ejemplo, a grandes rasgos, un contrato de alquiler dice que si el inquilino paga una determinada suma de dinero los primeros días del mes, el propietario lo deja utilizar su departamento o casa por un periodo de tiempo. Así de simple también es como funciona un Smart Contract. Los desarrolladores de estos contratos inteligentes escriben las condiciones para sus programas o Dapps y luego la red de Ethereum los ejecuta.

Entonces un Smart Contract es un código que puede ser ejecutado de una manera automática y determinística. Este código es almacenado y ejecutado en la Blockchain para que sea descentralizado y seguro. También tienen la posibilidad de recibir, guardar, enviar fondos y utilizar

otros Smart Contracts en simultaneo, todo esto utilizando la premisa “IF – THEN”. El objetivo es eliminar el factor humano a la hora de la toma de decisiones. ¿Por qué se busca eliminarlo? Porque está probado que este factor es el mayor causante de errores y de desconfianza a la hora de ejecutar los contratos tradicionales.

La adhesión de un contrato sobre Blockchain permite abordar los aspectos críticos de una transacción tales como registro, mantenimiento y auditoría de las transacciones de una manera muy eficiente y confiable porque la liquidación de la transacción es instantánea e independiente de la injerencia de las partes involucradas.

Otro aspecto a destacar es que los costos adicionales y tasas de servicios financieros son eliminados debido a la naturaleza intrínseca de la tecnología Blockchain. A su vez, la previa definición de las reglas permite un ahorro sustancial en los costos legales de supervisión y ejecución del contrato.

Los Smart Contracts de la red de Ethereum, tienen tres características principales:

1) Inmutabilidad: A diferencia de un software normal, una vez que se ponen en la red, los Smart Contracts no pueden modificarse. Nadie ni nada puede alterar sus condiciones iniciales. La única manera de modificar el contrato sería convencer a la mayoría de los participantes de la red de Ethereum que esa modificación es buena para todos, algo que no es tarea fácil y muchas veces no vale la pena debido al tiempo que esto implicaría. Además, la inmutabilidad, permite resistencia a la manipulación.

2) Descentralización: Como estos se ejecutan sobre la Blockchain, garantizan que el acuerdo se cumpla automáticamente sin necesidad de una empresa que los mantenga ni de ningún tipo de intermediario. Tampoco hay alguien que tenga un grado de superioridad con respecto al resto. Todos los nodos almacenan los contratos con la misma información y el mismo estado.

3) Transparencia: Los Smart Contracts son de código abierto, por lo que cualquiera puede verlos. La confidencialidad es incrementada debido a que no existen compañías intermediarias que administren y utilicen la información del contrato inteligente para el beneficio de terceras partes.

Dapps

Como mencione anteriormente, los Smart Contracts son la base para la construcción de Daaps. Este concepto se refiere a las aplicaciones descentralizadas las cuales están basadas en un Smart Contract que se ejecuta en una red de miles de computadoras. La principal diferencia con las apps tradicionales es que las Dapps descentralizan la ejecución del programa y la seguridad de los datos. Esto quiere decir que no dependen de una entidad centralizada como podría ser Google, sino que usan el poder computacional y el almacenamiento de la red. Esto tiene una serie de ventajas; si los servidores de Google fallan, sus usuarios van tener problemas usando la app. Contrario a esto con una Dapp, como esta corre sobre miles de computadoras descentralizadas, si una falla la app va a seguir funcionando.

Oracle Services

Un Smart Contract se puede fundamentar pura y exclusivamente en la información que está disponible en la Blockchain. A su vez, estos también se pueden basar en información que esta por afuera de la Blockchain. Esto es un poco más complejo porque en este caso los contratos tienen que obtener información del mundo real, lo que implica la necesidad de un grado más de seguridad y confianza. Estos riesgos adicionales se pueden reducir utilizando Oracle Services, los cuales son servicios de terceros que permiten que los Smart Contracts reciban datos que no están en la Blockchain como lo puede ser el precio de un activo, coordenadas, temperaturas o el clima. El más popular es ChainLink.

Beneficios de los Smart Contracts

Para ver los beneficios vamos a hacer una comparación entre un Smart Contract y su equivalente en el espacio tradicional. Supongamos que queremos escribir el siguiente contrato; si María le envía X número de tokens A a Juan y Juan el mismo número de tokens B a María, va a existir un swap de los tokens en donde María recibe los de Juan y Juan los de María. Sin un Smart Contract, una manera de lograr esto sin que María tenga que confiar directamente en Juan y viceversa, es creando un contrato de Escrow con un intermediario. Este intermediario va a recibir los tokens de María y de Juan, y cuando se cumplan las condiciones le va a enviar a cada uno los tokens que le corresponden. Este escenario es el que se describe en la siguiente figura (Figura 6).

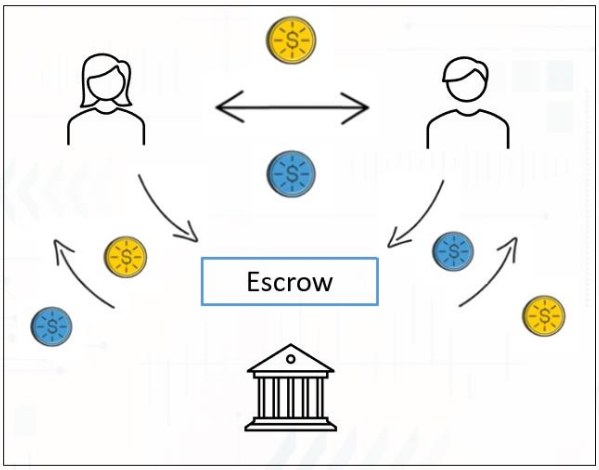


Figura 6: Swap de un token con un intermediario (Escrow). Fuente: elaboración propia

Esta situación tiene alguna serie de problemas que vamos a ver a continuación. El primero es que no nos queda alternativa que confiar en los intermediarios. No hay garantía de que el intermediario no robe los tokens después de recibirlos por lo que si o si tenemos que confiar en la reputación del mismo o incluso contratar un seguro para la operación. Debido a esto, claramente esta operación no es determinística. Si algo sale mal, el output que puede resultar tiene infinitas posibilidades dependiendo de muchos factores. En contraste a esto, el Smart Contract funciona de una manera totalmente automatizada y determinística, lo que asegura que ambas partes reciban los fondos cuando se cumplen las condiciones iniciales estipuladas en el contrato. Además, los Smart Contracts pueden almacenar fondos por sí solos, algo que claramente no es posible si utilizamos un contrato tradicional.

El segundo problema es en cuanto a la rapidez. Dependiendo del intermediario, María y Juan quizás tienen que esperar varios días hasta que se haga el swap de los tokens, además de la restricción de los fines de semanas y horarios no bancarios. Con los Smart Contracts estos problemas desaparecen ya que los contratos se pueden ejecutar en segundos después de que se cumplen las condiciones estipuladas y cualquier día del año, en cualquier horario.

