



FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES (ICADE)

El poder de un ecosistema descentralizado (DeFi): estudio de Ethereum, Cardano y Polkadot

Nombre: Ignacio Pedrosa Díez

Tutor: Lourdes Fernández Rodríguez

MADRID | Junio de 2021

RESUMEN

Este Trabajo de Fin de Grado estudia el potencial de un ecosistema descentralizado conocido por sus siglas en inglés DeFi y su tecnología *blockchain* subyacente. Además, se analizarán sus casos de uso y las aplicaciones descentralizadas (dApps) con sus características. En este contexto, se van a examinar tres proyectos de *blockchain* y su relación con las finanzas descentralizadas: Ethereum, Cardano y Polkadot. A través de un estudio analítico de la evolución y desarrollo de este sector, se pretende explicar el funcionamiento de un ecosistema DeFi y todas sus características. La peculiaridad de las finanzas descentralizadas es su capacidad disruptiva que tiene para desafiar a las finanzas tradicionales, por ello se explicarán diferentes casos de uso de esta tecnología, así como algunas aplicaciones actuales que existen en el mercado.

Palabras clave: DeFi, blockchain, token, ecosistema descentralizado, contratos inteligentes, Ethereum, Cardano, Polkadot, protocolo de consenso, tecnología de libro mayor distribuido (DLT), aplicaciones descentralizadas (dApps), criptomonedas.

ABSTRACT

This final dissertation studies the potential of a decentralized ecosystem known by its acronym DeFi. It also aims to analyze its underlying blockchain technology, use cases and decentralized applications (dApps) with their characteristics. In this context, the case of three blockchain DeFi projects Ethereum, Cardano and Polkadot is also analyzed. Through an analytical study of the evolution and development of this sector, the aim is to explain the functioning of a DeFi ecosystem and all its characteristics. The peculiarity of this decentralized finance is its disruptive capacity to challenge traditional finance, therefore different use cases of this technology will be explained, as well as some current applications that exist in the market.

Keywords: DeFi, blockchain, token, decentralized ecosystem, smart contracts, Ethereum, Cardano, Polkadot, consensus protocol, distributed ledger technology (DLT), decentralized applications (dApps), cryptocurrencies.

ÍNDICE

1. INTRODUCCIÓN	2
1.1 Propósito general	2
1.2 Justificación de la elección del tema	2
1.3 Objetivo de la investigación	3
1.4 Metodología	4
1.5 Estructura del trabajo	5
2. ¿QUÉ ES LA DESCENTRALIZACIÓN FINANCIERA?	7
2.1 Definición	7
2.2 Propiedades de un ecosistema DeFi	8
2.3 Evolución histórica	10
2.4 Comparación con las finanzas tradicionales	13
3. ¿QUÉ ES UNA PLATAFORMA BLOCKCHAIN?	16
3.1 Evolución y desarrollo	16
3.2 Funcionamiento de las plataformas <i>blockchain</i> y los <i>smart contracts</i>	17
3.3 Plataformas Blockchain	20
3.3.1 Ethereum	21
3.3.2 Cardano	24
3.3.3 Polkadot	25
4. APLICACIONES DE UN ECOSISTEMA DESCENTRALIZADO	29
4.1 DeFi vs <i>Fintech</i>	29
4.2 Casos de uso de la descentralización financiera	30
4.2.1 Intercambio de activos en la red de blockchain.....	31
4.2.2 Mercado de préstamos (PLFs) y pagos descentralizados	31
4.2.3 Criptomonedas estables.....	32
4.2.4 <i>Yield Farming</i>	32
4.2.5 Predicción de mercados.....	33
4.2.6 Servicios de custodia (<i>E-wallets</i>)	33
4.2.6 Tokens No Fungibles (NFTs).....	34
4.3 Análisis de las principales aplicaciones descentralizadas (dApps)	35
4.3.1 Uniswap	35
4.3.2 Maker	35
4.3.3 Aave	36
4.3.4 Compound.....	36
4.3.5 InstaDApp	36

4.3.6 Flexa.....	37
5. CONCLUSIONES DEL TRABAJO.....	40
6. BIBLIOGRAFÍA.....	42
7. ANEXOS.....	48
Anexo I: Datos de capitalización y TVL de Ethereum.....	48
Anexo II: Crecimiento del ecosistema DeFi a lo largo de 2021	48
Anexo III: Direcciones Ethereum que interactúan con protocolos DeFi.....	49

Capítulo I: Introducción

1. INTRODUCCIÓN

1.1 Propósito general

El propósito de este Trabajo Fin de Grado es el estudio del concepto de las finanzas descentralizadas, conocidas por su acrónimo en inglés DeFi. Consiste en un nuevo ecosistema de aplicaciones financieras que funcionan sobre redes *blockchain*. Una red de *blockchain* es una base de datos distribuida y segura que permite la transferencia de un valor o de un activo de un lugar a otro, sin intervención de una institución como intermediario. Por ello, se estudiarán no sólo las principales características y beneficios de las finanzas descentralizadas, sino también el funcionamiento de la tecnología *blockchain*. Además, este estudio se va a centrar en el caso particular de tres ecosistemas descentralizados, que son Ethereum, Cardano y Polkadot. se explicará por qué la mayoría de las aplicaciones DeFi se implementan en este tipo de redes que permiten utilizar contratos inteligentes, conocidos más por su acrónimo en inglés.

1.2 Justificación de la elección del tema

Pocos trabajos estudian el marco teórico-práctico de este nuevo ecosistema financiero que pretende revolucionar las finanzas tradicionales. La tecnología *blockchain* ha producido el auge de los servicios financieros descentralizados, que permiten desarrollar la innovación en el ámbito financiero, así como una mayor interoperabilidad y transparencia. Además, un ecosistema DeFi amplía la inclusión financiera, facilitando el acceso abierto a todos los individuos para crear una economía global. Según avanzamos hacia una economía digital, algunas empresas tecnológicas financieras conocidas como *fintech*, ya han comenzado a asumir algunos roles tradicionales pero las grandes instituciones financieras siguen manteniendo su posición. Su importancia a lo largo de la historia, actuando como mediadores y estructurando multitud de transacciones económicas les ayuda a conservar esa posición de liderazgo (Benston and Smith, 1976). Cabe destacar, que, aunque estas empresas tecnológicas financieras han conseguido reducir el monopolio de algunas grandes instituciones financieras, no han eliminado a los intermediarios del esquema financiero. Si la descentralización y la desintermediación continúan cobrando impulso, las finanzas descentralizadas pueden ser el siguiente paso en esta progresión.