Otro inconveniente a mencionar es el costo. Los contratos tradicionales no son costosos solamente por el uso de un intermediario sino que también hay que tener en cuenta los costos indirectos en caso de que algo salga mal, es decir, los costos que implican un arbitraje legal o un fraude. Estos últimos también son un gran problema y costo oculto para el intermediario. El fraude es algo muy común en las finanzas tradicionales y por eso es que las grandes empresas y bancos tienen equipos

enormes dedicados pura y exclusivamente a prevenirlos. Si volvemos a nuestro ejemplo, en el caso de los contratos tradicionales el intermediario tiene que asegurarse de que que ambos tokens son legítimos antes de iniciar el swap y también que ambas partes tienen la disponibilidad para utilizar esos tokens en ese momento del tiempo. Con los Smart Contracts, los tokens pueden ser verificados fácilmente en la Blockchain y con firmas digitales se puede ver también fácilmente si María y Juan pueden utilizar esos tokens, todo esto de una manera muy fácil, rápida y con un costo ínfimo.

Por último, otro beneficio de los Smart Contracts que es importante mencionar es la reusabilidad. El mismo Smart Contract que usan María y Juan para hacer un swap de tokens puede ser utilizado por otras personas mientras que los contratos tradicionales no, tendrías que firmar el contrato correspondiente y pagar los honorarios/comisiones de nuevo.

Principales riesgos asociados a los Smart Contracts

Si bien los Smart Contracts tienen muchos beneficios, es importante que a la hora de hablar de ellos también tengamos en cuenta los riesgos que estos implican. Uno de los riesgos más importantes a la hora de interactuar con los Smart Contracts es uno que puede afectar a cualquier software, los bugs, es decir, problemas o errores en los códigos del contrato. El mejor ejemplo para ilustrar porque esto puede ser un problema muy grande es el caso de The DAO (Decentralized Autonomous Organization). Esta organización, permitía a los usuarios depositar criptomonedas a través de un Smart Contract y obtener rendimientos en base a lo que el DAO hacía, tomando decisiones crow sourced y descentralizadas. Lo que sucedió fue que la organización había juntado USD 150 millones en Ether (cuando este valía USD 28 aproximadamente) pero el código no era lo suficientemente seguro por lo que hubo alguien que encontró la manera de vaciar el DAO. Esto puede ser visto como un hackeo o como alguien que simplemente sacó ventaja de cómo estaba hecho el contrato. Desde ese momento, todos los contratos de la red Ethereum pasan por una auditoria de seguridad que usualmente es hecha por muchos equipos, no solo uno.

Otro riesgo a la hora de interactuar con los Smart Contract son los cambios en los protocolos. Si hay un cambio en la red de Ethereum por ejemplo, puede darse el caso de que ciertos contratos se comporten de una manera distinta, lo que puede traer problemas muy serios.

Tokenización de activos

Otra de las funciones que proveen las Blockchains a través de los Smart Contracts tiene que ver con la tokenización de activos. Tal como surge de la organización Security Token Standard, existen dos tipos de tokens: los Security Tokens por un lado, diseñados para representar intereses de propiedad completos o fraccionados sobre activos, y los Utility Tokens que otorgan acceso a una red, y se utilizan como medio de pago para adquirir productos ofrecidos dentro de dicha red.

La Tokenización de activos surge como una herramienta que permite la representación, comercialización y registro descentralizado de propiedad de determinados activos subyacentes. Los tokens representan una unidad de valor digitalizada en la Blockchain, a partir de la existencia de un activo real o virtual. El valor del token se encuentra directamente vinculado al valor económico y los derechos derivados del activo que representan, los cuales pueden ser tanto físicos (por ejemplo commodities o real estate), como digitales o intangibles (acciones de empresas, títulos de deuda, índices accionarios o criptomonedas). En el caso de los activos nativos digitales (como podrían ser Bitcoin o Ether), estos solo existen en la Blockchain, dado que su existencia y valor se derivan de la propia tecnología, siendo la robustez y confianza en el protocolo que las rigen, su principal sustento.

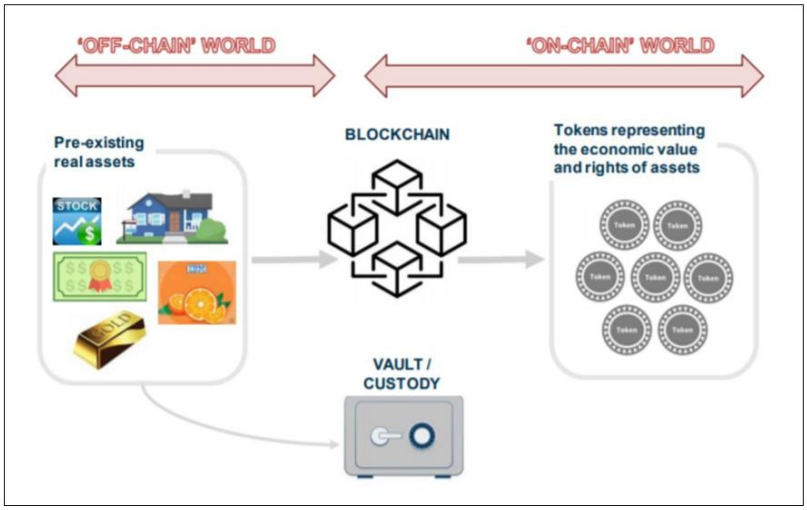


Figura 7: Proceso de tokenización de activos. Fuente: OECD, 2020

El proceso de creación y emisión de tokens sobre determinados activos reales, se puede realizar a través de un procedimiento conocido como Security Token Offering que es esencialmente la oferta pública de un instrumento que cumple con determinados requisitos regulatorios y utiliza la tecnología Blockchain. La Blockchain utilizada puede crearse específicamente con ese propósito o puede utilizarse un protocolo prexistente, como Ethereum.

A continuación vamos a enumerar algunos beneficios claros que pueden percibirse gracias a la Tokenización de activos. En primer lugar, los tokens sobre activos típicamente ilíquidos (como inmuebles, obras de arte, acciones de empresas de capital privado o instrumentos de deuda privada) podrían comercializarse en distintos mercados, permitiendo ampliar considerablemente la base de inversores potenciales. Así se beneficiarían por un lado los inversores, dada su mayor libertad y flexibilidad para invertir en activos que antes les eran inaccesibles y, por otro lado, los vendedores que podrían obtener un mayor redito por el activo subyacente transado. Además, la tokenización permite a nuevos inversores acceder a la compra de activos que antes se encontraban reservados para inversores institucionales. Esto se da gracias a fraccionamiento de activos de gran tamaño en unidades más pequeñas. Los tokens podrían representar porcentajes muy pequeños de los activos subyacentes, requiriendo un ticket de inversión mínimo y significativamente menor al que requeriría la inversión directa en el activo subyacente. Adicionalmente, estos tokens podrían comercializarse en mercados secundarios, globales y con funcionamiento las veinticuatro horas del día todos los días del año, implicando una reducción notable en los horizontes de inversión requeridos para ciertos activos y mercados.

La utilización de contratos inteligentes para la compra-venta de activos, permite la automatización de procesos que tradicionalmente implicarían la participación de múltiples intermediarios y procesos manuales. Esto significaría una reducción en la carga administrativa y menor participación de intermediarios, generando un impacto directo en los costos de intermediación. En ese sentido, la desintermediación y automatización redundan en una mayor eficiencia en la transferencia de valor, resultando en transacciones más rápidas, potencialmente menos costosas y sin fricciones.

Los security tokens ofrecen un registro de los derechos y responsabilidades de su tenedor, así como también un historial de propiedad. Esto puede permitirle al potencial comprador informarse sobre la identidad de la contraparte y el origen o proveniencia del activo transado. A su vez, el monitoreo en tiempo real permite una mayor integridad, inmutabilidad y seguridad en la información, facilitando la tarea de los reguladores por medio de auditorías automáticas o semiautomáticas.

Un nuevo sistema financiero

Luego de haber visto en detalle los fundamentos teóricos y técnicos del ecosistema cripto, estamos en condiciones de ver cómo y por qué las criptomonedas y las distintas Blockchain están creando un nuevo sistema financiero que es capaz de competirle al sistema tradicional y quizás en un futuro llegar a reemplazarlo. Para esto vamos a ver distintas alternativas dentro del mundo crypto, tanto en los productos centralizados como en los descentralizados.

Decentralized Finance (DeFi)

El concepto DeFi viene de Decentralized Finance y es un movimiento que busca lograr un nuevo sistema financiero que esté abierto para cualquier persona sin ningún intermediario como lo podrían ser los bancos, los brokers, cualquier servicio escrow o incluso los gobiernos. Es una nueva manera de acceder a lo que son los servicios financieros que todos conocemos como podrían ser los sistemas de pagos, préstamos, trading pero de una forma más eficiente, justa, barata y abierta.

Para alcanzar ese objetivo, DeFi se basa fuertemente en la criptografía, Blockchain y los Smart Contracts, los cuales son los ladrillos en base a los que todo este sistema es construido. Hoy en día, la mayoría de los proyectos DeFi están basados en la red de Ethereum y en este trabajo me voy a enfocar en ellos pero hay que tener en cuenta que la competencia está surgiendo muy rápidamente. Las razones por las que Ethereum Network es la más fuerte en este ecosistema son: la red de Ethereum y su lenguaje de programación Solidity permiten escribir Smart Contracts avanzados que contienen toda la lógica para las aplicaciones DeFi, Ethereum tiene el ecosistema más desarrollado con miles de desarrolladores y usuarios trabajando e interactuando con nuevas Dapps. Además es la red que tiene más TVL (Total Value Locked), lo que genera un valor agregado en términos de confianza y seguridad.

¿Qué se puede hacer en DeFi?

- Lending and borrowing

El pedir prestado y prestar dinero es uno de los pilar de las finanzas tradicionales y generalmente se hace a través de bancos o alguna entidad financiera de ese estilo. Ahora, gracias a Defi también se puede hacer de una manera descentralizada, sin intermediarios y sin tener que pedir permisos a nadie. Como todo esto que estamos viendo, esto se hace a través de Smart Contracts.

Un ejemplo es el caso de Compound el cual es uno de los cientos de protocolos algorítmicos autónomos de interés que podemos encontrar en el ecosistema DeFi. ¿Qué quiere decir esto? Son plataformas que le permiten a los usuarios ofrecer sus activos en una especie de Money Market (que obviamente es un Smart Contract) para que otro los tome prestados y pague una tasa de interés por ello. Para poder pedir prestado tenes que dejar un colateral y en la mayoría de los casos estos préstamos son sobre colateralizados lo que quiere decir que la persona que desea recibir el préstamo tiene que dejar una garantía mayor que el préstamo que está tomando. Esto se debe a la alta volatilidad que tenemos en el mundo crypto. Con la sobrecolateralización se reducen los riesgos de liquidación de las posiciones.

Otra cosa importante de definir es cuales son los limites para pedir prestado y cómo se definen. Existe un limite y este depende principalmente de dos cosas; la primera es cuantos fondos hay disponibles para pedir prestado en un mercado en particular y la otra es el colateral factor. Esto es lo que determina cuanto podes tomar prestado basado en la calidad del activo que vos dejas en garantía. DAI y ETH por ejemplo tienen un colateral factor de 75% en Compound, lo que te dice que si vos pones $100, te podes llevar hasta $75 prestado. Si queremos llevar este razonamiento a una formula, cuando uno toma prestado siempre se tiene que cumplir que:

Valor del préstamo < Valor del colateral x Collateral Factor

Si esta condición se cumple no hay límite acerca de cuánto tiempo el usuario puede tener el préstamo, ahora, si el lado derecho de la ecuación se pone por debajo del izquierdo, la posición se liquida para repagar el préstamo y de este modo evitar que el prestamista tenga chance de perder el capital que prestó.

Otra pregunta que tenemos que responder es cómo se determina la tasa de interés que se paga. En la mayoría de los protocolos es determinado por el ratio entre tokens en oferta y tokens que ya se tomaron prestados. Este interés es calculado por cada Bloque de Ethereum (cada quince segundos aproximadamente), lo que significa que la tasa de interés es muy variable. De todos modos existen protocolos que ofrecen tasas estables como por ejemplo AAVE.

- Stablecoins

Las stablecoins son criptomonedas diseñadas para mantener una paridad con respecto a otro activo, como por ejemplo el dólar estadounidense, y fueron creadas con el objetivo de poder tener una opción con casi nula volatilidad dentro del ecosistema cripto. Estas han ganado mucha popularidad en países con fuertes controles/restricciones cambiarias y alta inflación como son el caso de Argentina y Venezuela, ya que son una alternativa fácil y muy barata para poder dolarizar ahorros y de ese modo proteger la riqueza frente a la incertidumbre y perdida de valor de riqueza. También son una muy buena alternativa para enviar dinero de un lugar a otro porque las transacciones se hacen de forma instantánea, sin la necesidad de permisos y a un costo extremadamente bajo en comparación a lo que es una transferencia bancaria, la cual puede tardar varios días, es costosa y con muchos requerimientos y autorizaciones previas. Por esto es que también son muy populares entre las personas que han emigrado y necesitan enviar remesas a sus familiares que aún se encuentran en su país de origen. A su vez, debido a los bajos costos y su rapidez, son un gran acelerador de la adopción de las criptomonedas como medios de pago y la principal fuente de entrada al ecosistema. Esto último se ve claramente en la figura 8, donde se muestra el gran crecimiento que ha tenido la capitalización de mercado de estos activos en el ultimo bull run del ecosistema, pasando de una capitalización de mercado de 20 billones de dólares a 120 billones. Como hay cada vez más gente ingresando a este mundo, la demanda por stablecoins creció exponencialmente.

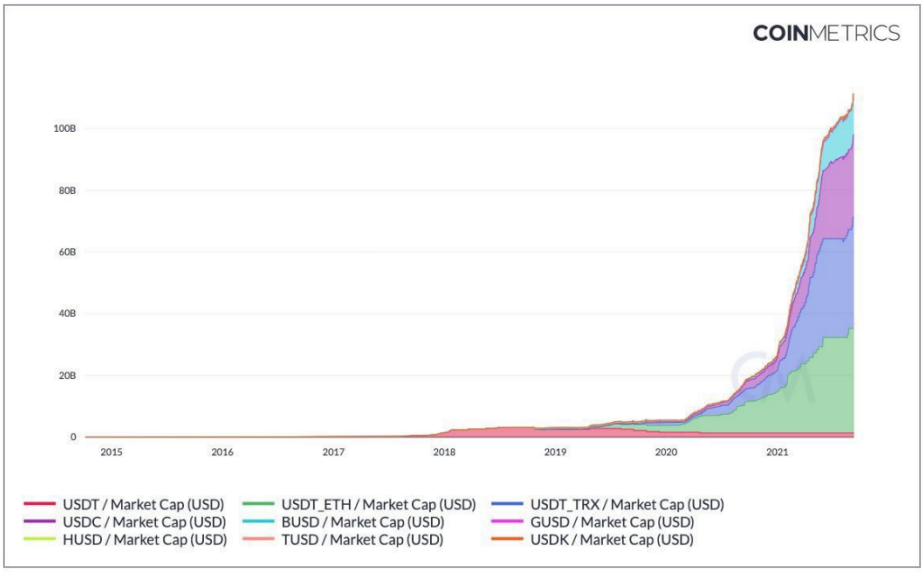


Figura 8: Crecimiento de la capitalización de mercado de las stablecoins. Fuente: Coinmetrics