El ecosistema DeFi se inspira en el Bitcoin y su revolucionaria “tecnología *blockchain*”, que permite que las transacciones se verifiquen en la red mediante consenso de los usuarios, evitando

así el control de una fuente central. Este nuevo planteamiento difiere de los sistemas centralizados que hasta ahora se utilizaban, ya que no solo pueden limitar la velocidad, sino que reducen la sofisticación de las transacciones al tiempo que ofrecen a los usuarios un control menos directo sobre su dinero. DeFi es diferente porque expande el uso de esta tecnología no sólo para realizar transferencias financieras sin intermediarios, sino que también extiende su uso a productos financieros más complejos. En el caso de las compras directas, las tecnologías descentralizadas basadas en *blockchain* destacan frente a los métodos tradicionales de pago como Visa o Paypal, ya que eliminan los intermediarios de las transacciones. Es decir, cuando una persona realiza un pago de una compra en un establecimiento, una institución financiera actúa entre el cliente y el negocio, controlando y haciendo posible que tenga lugar la transacción. En cambio, en un entorno DeFi las instituciones financieras quedan al margen, y esto podría extenderse a otras operaciones como préstamos, seguros, *crowdfunding*, derivados o apuestas.

Por ello, este trabajo pretende explicar las características fundamentales de los ecosistemas DeFi, analizar en detalle su funcionamiento y diferentes usos, así como destacar aquellos ecosistemas *blockchain* más relevantes en el mercado para el desarrollo del entorno descentralizado. Toda esta disrupción de estos nuevos ecosistemas es desafiante ya que intenta enfrentarse directamente a las instituciones tradicionales. Hay muchas incógnitas sobre el entorno DeFi y su futuro, pero cada vez hay más adeptos que creen en su potencial para revolucionar el sistema financiero. Aún así, todo depende de muchos factores como la aceptación social o regulación gubernamental, que afectará en el futuro a estas plataformas. Esta tecnología financiera es nueva, experimental y no está exenta de problemas, especialmente en lo que respecta a la seguridad o escalabilidad.

1.3 Objetivo de la investigación

Este trabajo se centrará en elaborar una guía introductoria a los ecosistemas DeFi, explicando sus principales características, focalizando el estudio en diferentes redes descentralizadas y su escalabilidad para otras aplicaciones DeFi. Para ello, se articulará la investigación en torno a los siguientes tres puntos:

- El primer objetivo es destacar las características principales de la idea de la descentralización financiera (DeFi), y qué supone la eliminación de intermediarios en las transacciones financieras. A través de este estudio, se quieren esclarecer las principales

oportunidades y desventajas que este cambio conlleva, así como realizar una guía introductoria para todas las personas ajenas a este concepto.

- En segundo lugar, se analizarán algunos de los diferentes ecosistemas de red descentralizada que predominan actualmente como Ethereum, Cardano y Polkadot, en los cuales se desarrollan la mayoría de las aplicaciones DeFi.
- Por último, se estudiarán algunas de las aplicaciones DeFi, clasificándolas según su utilidad. Muchas de ellas están ofreciendo oportunidades para un modelo económico completamente nuevo en todo el mundo, abarcando multitud de usos y solucionando problemas relevantes. Esto demuestra la capacidad de desarrollo del entorno DeFi, un ecosistema financiero disruptivo que pretende desafiar a los servicios centralizados.

1.4 Metodología

Con el fin de cubrir los objetivos de este trabajo, se realizará un análisis de la teoría general de la descentralización financiera a través del estudio de su tecnología subyacente: *el blockchain*. Para la elaboración de este estudio ha sido necesaria la lectura, comprensión y revisión de la literatura académica referente a la descentralización financiera y la tecnología *blockchain*. Para la búsqueda de estos artículos se han utilizado diferentes fuentes académicas como Google Scholar o Dialnet, además de otras plataformas de monitorización del mercado cripto como Coingecko o Defipulse.

Mi experiencia universitaria participando en un club de *blockchain* de la universidad de Northeastern me ha facilitado multitud de recursos como, por ejemplo, el estudio de proyectos relacionados con este ámbito, así como la comprensión y síntesis de los aspectos generales de los ecosistemas descentralizados.

En la primera parte del trabajo, se han utilizado artículos de autores relevantes dentro del campo de la descentralización financiera, como Yan o Bellavitis, así como informes de *blockchain* de diferentes instituciones. En la segunda parte, al tratarse de una visión más práctica que explicará las diferentes aplicaciones DeFi y algunos de los proyectos que existen en la actualidad, se ha tomado como referencia estudios específicos y los documentos explicativos de los propios proyectos de estas aplicaciones (*whitepapers*), así como plataformas de análisis del mundo cripto como Coingecko.

1.5 Estructura del trabajo

La estructura del trabajo es la siguiente:

En la primera parte, se va a presentar la teoría general sobre la descentralización financiera, analizando los siguientes aspectos: definición y concepto, evolución histórica y desarrollo y su comparación con las finanzas tradicionales. Este apartado finalizará con un análisis de la innovación que conlleva la descentralización financiera en el futuro.

En la segunda parte, se analizará y explicará la tecnología *blockchain* que utiliza un ecosistema descentralizado, explicando la importancia de que estas redes puedan ejecutar contratos inteligentes. Además, se estudia no sólo la red descentralizada principal conocida como Ethereum, sino también otras nuevas plataformas de *blockchain* innovadoras que ejecutan contratos inteligentes como Cardano y Polkadot. Esta parte, a su vez se dividirá en tres bloques:

1. Breve introducción histórica del desarrollo de la tecnología *blockchain*.
2. Explicación del funcionamiento de esta tecnología y del papel que juegan los contratos inteligentes, resaltando sus principales funciones y elementos.
3. Análisis de las tres principales plataformas descentralizadas y más innovadoras que existen actualmente: Ethereum, Cardano y Polkadot.