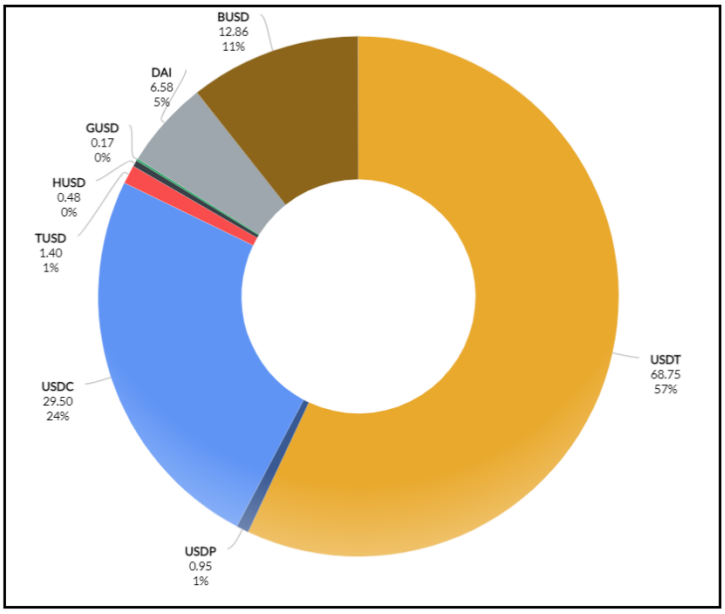


Figura 9: Capitalización de mercado de las stablecoins. Fuente: TheBlockCrypto.com

Dentro de ellas tenemos principalmente dos; las stablecoins colateralizadas por moneda Fiat (USD en la mayoría de los casos) y las que están colateralizadas en criptomonedas. Las primeras no pertenecen al ecosistema DeFi ya que son emitidas y controladas por empresas centralizadas. Aunque para muchos esta no es la mejor opción, de todos modos permiten una gran cantidad de beneficios para los usuarios y son el principal método de entrada al ecosistema cripto. Estas empresas centralizadas se encargan de recibir depósitos bancarios en moneda Fiat y emitir 1 unidad de stablecoin por cada dólar depositado. Cuando un usuario desea reconvertir su stablecoin a dólar, la empresa se encarga de destruir el token y le devuelve los dólares al usuario. De esta manera se mantiene la paridad. Las más conocidas son Tether (USDT) y USDCoin (USDC). Al ser empresas centralizadas, el usuario debe confiar en que estas cumplen con lo prometido, es decir que mantienen los dólares equivalentes a los tokens que emiten. Para mayor tranquilidad de los usuarios y obviamente por cuestiones regulatorias, estas empresas son auditadas por organismos independientes que garantizan que las emisoras no estén entrando en falta.

Por otro lado, con el uso correcto de Smart Contracts y ciertos incentivos se pueden crear stablecoins que siguen el valor del dólar estadounidense sin la necesidad de tener USD depositados en un banco. Estas son las stablecoins colateralizadas en criptomonedas las cuales también son del tipo "trust-minimized" lo que significa que son totalmente descentralizadas por lo que estas si van a pertenecer al ecosistema DeFi. El ejemplo más conocido de este tipo de criptomonedas es DAI de

MakerDao. En este caso, la política monetaria (emisión) es determinada por un grupo de tenedores de otra criptomoneda llamada MakerDao (MKR). Esto significa que no depende de ninguna institución centralizada, pero sí de una red de participantes que actuará a favor de los intereses de los usuarios. Como esto se hace a través de un Smart Contract, todos los participantes tienen la garantía de que si las condiciones no se cumplen, el contrato no se ejecutará.

Para generar los DAI se entrega otra criptomoneda como colateral a lo que se denomina un "Maker Vault" donde esos fondos quedan bloqueados y a cambio se recibe la cantidad de DAI correspondiente. Para recuperar una parte o la totalidad del colateral, el propietario del Vault debe pagar o saldar por completo los DAI que generó, más un interés. Una vez hecho esto, el Vault destruye los DAI y de esta manera el sistema automáticamente se balancea, evitando que se desarrolle un sistema inflacionario. Si el Vault no destruyera los DAI y permitiese la liberación del colateral, habría tokens circulando sin respaldo y los DAI valdrían cada vez menos.

- Decentralized Exchanges (DEXs)

Como ya vimos, el ecosistema cripto en su diseño original propone la total descentralización de los procesos de confirmación y generación de transacciones, así como el anonimato implícito en los pagos y operaciones. Sin embargo, dentro de la red han surgido nuevos servicios centralizados que crecen a pasos agigantados como el caso de los Centralized Exchanges (CEXs) los cuales es importante mencionarlos y caracterizarlos para luego pasar a hablar de los Decentralized Exchanges (DEXs). Los CEXs son plataformas que facilitan la compra y venta de criptomonedas, ya sea con monedas Fiat como el dólar estadounidense, como también con otras criptomonedas. Funcionan como intermediarios confiables en las operaciones y actúan como custodios al almacenar y proteger los fondos de los usuarios, por lo que son justamente un bróker como lo podría ser Interactive Brokers o TD Ameritrade pero en lugar de operar en el mercado financiero estadounidense, lo hacen en el mercado de las criptomonedas.

Si bien son un intermediario, es decir que en este caso no tenemos descentralización, es muy importante mencionarlos ya que han desempeñado y continúan desempeñando un papel vital en la aceptación de la criptomonedas por parte de los gobiernos, las empresas e instituciones de todo el mundo. Además de esto, estas plataformas son las que cursan la mayor parte del volumen de operaciones que se desarrolla en este mercado (ver Figuras 10 y 11).

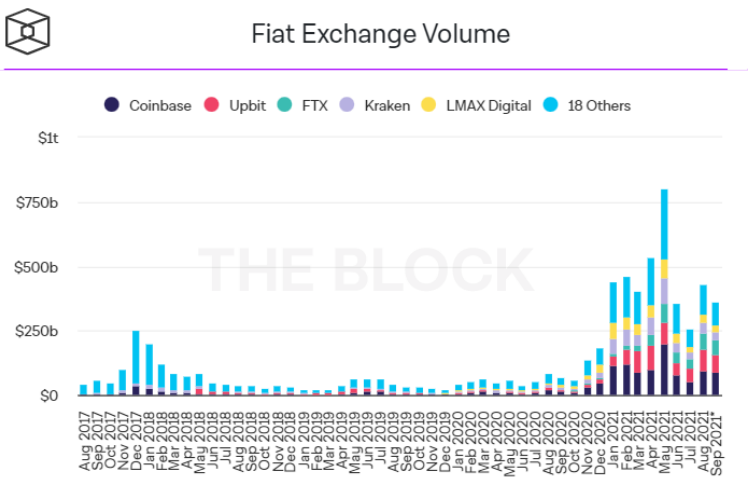


Figura 10: Volumen mensual Fiat Cripto operado en CEXs.

Fuente: TheBlockCrypto.com

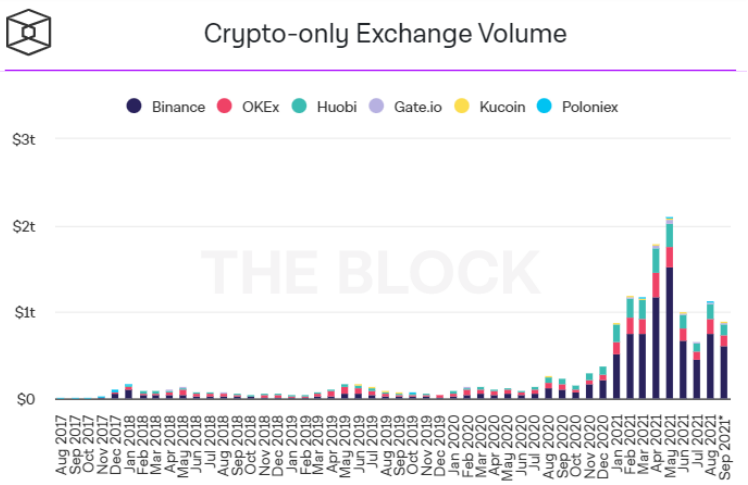


Figura 11: Volumen mensual Cripto-only operado en CEXs.

Fuente: TheBlockCrypto.com

Contrario a lo que sucede con los CEXs como puede ser el caso de Binance o Coinbase, los DEXs permiten a los usuarios intercambiar criptomonedas de una manera totalmente descentralizada sin la necesidad de permisos y sin tener que darle la custodia de tus activos a otra persona o intermediario debido a que los swaps se hacen directamente desde la wallet de un usuario hacia la del otro. Es importante destacar que no es que una opción es mejor que la otra ya que apuntan a usuarios distintos e intentan satisfacer necesidades distintas.

Tenemos principalmente dos tipos de DEXs, los Liquidity Pool Based y los Order Book Based. Un liquidity pool es un pool de tokens que están almacenados en un Smart Contract y son usados para facilitar el trading dentro de un DEX al proveer liquidez al mercado. Para entender por qué los necesitamos veamos primero como funcionan en detalles los CEXs mencionados anteriormente, los cuales son Order Book Based al igual que el NYSE o el NASDAQ. En estos mercados, los compradores y vendedores se juntan en los libros de ordenes colocando sus órdenes de compra y venta. Los compradores intentan comprar lo más barato posible y los vendedores, vender los activos al precio más alto que se pueda. Para que la operación se lleve a cabo se tienen que poner de acuerdo en el precio. Ahora, ¿qué sucede si no hay nadie que quiere poner su orden en el precio del momento o si no hay suficientes monedas para comprar? Acá es cuando aparecen los Market Makers que son entidades que facilitan el trading al estar siempre dispuestos a comprar o vender un activo en particular.

Este mismo mecanismo podría ser utilizado en los DEXs que corren sobre la red de Ethereum pero sería muy lento y caro, lo que resultaría en una experiencia de usuario muy mala. La razón de esto es que el Order Book Based Model dependen fuertemente de que tengas muchos Market Makers que estén despuestos a "Make the Market" para cierto activo. Sin estos se torna muy ilíquido y casi inusable. Los Market Makers colocan y cancelan cientos de miles de órdenes por minuto, cosa que hoy la red de Ethereum no puede soportar ya que procesa solamente entre 12 y 15 transacciones por segundo. Además, cada interacción con un Smart Contract cuesta un fee, entonces los Market Makers perderían fortunas solo por actualizar sus órdenes. Por todo esto es que aparecen los liquidity pools. En la manera más básica, un liquidity pool contiene dos tokens y cada pool crea un nuevo mercado para esos tokens en particular. Por ejemplo puede ser DAI/ETH en el DEX Uniswap. Cuando se crea un pool nuevo, el primer proveedor de liquidez es quien le pone el precio inicial al pool. Al dar liquidez, el proveedor recibe LP Tokens en proporción a cuanta liquidez le dio al pool y cuando se lleva a cabo un tarde, todos los tenedores de esos tokens se llevan un % de la comisión que se cobra por la operación.

Durante el último año todo el ecosistema basado en DEXs ha crecido mucho lo cual es muy importante para el desarrollo de la comunidad cripto porque le da a los usuarios la posibilidad de operar en el mercado sin tener que cumplir con regulaciones innecesarias y también poder hacerlo de una manera anónima y descentralizada. En términos de volumen, la utilización de los exchanges descentralizados no solo ha crecido de una manera exponencial en el último año (ver Figura 12) sino que también lo ha hecho en termino de sus rivales, los exchanges centralizados, a los cuales les ha robado parte del market share (ver Figura 13).