En la tercera parte, se explican los principales usos y aplicaciones de un ecosistema descentralizado destacando las principales oportunidades y limitaciones de cada uno de ellos. También, se destacará el crecimiento exponencial en los últimos años a través de diferentes métricas, con el fin de mostrar los máximos históricos que roza el valor total del sector DeFi.

Finalmente, se presentan las conclusiones del trabajo para poder responder a los objetivos previstos. También, se incluye una perspectiva futura que resuma el potencial de este entorno DeFi tan innovador y disruptivo.

Capítulo II:

Marco conceptual

2. ¿QUÉ ES LA DESCENTRALIZACIÓN FINANCIERA?

2.1 Definición

Hay muchas definiciones sobre la descentralización financiera, por lo que se expondrán algunas de ellas para tener un conocimiento más amplio de su significado. En su forma más simple, las finanzas descentralizadas son un concepto en el que los productos financieros están disponibles en una red pública de cadena de bloques descentralizada (*blockchain*), haciéndolos accesibles a todo el mundo y eliminando intermediarios. Esta descentralización financiera conocida como DeFi, utiliza criptomonedas y tecnología *blockchain* para realizar transacciones financieras. Se pretende democratizar las finanzas reemplazando a las instituciones tradicionales y centralizadas, por relaciones *peer-to-peer* que puedan proporcionar el espectro completo de servicios financieros (Napoletano & Schmidt, 2021). Otra conceptualización más específica de la descentralización financiera, la define como la transformación de productos financieros tradicionales en productos que operan sin un intermediario a través de contratos inteligentes en una cadena de *blockchain* (Meegan & Koens, 2010). Gudegeon et al., indica que un ecosistema DeFi es un “sistema financiero de igual a igual, que aprovecha los contratos inteligentes distribuidos basados en el libro mayor para garantizar su integridad y seguridad” (2020). Estas dos definiciones mencionan a los contratos inteligentes (*smart contracts*) como elemento fundamental de la descentralización financiera. Otra definición explica que este entorno DeFi es “un ecosistema de aplicaciones financieras que se está desarrollando sobre blockchain y “*Distributed Ledger Technology*” (DLT) o Tecnología de Libro Mayor Distribuido (Popescu, 2020).

En resumen, las definiciones mencionadas anteriormente describen las finanzas descentralizadas como un ecosistema de aplicaciones financieras, que utiliza los *smart contracts* como componente, consiguiendo tener dos propiedades clave: la integridad y la seguridad. El uso de redes de *blockchain* utiliza una tecnología conocida como *distributed ledger technology* que permite la realización y el funcionamiento de los *distributed ledgers*, que son un consenso de datos digitales replicados, compartidos, sincronizados y distribuidos geográficamente por diferentes sitios. A través de un mecanismo de consenso compartido, este sistema electrónico permite registrar transacciones que no son ejecutadas por una sola entidad, permitiendo el almacenamiento y utilización de datos descentralizados (Sunyaev, 2020). Por ejemplo, la red *blockchain* es una DLT con características específicas que, como su nombre indica se distribuye a través de bloques

formando una red. No hay un acuerdo general en la definición de descentralización financiera, por lo que este trabajo se va a centrar en la siguiente: DeFi son servicios financieros que no requieren intermediarios, ya que en su lugar ejecutan *smart contracts* que operan en una *blockchain* pública sin permisos.

2.2 Propiedades de un ecosistema DeFi

A través de la literatura estudiada sobre este trabajo, se pueden identificar diferentes características propias de un ecosistema financiero descentralizado. Según Meegan & Koens, hay diferentes características que definen las redes descentralizadas, (2010). En este estudio, queremos destacar las siguientes:

1. Modular: se puede explicar como la capacidad para construir un sistema financiero complejo y con múltiples componentes interconectados sobre criptoactivos (Gudegeon et al., 2020). Además, esta característica indica que los *smart contracts* pueden unirse como ladrillos de Lego para construir arquitecturas financieras complejas (Werner et al., 2021).

2. Flexibilidad: las finanzas descentralizadas se basan en un código fuente abierto, lo que permite que el programa sea utilizado, copiado y ajustado por cualquier persona. Además, la falta de regulación posibilita que no haya limitaciones para crear y usar diferentes servicios (Pierluigi et al., 2020).

3. Descentralización: como se ha explicado anteriormente, la descentralización se puede describir como la realización de servicios financieros sin necesidad de un intermediario de confianza, a través de un consenso descentralizado programable (Chen & Bellavitis, 2020).

4. Accesibilidad: las finanzas descentralizadas no tienen la capacidad de monopolizar la red por sí mismas y excluir a otros para participar, lo que permite que todos se beneficien de los efectos de la red y tener la capacidad de realizar transacciones (Huberman et al., 2019).

5. Innovación: las plataformas descentralizadas no tienen un poder controlador central por lo que el acceso es libre y fomenta la innovación directa. Esto significa, que los desarrolladores pueden crear y experimentar libremente con nuevas aplicaciones (Cerf, 2012). Por ello, las tecnologías centrales se comparten a través de licencias de código abierto, como la plataforma financiera sobre la que se construyó Bitcoin (Nakamoto, 2019).

6. Interoperabilidad: un entorno DeFi permite un mayor desarrollo en la interoperabilidad, ya que, en el sistema centralizado actual, cada institución financiera mantiene su propia plataforma, lo que causa que mover capital de una institución implique a muchas partes y los costes sean altos. Lafourcade y Lomabar-Platet indican que el problema de la interoperabilidad entre diferentes *blockchains* no está plenamente solucionado, ya que según la definición clásica es imposible. Sin embargo, bajo una definición más débil, se confirma que la interoperabilidad es únicamente posible si se crea una *blockchain* “2 en 1” que contenga a ambas (2009). Esto significaría que, con el paso de los años, un ecosistema DeFi tendría amplios beneficios sobre los servicios financieros tradicionales.