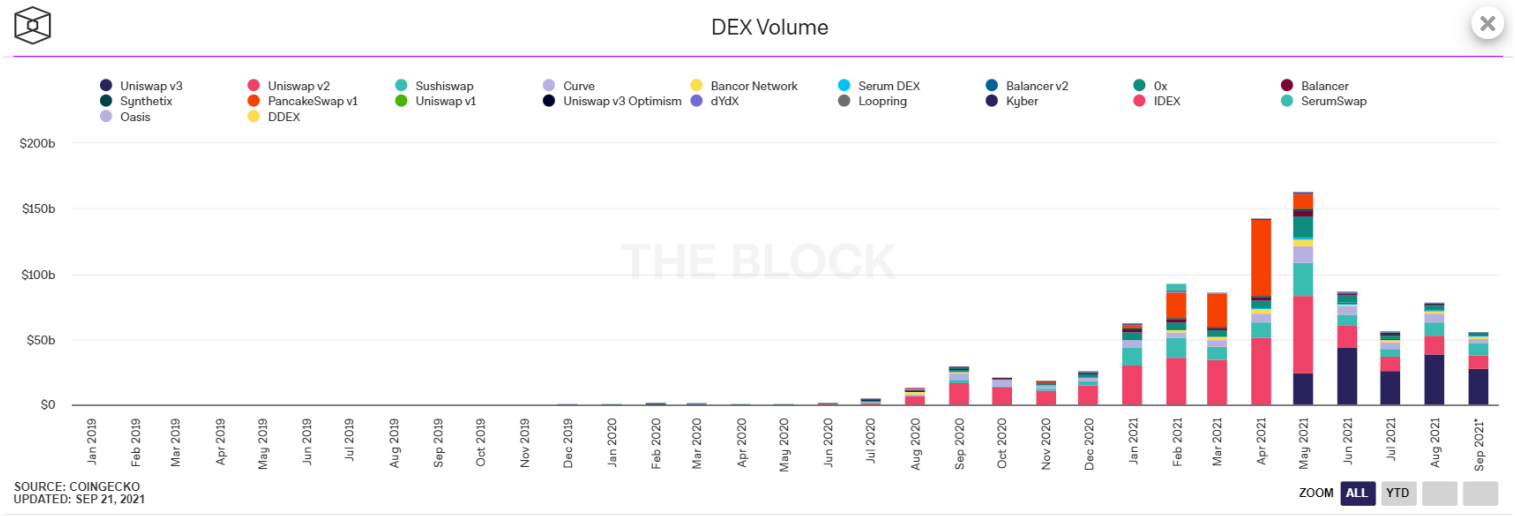


Figura 12: Volumen mensual operado en DEXs. Fuente: TheBlockCrypto.com

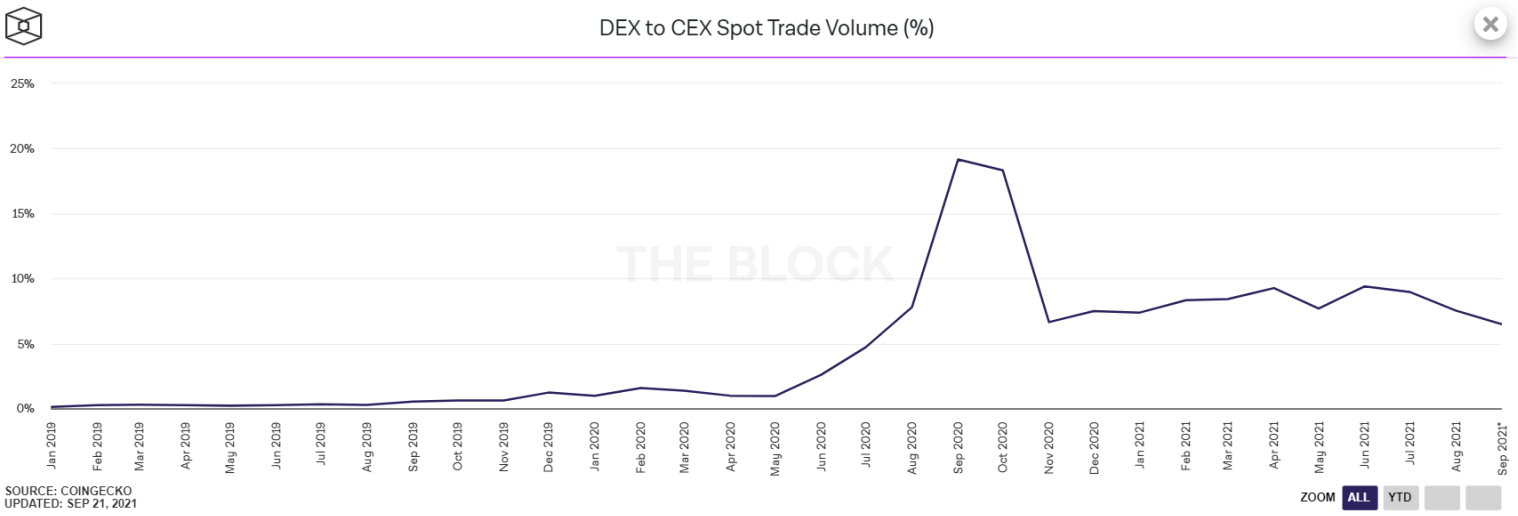


Figura 13: DEX/CEX volumen operado en el mercado Spot. Fuente: TheBlockCrypto.com

- Mercado de derivados

El volumen de los mercados de derivados siempre termina siendo mayor que el operado en el mercado de los activos subyacentes y por eso es que en el entorno DeFi hoy en día hay mucho desarrollo en esta rama del sistema financiero. Esto va desde los derivados clásicos como los swaps, futuros, forwards y opciones sobre las propias criptomonedas hasta la creación de derivados descentralizados de activos del sistema financiero tradicional. La diferencia con el mercado tradicional es que todo esto se va a construir de manera descentralizada sobre la Blockchain, sin la necesidad de una autoridad central, permisos y licencias y a un costo más bajo. Esto tiene como ventaja que acelera e incrementa el grado de innovación ya que cualquiera pude participar. Un ejemplo claro es Synthetics, una plataforma descentralizada que permite operar derivados.

- Seguros

Los seguros son otra parte de las finanzas tradicionales que pueden ser reproducidas en lo que es el ecosistema de DeFi. Uno de los usos más populares de los seguros en DeFi es la protección contra el fallo de un Smart Contract y protección de los depósitos. Incluso también existe la posibilidad de asegurar activos reales a través de contratos inteligentes descentralizados.

2021 Global Crypto Adoption Index

Para ver y entender como la adopción de las criptomonedas esta creciendo a un nivel muy fuerte vamos a hacer referencia al "2021 Global Crypto Adoption Index", un informe que analiza el crecimiento en la adopción de las criptomonedas a lo largo del mundo, elaborado por la empresa Chainalysis. Esta empresa es una plataforma analítica de Blockchain que brinda datos, software y servicios de research sobre el mundo de las criptomonedas y Blockchain a agencias gubernamentales, brokers, instituciones financieras, compañías de seguros y ciberseguridad en más de 60 países.

El objetivo del índice es proporcionar una medida objetiva de qué países tienen los niveles más altos de adopción de criptomonedas. Una forma de hacerlo sería simplemente clasificar los países por volumen de transacciones pero el inconveniente es que eso favorecería solo a los países con altos niveles de adopción institucional y profesional, ya que esos segmentos del mercado mueven la mayor parte del volumen. Si bien los mercados profesionales e institucionales son cruciales, el índice busca destacar los países con la mayor adopción de criptomonedas por parte de la gente común y centrase en casos de uso relacionados con transacciones y ahorro individual.

La metodología del índice

The Global Crypto Adoption Index se compone de tres métricas las cuales voy a explicar en detalle a continuación. Luego de recolectar los datos de esas métricas, clasifican a los 154 países que forman parte del índice, toman la media geométrica de la clasificación de cada uno en las tres métricas y luego normalizan ese número final en una escala de 0 a 1 para dar a cada país una puntuación que determina la clasificación general. Cuanto más cerca de 1 esté la puntuación final del país, mayor será la clasificación y por lo tanto su grado de adopción.

Métricas

- "On-chain cryptocurrency value received weighted by purchasing power parity (PPP) per capita": El objetivo de esta métrica es clasificar a cada país por su actividad total en el ecosistema de las criptomonedas, pero a su vez ponderar las clasificaciones para favorecer a los países donde ese valor es más significativo en función de la riqueza de la persona promedio y el valor del dinero dentro del país.

Calculan esta métrica estimando el valor total de las criptomonedas recibidas por ese país y ponderando el valor on-chain según la PPA (paridad de poder adquisitivo) per cápita, que es una medida de riqueza por residente. Cuanto mayor sea la relación entre el valor on-chain recibido y la PPA per cápita, mayor será la clasificación, lo que significa que si dos países tuvieran el mismo valor recibido, el país con la PPA per cápita más baja ocuparía el primer lugar.

- "On-chain retail value transferred, weighted by PPP per capita": El objetivo de esta métrica es medir la actividad de los usuarios no profesionales del ecosistema cripto, en función de la cantidad de transacciones que realizan con criptomonedas en comparación a la riqueza de la persona promedio de ese país. Para eso se realiza una aproximación de la actividad de las personas midiendo la cantidad de transacciones retail efectuadas con criptomonedas (transacciones menores a USD 10.000). Luego se realiza una clasificación para cada país de acuerdo con esta métrica, pero es ponderada para favorecer a los países con una PPA per cápita más baja.
- "Peer-to-peer (P2P) exchange trade volume, weighted by PPP per capita and number of internet users": El volumen de comercio P2P representa un porcentaje significativo de toda la actividad en el ecosistema de las criptomonedas, especialmente en los países emergentes y países con fuertes restricciones y controles cambiarios. Para este índice, Chainalysis clasifica a los países por su volumen de comercio P2P y los pondera para favorecer a los países con una PPA per cápita más baja y una menor cantidad de usuarios de Internet. El objetivo de esto es poder destacar a los países donde una gran parte de sus residentes están colocando una mayor porción de su riqueza en transacciones P2P con criptomonedas.