7. Transfronterizo: las finanzas tradicionales dependen de una moneda fiduciaria, por lo que siempre están ligadas con una región geográfica. Esta característica de las transacciones a través de redes blockchain permite que las comisiones se cobren independientemente de dónde residan las dos partes implicadas. Por ejemplo, el ahorro que permitiría el *blockchain* sería en transacciones internacionales como el envío de remesas, que suelen costar entre el 7,6%-20% del coste total (Hernandez, 2017).

8. Transparencia: debido a la técnica irreversible de almacenar datos en la *blockchain* y su visibilidad pública, esta tecnología permite crear un nivel único de credibilidad, transparencia y trazabilidad (Jeppsson, & Olsson, 2017). Esto supone una oportunidad para el entorno DeFi ya que cualquier persona puede observar la ejecución de los *smart contracts* y la información financiera que contienen.

9. Automatización de procesos: el uso de *smart contracts* permite la automatización de multitud de tareas y procesos. Según Popescu, a mayor cantidad de procesos automatizados, se conseguirán no solo una mayor eficiencia sino también autonomía. Para mitigar riesgos en la ejecución automatizada de estos contratos, habría que poner medidas que los regularan, lo que podría incrementar los costes. Por ello, el debate de si un ecosistema DeFi reduciría costes sigue estando abierto (2020).

10. Finalidad Consensuada: las transacciones se verifican mediante el consenso de los nodos de la red de *blockchain*, que se ponen de acuerdo en la veracidad de la transacción. Además, las transacciones ya escritas en la red son inmutables y no se pueden modificar. Por ello, existen

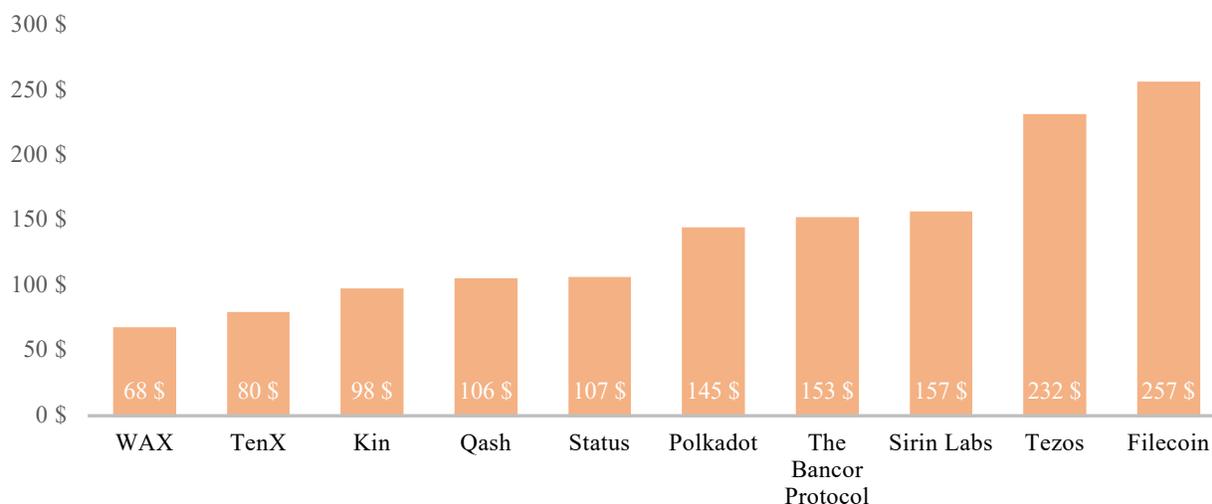
diferentes características a tener en cuenta cuando se desarrollan los algoritmos de consenso, en función de prioridades como rendimiento, seguridad o funcionamiento (Chaudhry & Yousaf, 2018).

2.3 Evolución histórica

El concepto inicial de *smart contract* fue desarrollado en 1994 (Szabo, 1994). Este autor utilizó el ejemplo de una máquina expendedora para describir la idea, en la cual argumentó que muchos acuerdos podrían estar: "integrados en el hardware y software con los que tratamos, de tal manera que el incumplimiento del contrato sea costoso ... para que no se produzca el incumplimiento" (Szabo, 1997). Años más tarde, el protocolo de Bitcoin inició una nueva era de servicios financieros *peer-to-peer* a partir de 2009, pero no fue con la creación de Ethereum hasta que se inició un nuevo recorrido hacia la descentralización financiera. Este proyecto fue la primera *blockchain* capaz de ejecutar *smart contracts*, permitiendo desarrollar aplicaciones financieras complejas sobre su plataforma. Este proyecto fue lanzado por Vitalik Buterin en noviembre de 2013 a través de un *whitepaper* (documento técnico sobre un proyecto de *blockchain*) titulado: "*A Next-Generation Smart Contract and Decentralized Application Form*". Este proyecto permitió la evolución del ecosistema DeFi, ya que consistía en un sistema financiero abierto sin inclusión de entidades financieras tradicionales (Buterin, 2013). Su lanzamiento fue en 2005, y rápidamente tuvo una gran acogida por desarrolladores, los cuales querían construir todo tipo de aplicaciones gracias a la arquitectura de Ethereum. Esta estructura permitía integrar aplicaciones descentralizadas conocidas por su acrónimo anglosajón como *DApps*, en las cuales los acuerdos se aplican mediante código (*smart contracts*), ejecutando transacciones de forma segura y veraz. En diciembre de 2014 se funda la organización MakerDao, conocida como la primera plataforma de préstamos y aplicación DeFi con un uso significativo en la red de Ethereum. Su fundador fue Rune Christensen y la plataforma fue financiada por fondos de *venture capital*, siendo finalmente lanzada en 2017. Su criptomoneda Dai tiene como objetivo mantener su valor lo más cercano al dólar estadounidense, a través de un sistema de *smart contracts* que tiene exige a los usuarios colateral cuando piden préstamos. La criptomoneda Dai es mantenida por aquellos usuarios que poseen el token de gobernanza de MakerDao (MKR), los cuales deciden y votan sobre ciertos parámetros de los contratos inteligentes de la plataforma (Christensen, 2020). En 2017, se produjeron numerosas ofertas públicas de monedas conocidas por sus siglas en inglés como ICOs. Con ello, los desarrolladores pretendían levantar fondos a través de la red de Ethereum, en lugar

de usar los métodos tradicionales. Numerosos proyectos empezaron a recaudar fondos ofreciendo sus propios tokens, intercambiables en plataformas descentralizadas por dinero real, y así financiar sus operaciones. Esta idea de descentralizar la recaudación de fondos era buena, pero, sin embargo, dio lugar a una sobrevaloración de algunos proyectos que levantaban grandes cantidades de dinero con tan solo unas páginas de información en sus *whitepapers*. Alrededor de 3.500 millones de dólares de fondos fueron recaudados por *startups* de *blockchain* en 2017, siendo los diez proyectos DeFi más interesantes y que más fondos recaudaron en sus ICOs, los que se recogen el gráfico 1 (Williams-Grut, 2018):

Gráfico 1. Dinero recaudado (millones de dólares)



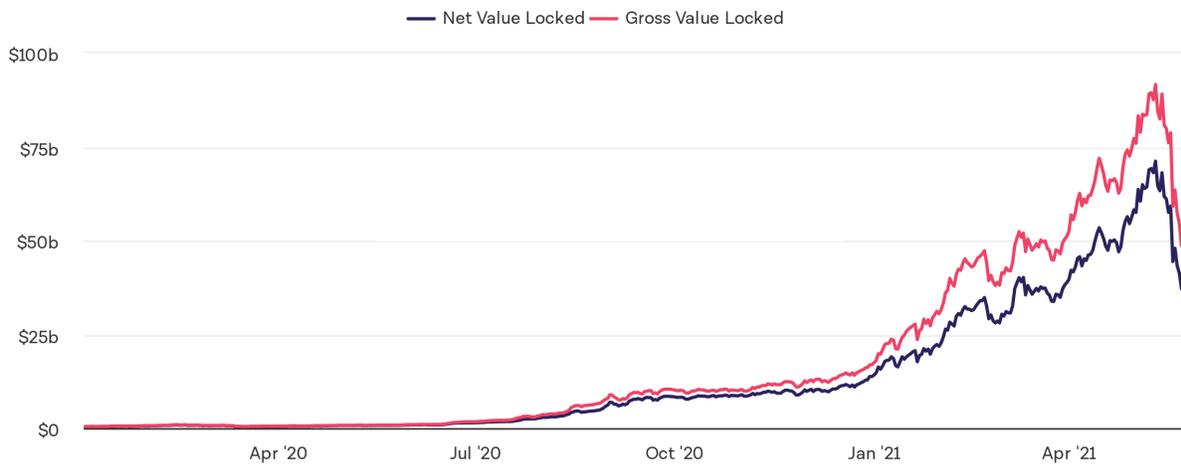
Fuente: Williams-Grut (2018). Elaboración propia

En el 2018, una serie de acontecimientos hizo estallar la burbuja en las valoraciones de las criptomonedas, reduciendo su valor en más del 80% (Panda et al., 2020). Sin embargo, hubo muchos proyectos que se iniciaron en aquella época que ahora están considerados como algunos de los protocolos del ecosistema DeFi: Aave, Polkadot, Ox o Bancor. Después de que terminara la tendencia de las ICOs (ofertas públicas de monedas) y empezara el mercado bajista, el entorno DeFi experimentó un período tranquilo, aunque en verdad empezaron a emerger los principales protocolos que iban a continuar con el desarrollo de la descentralización financiera. El 2 de noviembre de 2018, se publicó la primera versión de Uniswap en la red principal de Ethereum, creado por Hyaden James. Este proyecto es claramente uno de los más relevantes en el entorno descentralizado, gracias a sus fondos de liquidez y creadores de mercado (*market-makers*)

automatizados a través de contratos inteligentes. Los usuarios proporcionan liquidez a la bolsa de intercambio agregando sus tokens a un *smart contract* que otros usuarios pueden comprar y vender, recibiendo un porcentaje de las tarifas de compraventa (Adams, 2018). Entre 2018 y 2020, numerosos proyectos DeFi fueron apareciendo como Compound, REN u Ox principalmente en la red de Ethereum. Esta evolución dio lugar al *boom* del verano DeFi a partir de mayo de 2020, donde el principal catalizador fue el programa de extracción de liquidez de los tokens de gobernanza lanzados por Compound (COMP) que atrajo multitud de usuarios. Este protocolo no sólo es uno de los más llamativos del momento, sino que su modelo de pools de liquidez, recompensas y gobernanza crea un ecosistema de financiación y préstamos. Su objetivo buscar oportunidades para crear *pools* de inversión que ofrezcan préstamos y que no sólo rentabilicen a la plataforma, sino también a los usuarios que aportan la liquidez (Leshner & Hayes, 2019). Al igual que con casi todos los proyectos innovadores que fueron surgiendo alrededor del ecosistema DeFi, el éxito de Compound fue seguido rápidamente por otros equipos que se animaron a lanzar proyectos similares con diferentes modificaciones. Una de las métricas más utilizadas para calcular el crecimiento es el valor total bloqueado de todas las aplicaciones que se encuentran en un determinado protocolo descentralizado, conocido por sus siglas en inglés como *TVL*. El entorno DeFi en general, vió crecer su *TVL* desde los 738 millones de dólares en abril, hasta los 8.380 millones de dólares en septiembre (DeBank, 2021). Este ascenso parabólico no era sostenible en el tiempo, lo que causó un cambio en el sentimiento del mercado a principios de septiembre de 2020. Este giro es conocido como el invierno DeFi, causó una gran caída en el valor de la mayoría de los tokens descentralizados. El mercado tocó fondo a principios de noviembre, con caídas en el valor de más del 70% en algunos protocolos. Después de un ligero rebote, el mercado descentralizado volvió a recuperar su tendencia alcista hasta el final del año. Por ello, el año 2020 fue considerado por muchos como el año DeFi, con más de 11.000 millones de dólares invertidos en protocolos DeFi. (Chochan, 2021). De cara a 2021, el futuro DeFi ha demostrado ser más brillante, y su crecimiento no ha parado de crecer. Se puede comprobar el crecimiento del ecosistema Defi hasta alcanzar un TVL de 102.000 millones de dólares (Anexo II). Los desarrolladores DeFi siguen apostando por la innovación, creando nuevos protocolos con multitud de aplicaciones. Ethereum 2, es la nueva versión que se implementará a lo largo del año que permitiría una mayor escalabilidad, así como la aparición de otras *blockchains* que se explicarán a lo largo de este trabajo. Además, una tendencia que ha visto la luz en este año ha sido la