Resultados

La tabla de la Figura 14 muestra el Top 20 del "2021 Global Crypto Adoption Index", así como las calificaciones de estos países en cada una de las tres métricas mencionadas anteriormente.

Los datos también muestran que los residentes de cada vez más países de todo el mundo se están introduciendo en el ecosistema de las criptomonedas. La Figura 15 refleja la suma de los puntajes del índice de los 154 países que lo conforman para cada trimestre desde el segundo trimestre de 2019 hasta el presente. Claramente se ve el crecimiento exponencial de la adopción a lo largo de todo el mundo.

Country	Index score	Overall index ranking	Ranking for individual weighted metrics feeding into Global Crypto Adoption Index		
			On-chain value received	On-chain retail value received	P2P exchange trade volume
Vietnam	1.00	1	2	4	3
India	0.37	2	3	2	72
Pakistan	0.36	3	12	11	8
Ukraine	0.29	4	5	6	40
Kenya	0.28	5	28	41	1
Nigeria	0.26	6	10	15	18
Venezuela	0.25	7	22	29	6
United States	0.22	8	4	3	109
Togo	0.19	9	42	47	2
Argentina	0.19	10	17	14	33
Colombia	0.19	11	23	27	12
Thailand	0.17	12	11	7	76
China	0.16	13	1	1	155
Brazil	0.16	14	7	5	113
Philippines	0.16	15	9	10	80
South Africa	0.14	16	16	18	62
Ghana	0.14	17	37	32	10
Russian Federation	0.14	18	6	8	122
Tanzania	0.13	19	45	60	4
Afghanistan	0.13	20	38	53	7

Figura 14: The 2021 Global Crypto Adoption Index Top 20. Fuente: Chainalysis

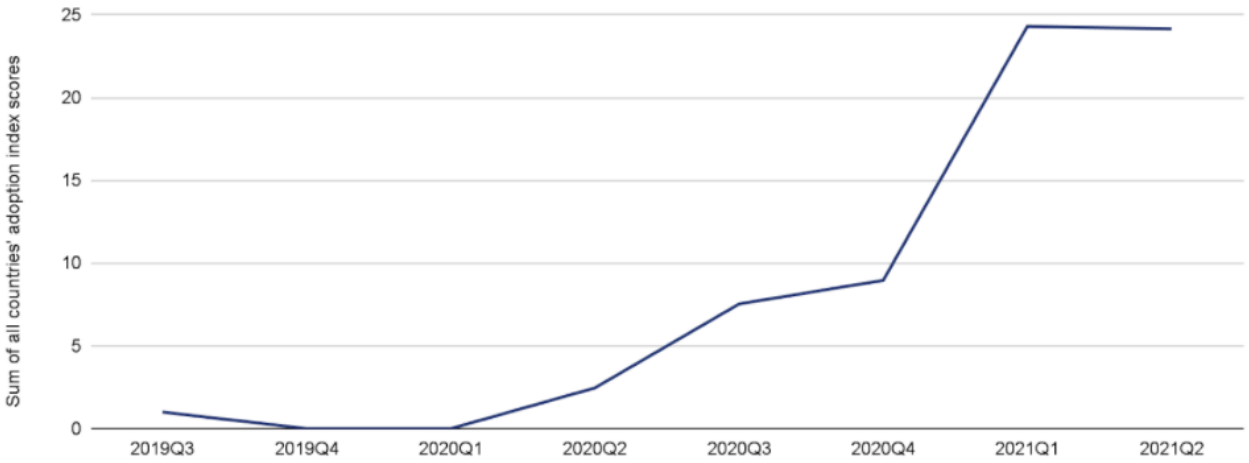


Figura 15: Global Crypto Adoption Index, sum of all countries index by quarter.

Fuente: Chainalysis

Al final del segundo trimestre de 2020, luego de un período de poco crecimiento debido a la gran caída de principios del año pasado por la crisis del Covid-19, la adopción global total se situó en 2.5.

Para el segundo trimestre de 2021, ese puntaje total fue de 24, lo que sugiere que la adopción global ha crecido más del 2300% desde el tercer trimestre de 2019 y más del 881% en el último año.

Las razones de esta mayor adopción difieren en todo el mundo. En los mercados emergentes, como ya mencionamos anteriormente, muchas personas recurren a las criptomonedas para preservar sus ahorros frente a la devaluación de las monedas Fiat de sus países y frente a los altos niveles de inflación. En estas áreas también se utilizan para realizar transacciones internacionales, ya sea para remesas individuales o para casos de uso comercial, como la compra de bienes para importar y vender. Esto se debe a que en muchos casos los gobiernos limitan la cantidad de moneda nacional que los residentes pueden sacar del país. Las criptomonedas les brinda a los residentes una forma de eludir esos límites para que puedan satisfacer sus necesidades financieras.

Un ejemplo claro es el caso de Argentina. Actualmente en ese país existe un fuerte control de capitales, el cual implica limitaciones para la compra de moneda extranjera pero también para el envío de fondos hacia el exterior. Una de esas limitaciones a la compra de moneda extranjera es para las personas físicas y jurídicas que son importadoras, las cuales tienen acceso al dólar oficial y por eso se les prohíbe acceder a otros tipos de dólares legales como pueden ser el dólar MEP o el dólar CCL. Ante la imposibilidad de acceder a los dólares legales de la bolsa, muchos importadores utilizan a las criptomonedas para poder hacerse de dólares legales. El proceso es muy parecido a la operatoria tradicional en la bolsa pero en lugar de utilizar bonos, se utilizan criptomonedas. El usuario compra alguna criptomoneda con pesos argentinos en un bróker local (usualmente se utilizan stablecoins para evitar la volatilidad) e inmediatamente la vende contra dólar.

Esto es bastante común en los productores agropecuarios que además de ser los grandes exportadores de Argentina, muchas veces son importadores de insumos para la producción por lo que se les aplica la restricción mencionada anteriormente. Como este negocio necesita de dólares para su desarrollo, por ejemplo para la compra de maquinaria, a los productores no les queda otra opción que utilizar criptomonedas para acceder a la compra de dólares sin la necesidad de recurrir al mercado ilegal. De este modo se ve claramente como las criptomonedas brindan una solución ante los controles de capitales que algunos gobiernos aplican sobre sus países.

Por esto, varios países de mercados emergentes, incluidos Kenia, Nigeria, Vietnam, Venezuela y Argentina, ocupan un lugar destacado en el índice. En gran parte esto también se debe a que tienen enormes volúmenes de transacciones en plataformas peer-to-peer (P2P). Muchos de los residentes

de estos países utilizan los exchanges de criptomonedas P2P como su principal acceso a este mundo porque no tienen acceso a exchanges centralizados o porque justamente buscan esquivar el control de sus gobiernos. Sabiendo esto, no sorprende que las regiones con muchos países emergentes como Asia central y meridional, América Latina y África, representen una gran parte del tráfico a los sitios web de servicios P2P (ver Figura 16).

.