tokenización de activos tradicionales para crear versiones sintéticas de los mismos e introducirlos en la red de *blockchain*. Esta idea general de tokenización permite que los activos sean más accesibles y las transacciones más eficientes. Estos activos digitales pueden transferirse fácil y rápidamente a cualquier usuario del mundo a través de redes de *blockchain* (Schär, 2021). En el siguiente gráfico se puede ver la evolución del valor bruto y neto bloqueados, una de las métricas más importantes en el entorno DeFi, que muestra el incremento exponencial del valor total de activos descentralizados.

Gráfico 2: Valor Bruto y Valor Neto Bloqueados (miles de millones de dólares)



Fuente: Debank, 2021

2.4 Comparación con las finanzas tradicionales

El sistema financiero tradicional es aquel con el que todo el mundo está familiarizado. Se podría definir como una gran red de empresas dedicadas a diferentes funciones como la inversión, el crédito, la deuda, los mercados monetarios, los préstamos, los seguros y aquellos negocios relacionados con el dinero. Normalmente, este protocolo está muy centralizado y controlado por empresas muy consolidadas y con un ánimo de lucro. Actualmente, los sistemas financieros a nivel mundial operan con dinero fiduciario. De hecho, la palabra *fiat* viene del latín y significa que se haga. El dinero se imprime a través de los bancos centrales sin ningún respaldo real y se presta a las instituciones bancarias. Éstas tienen una gran ventaja ya que reciben altas cantidades de capital

a un interés muy bajo, para luego volver a prestar a sus clientes con intereses más altos y sacar beneficio. La competitividad que ha aparecido con las *fintech* ha supuesto un verdadero golpe para el sistema bancario tradicional, y, sobre todo, algunos expertos indican que ha causado el declive del sector. Según Edwards y Mishkin, las fuerzas económicas han obligado a una rápida adaptación de la innovación tecnológica en las instituciones financieras, causando mayor competitividad en los mercados financieros. A mayor rivalidad, los bancos pierden ventaja en adquirir fondos lo ven reducida su posición dominante. Este suceso, no sólo afectó a la estabilidad y crecimiento de los ingresos del sector, sino que causó la aparición de nuevas empresas disruptivas para desafiar al sistema tradicional (1995). Por otra parte, el ecosistema DeFi como se ha mencionado anteriormente, puede imaginarse como un sistema financiero construido por un grupo de programadores en una red de *blockchain*. Esta red está abierta para todos, facilitando las finanzas a todo el mundo y en cualquier país. La verdadera característica y diferenciación de las finanzas descentralizadas, es establecer la lógica del negocio financiero tradicional bajo contratos inteligentes programables. Estos se ejecutan automáticamente cuando se cumplen los parámetros del código, facilitando y agilizando todo el proceso que conocemos hasta ahora. El principal problema de las finanzas siempre ha sido cómo asegurar y conseguir que los clientes depositen su confianza en las instituciones para que los usuarios puedan depositar su dinero. Por ello, otro factor destacable del entorno DeFi, es la resolución del problema del factor de confianza ya que no necesita de intermediarios. Con los *smart contract* de código abierto que se utilizan en un entorno descentralizado, se permite que los desarrolladores creen aplicaciones financieras con reglas escritas para que se ejecuten continuamente, sin importar lo que suceda. El esfuerzo colectivo que requieren estas plataformas permite que se innove continuamente en el sector, así como avanzar con la disrupción tecnológica en el entorno de *blockchain* (Chen & Bellavitis, 2020).

Capítulo III:
***Blockchain* como**
plataforma
descentralizada

3. ¿QUÉ ES UNA PLATAFORMA *BLOCKCHAIN*?

3.1 Evolución y desarrollo

En el año 1976 se publicó un documento titulado *New Directions in Cryptography* en Estados Unidos, en el cual se discutía el concepto de *Distributed Ledger (DLT)* o Tecnología de Libro Mayor Distribuido. A finales de los años 1980, Haber, criptógrafo y Stornetta, físico, trabajaban juntos como investigadores en Bellcore, en Morristown, Nueva Jersey. Los dos científicos observaron cómo rápidamente la gente iba adoptando la informática personal. Esta dependencia digital les hizo plantearse dos preguntas: si es tan fácil manipular un archivo digital en un ordenador... ¿cómo sabremos qué era verdad sobre el pasado? ¿cómo podemos confiar en lo que sabemos del pasado sin tener que confiar en una autoridad central que lleve el registro? Estas dos cuestiones los llevaron a plantear un problema matemático complejo, ¿se podría construir un sistema de registro fiable de archivos digitales sin un administrador central? Lo que plantearon como solución fue el sistema subyacente a una cadena de *blockchain*, un sistema de registro de sello temporal enlazado de tal manera que no se pueda manipular, y que sea criptográfico y registrador. Los registros marcados en el tiempo están unidos de tal manera que uno no puede agregarse a otro sin interrumpir la cadena entera. Las *ledgers* (es el registro de todas y cada una de las operaciones y transacciones realizadas dentro de una blockchain) están unidas internamente con los bloques de transacciones y luego se distribuyen por la red, permitiendo que la confianza de un *ledger*, se deposite en un algoritmo y no en un administrador central (Whitaker, 2019). Todos estos avances en el campo de la criptografía fueron recogidos por Haber y Stornetta en su proyecto con título “Hot to Time-Stamp a Digital Document” explicando el concepto de la importancia de determinar la fecha y hora de los datos en lugar del medio (Haber & Stornetta, 1990). Otro avance importante fue el reconocimiento del dinero electrónico o divisa digital, que vio la luz a partir del modelo creado por David Chaum. En 1997, Adam Black introdujo el *hascash*, una solución para controlar el *spam* de los correos electrónicos. Esto supuso la creación de dinero llamado “*b-money*” por Wei Dai en una red *peer to peer*. Sin embargo, el verdadero creador del *blockchain* es Satoshi Nakamoto cuando publicó en 2008 su trabajo sobre bitcoin “*Bitcoin: A Peer-to-Peer Electronic Cash System*”. El resumen del trabajo lo definía como un sistema de pago ubicada en una red, y basado en criptografía, capaz de enviar pagos de una parte a otra sin necesidad del consenso de una tercera. Este trabajo solucionaba el problema del doble gasto donde una moneda digital no

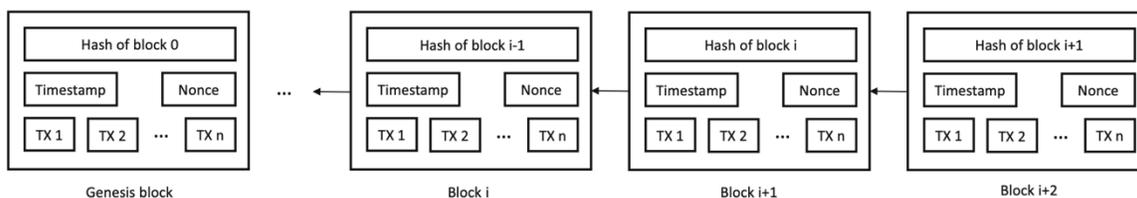
podía ser duplicada y nadie podía gastarla más de una vez. Su programa de código abierto fue lanzado meses después de la presentación de este trabajo y la primera red *blockchain* de bitcoin se inició a principios del 2009 con la creación de los primeros bitcoins (Sarmah, 2018). La principal innovación de Nakamoto fue crear un incentivo financiero para mantener las copias del ledger conectadas, con el desarrollo clave de la minería, es decir, permitir a las personas ganar monedas - los bitcoins – mediante la resolución de puzzles y problemas matemáticos intentando verificar las transacciones de un bloque (Whitaker, 2019). Poco después, Nakamoto lanzó el proyecto para minar ethereum, que marcó el comienzo de una ola posterior de criptomonedas que fue creciendo lentamente durante varios años. En 2014, Vitalik Buterin introdujo el protocolo de Ethereum, la estructura de contratos inteligentes que permitía la tokenización, iniciando así lo que hoy conocemos como la descentralización financiera (Buterin, 2013). Aunque la tecnología blockchain necesite todavía progresar, cabe mencionar que pertenece al ranking de innovaciones tecnológicas sobre las que se construyen estructuras sociales de gran escala. Por ejemplo, algunos de los principales soportes del sistema financiero actual fueron el resultado de proyectos de investigación galardonados con el premio Nobel: Harry Markowitz's y su *Modern Portfolio Theory* (1952), William Sharpe's con su "*Capital Asset Pricing Model*" (1964) y la de Fisher Black's and Myron Scholes, conocida como "*Black-Scholes Options Pricing Model*" (1973) (Whitaker, 2019).

3.2 Funcionamiento de las plataformas *blockchain* y los *smart contracts*

Una cadena de *blockchain* se compone de conjuntos de datos que se componen de una cadena de paquetes de datos (bloques), cada uno de los cuales contiene varias transacciones. Cada bloque sucesivo extiende la cadena de bloques, lo que da como resultado un registro completo del historial de transacciones. La red puede validar bloques utilizando métodos criptográficos. Además, cada bloque contiene una marca de tiempo, el valor hash del bloque anterior (el "padre") y un *nonce*, que es un número entero aleatorio que se utiliza para validar el *hash*. Este concepto protege la integridad de la cadena de bloques hasta el primer bloque (el "bloque génesis"). Debido a que las modificaciones a un bloque en la cadena afectan inmediatamente al valor del hash asociado, los valores hash son únicos y el fraude se puede prevenir con éxito. El bloque se puede agregar a la cadena si la mayoría de los nodos de la red acuerdan mediante un proceso de consenso la legitimidad de las transacciones en el bloque, así como la validez del bloque en sí (Swanson, 2015). A continuación, se puede observar en el gráfico 3, cómo se conectan unos nodos a otros para

consensuar la operación, y se puede observar los elementos principales de una cadena de *blockchain*.

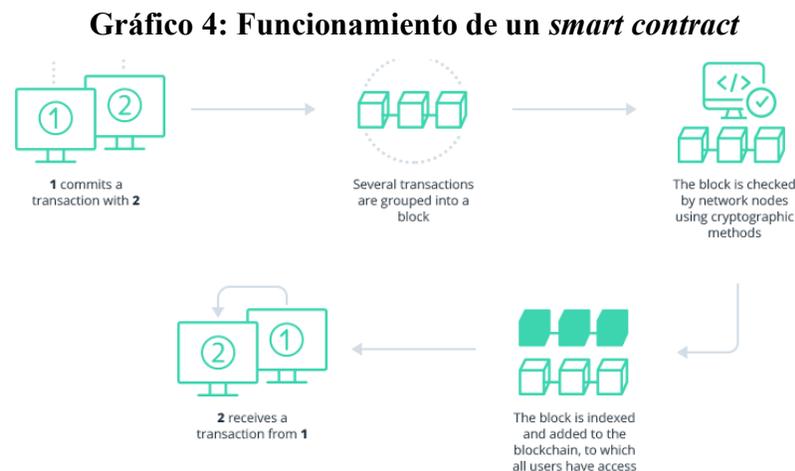
Gráfico 3: Ejemplo de una red de *blockchain*