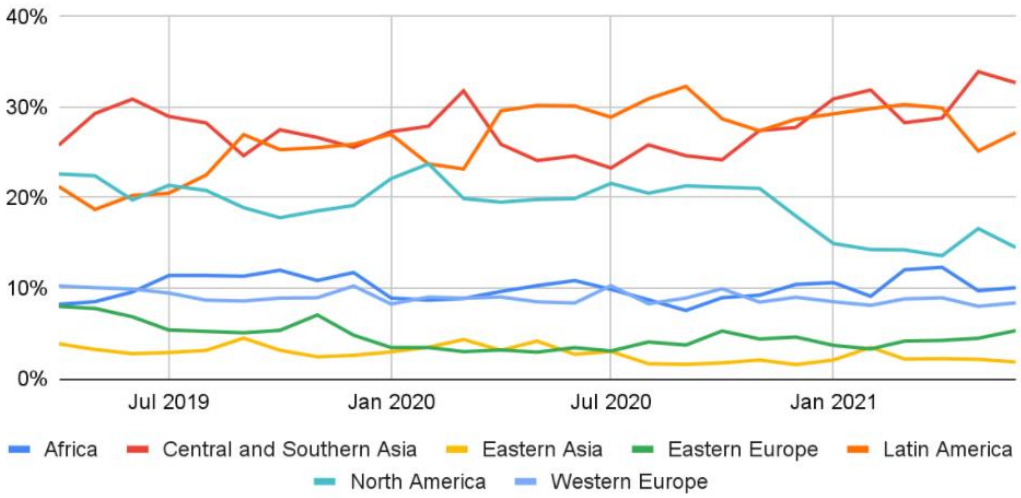


Figura 16: Monthly share of all web traffic P2P cryptocurrency platforms, Apr 19´ - Jun 21'.

Fuente: Chainalysis

Por el lado de la adopción en América del Norte, Europa occidental y Asia oriental, el crecimiento durante el último año se ha visto impulsado en gran medida por la inversión institucional. Esto va desde empresas que comienzan a comprar criptomonedas como una inversión a largo plazo hasta grandes instituciones financieras tradicionales como pueden ser bancos u fondos de inversión que frente a la demanda de sus clientes empiezan a ofrecer servicios vinculados a las criptomonedas y Blockchain.

Conclusiones

Luego de haber visto la gran cantidad de alternativas que pueden ser utilizadas y desarrolladas dentro del ecosistema de las criptomonedas y Blockchain, no quedan dudas de que son una gran competencia para el sistema financiero tradicional. Esto no viene simplemente por el lado de que gracias a DeFi y otros productos del ecosistema podemos replicar casi cualquier producto de la industria financiera que todos conocemos pero con la diferencia de que se hace de una manera descentralizada, menos costosa y más rápida sino también por el lado de que este nuevo sistema permite el ingreso de personas que quedan rezagadas de las finanzas tradicionales.

Las criptomonedas ayudan a disminuir las barreras de entrada a nuevos proveedores y desarrolladores de aplicaciones pero sobre todo, reducen las barreras de entrada al mundo de las finanzas para las personas que no están bancarizadas y para aquellos que residen en países con instituciones o marcos legales poco confiables, con fuertes controles cambiarios, altos niveles de inflación y devaluación. Por esto es que el mayor crecimiento de la adopción de criptomonedas se esta llevando a cabo en los países emergentes como vimos anteriormente.

A medida que los años pasan, la gente se va dando cuenta de que esto es una tecnología revolucionaria que va más allá de la especulación con una suba de precios de los tokens y que es algo que ha llegado para quedarse. Por esto es que la cantidad de usuarios, transacciones, aplicaciones, productos, el volumen operado y la cantidad de dinero que ingresa desde el sistema financiero tradicional hacia este nuevo ecosistema crecen de manera exponencial, incluso llegando al punto de que ciertas personas decidan dejar de utilizar los productos y sistemas financieros tradicionales para pasarse cien por ciento al ecosistema cripto, algo que hasta hace unos años era impensado y hoy es una realidad.

A su vez, en el ultimo año, las instituciones financieras tradicionales como por ejemplo bancos o fondos de inversión han empezado a ofrecer soluciones ligadas a las criptomonedas y Blockchain debido a la fuerte demanda por parte de sus clientes. El hecho de que estas instituciones comiencen a introducirse en este nuevo paradigma denota claramente que se han dado cuenta que es una gran competencia que ha llegado para quedarse y que en un futuro muy cercano podría darse el caso de que los productos vinculados a las criptomonedas y Blockchain manejen un volumen superior que el de la banca tradicional.

Si bien este trabajo se concentra en los aspectos financieros de las criptomonedas y su tecnología subyacente Blockchain, me gustaría mencionar que este ecosistema también tiene la capacidad de ser empleado en cualquier ámbito de la administración, política y gobierno. La inmutabilidad de la Blockchain permite garantizar la irreversibilidad, autenticidad, y auditabilidad de la actividad empresarial, gubernamental y ciudadana. A su vez, la característica de anonimato tiene la promesa de proteger la confidencialidad de sus participantes por lo que actividades tales como transferencia de fondos, votaciones, registro de activos tangibles e intangibles pueden mantenerse anónimas y de esta forma, lograr mantener la discreción del comportamiento ciudadano.

En conclusión, con lo presentado a lo largo de todo este trabajo se ve que este ecosistema ha llegado para quedarse, que tiene un potencial de crecimiento enorme y que es una clara competencia para el sistema financiero tradicional. De acá en adelante habrá que ver si ambos sistemas logran algún tipo de integración o si cada uno seguirá por su lado, compitiendo entre sí.

Bibliografía

"Internet del Dinero", Andreas Antonopoulos, Noviembre 2017.

"Mastering Bitcoin: Programming the Open Blockchain", Andreas Antonopoulos, Diciembre 2014.

"Mastering Ethereum: Building Smart Contracts and DApps", Andreas Antonopoulos, 2018.

"El Patrón Bitcoin", Saifedean Ammous, Octubre 2018.

"El Libro de Satoshi", Phil Champagne, Junio 2018.

"Cryptoeconomics: Fundamentals principles of Bitcoin", Eric Vouskil, Febrero 2020.

"Cryptoeconomy: how Blockchain, Cryptocurrencies and Token-Economy are disrupting the financial world", Aries Wanlin Wang, Noviembre 2018.

https://www.gemini.com/cryptopedia/centralized-exchanges-crypto#section-the-regulation-of-centralized-exchanges

https://coinmetrics.io/insights/original-research/

https://analytics.skew.com/dashboard/stable-coins

https://www.chainalysis.com/company/

https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index

https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

https://coinmarketcap.com/charts/

https://academy.binance.com/es/articles/proof-of-work-explained

https://www.theblockcrypto.com/data/crypto-markets/spot

https://es.ihodl.com/tutorials/2018-04-25/transacciones-chain-y-chain-como-funcionan/

Autorización para publicar los trabajos finales

Completar cada punto con SI o NO:

- **Repositorio Institucional** *(completar con SI o NO)***:**

  ___SI__ autorizo a la Universidad del CEMA a publicar y difundir en el **Repositorio Institucional** de la Universidad de la Biblioteca con fines exclusivamente académicos y didácticos el Trabajo Final de mi autoría.

- **Catálogo en línea** *(completar con SI o NO)***:**

  ___SI__ autorizo a la Universidad del CEMA a publicar y difundir en el **Catálogo en línea** (acceso con usuario y contraseña) de la Biblioteca con fines exclusivamente académicos y didácticos el Trabajo Final de mi autoría.

- **Página web UCEMA** *(completar con SI o NO)***:**

  ___SI__ autorizo a la Universidad del CEMA a publicar y difundir en la **página web de la Universidad** como Trabajo destacado, si el mismo obtuviese la distinción correspondiente, con fines exclusivamente académicos y didácticos el Trabajo Final de mi autoría.

Juan Martin Vergara

Alumno: Juan Martin Vergara
D.N.I. : 40783668