Fuente: Zhen et al., 2016

Las nuevas transacciones no se agregan automáticamente al *ledger* (libro mayor de la cadena), sino que más bien, el proceso de consenso garantiza que estas transacciones se mantengan en un bloque durante un período de tiempo específico (por ejemplo, 10 minutos en la *blockchain* de Bitcoin) antes de trasladarse al *ledger*. Después de eso, la información en la cadena de bloques ya no se puede modificar. Esto demuestra que el uso de la criptografía permite que todo el mundo, pueda confiar en otros usuarios y transferir diferentes activos *peer-to-peer* a través de internet (Nofer et al., 2017). El desarrollo del *blockchain* en los últimos años permitió dar soporte a otros conceptos ya estudiados en trabajos de investigación. Szabo introdujo el concepto de los *smart contracts*, que combinaban el uso de protocolos de ordenador con interfaces de usuario para ejecutar un contrato (1997). Los contratos inteligentes son flujos de valor que se basan en términos y circunstancias específicos, funcionando de manera similar a los contratos en el mundo real. La única diferencia es que son completamente digitales, lo que implica un pequeño fragmento de código de programación guardado dentro de una cadena de bloques. Hay otros sistemas *blockchain* que pueden usarse para crear contratos inteligentes, pero Ethereum es el más popular (Macrinici, 2018). Esencialmente, los contratos inteligentes son simplemente contenedores de código que encapsulan y replican acuerdos contractuales del mundo real en internet. Un concepto fundamental de los contratos es que constituyen un acuerdo vinculante entre dos o más partes, y cada entidad está obligada a cumplir con su parte. Otro aspecto crítico es que el acuerdo es legalmente ejecutable, normalmente a través de entidades centralizadas. Sin embargo, los contratos inteligentes reemplazan estos intermediarios con la ayuda de la ejecución automática de código, que es distribuido y verificado por los nodos de la red en una red *blockchain* descentralizada

(Swan, 2015). Este tipo de contratos se están volviendo más populares como resultado del uso de redes *blockchain*, ya que se pueden usar más fácilmente mediante el uso de esta tecnología a pesar de que existe desde hace más de 20 años. Esta nueva metodología puede, por ejemplo, reemplazar a abogados y bancos que han estado involucrados en transacciones de compra de activos con base en criterios establecidos (Fairfield, 2014). En el siguiente gráfico se puede ver el funcionamiento de un contrato inteligente, desde que se produce la transacción hasta que se confirma.



Fuente: Oleksiuk, 2021

Existen dos protocolos de consenso para verificar las transacciones, los cuales son el mecanismo que regula de que manera los nodos que unen cada bloque llegan a un acuerdo común para realizarlo e incorporar ese bloque a la cadena de *blockchain*. Este protocolo busca asegurar que el próximo bloque de transacciones agregado a la cadena sea el verdadero, por lo que tiene que poder evitar aquellos peligros que intenten introducir cambios ilegítimos en la cadena de *blockchain*. El primer protocolo fue el *Proof-of-Work* (PoW) o prueba de trabajo. Se diseñó para *blockchains* públicas y fue introducido por Satoshi Nakamoto. En este protocolo, los mineros (aquellas personas que utilizan sus ordenadores para resolver un acertijo criptográfico a través de la capacidad computacional de los equipos), realizan el proceso de intentar resolver ese acertijo criptográfico. Cuanto mayor sea esta capacidad de cómputo (*hashrate*), mayor probabilidad tiene de resolver este acertijo y ganan el derecho a establecer el siguiente bloque en la cadena. El *hashing* es una función que mapea entre una entrada de cualquier longitud a un número de una longitud determinada (256 bits para Bitcoin). El mapa es determinista, pero pequeñas modificaciones en la

entrada provocan cambios arbitrarios en la salida, de modo que reconstruir la entrada es inviable y el número de salida está relacionado de forma única con la entrada dada (Aste, 2016). Al continuar con la cadena de *blockchain* introduciendo el siguiente bloque, el minero recibe unos Bitcoins como recompensa, más del 90% de las *blockchains* actuales utilizan este método (Nakamoto, 2019).

El otro protocolo de consenso es el *Proof of Stake* o *prueba de participación*. Este protocolo es mucho más sencillo, incrementa la velocidad de las transacciones y reduce el consumo de energía. El algoritmo utiliza un proceso de elección pseudoaleatorio para seleccionar un nodo que será el validador del siguiente bloque, estos nodos son responsables de comprobar y confirmar los bloques que no crean. Se basan en una combinación de factores que podrían incluir la edad de la apuesta, la aleatoriedad y la riqueza del nodo. (Larimer, 2013) Estos validadores deben tener una participación suficiente, por ejemplo, en el caso de Ethereum los usuarios deberán dejar bloqueadas en depósito (*stake*) 32 Ethereum para convertirse en validadores. La apuesta de un usuario también se utiliza como forma de incentivar el buen comportamiento de los validadores. El tamaño de la cantidad bloqueada de Ethereum (ETH) determina las posibilidades de que un nodo sea seleccionado como el siguiente validador para añadir el siguiente bloque, pero también cuanto mayor sea la cantidad bloqueada, mayores serán las posibilidades. Por ejemplo, un usuario puede perder toda su participación por colusión deliberada, es decir, si atestigüas bloques maliciosos, pierdes la capacidad de validar. A diferencia del *Proof of Work*, los validadores no necesitan utilizar cantidades significativas de potencia computacional (*hashrate*) porque se seleccionan al azar y no compiten entre ellos. No necesitan “minar” bloques; solo tienen que crear bloques cuando son elegidos y validar los bloques propuestos cuando no los crean, usando generalmente las tasas de las transacciones como recompensa (Buterin, 2013).

3.3 Plataformas Blockchain

El ecosistema descentralizado ha tenido una evolución exponencial en los últimos años, sin embargo, sus plataformas y productos siguen siendo difíciles de entender, por lo que se va a realizar una descripción de las principales plataformas sobre las que se desarrolla la descentralización financiera. En primer lugar y la más conocida es la red de Ethereum, la cual se ha convertido en la *blockchain* elegida por la mayoría de los desarrolladores de aplicaciones descentralizadas. Ethereum tiene, con diferencia, la mayor comunidad de desarrolladores,

superando incluso a la de Bitcoin, ya que está mucho más orientada a la tecnología y a la inclusión de nuevos proyectos. Sin embargo, recientemente han surgido más y más proyectos prometedores que podrían robarle el liderazgo. Como ya se ha mencionado anteriormente, la base de la descentralización financiera es la posibilidad de ejecutar contratos inteligentes sobre la red de *blockchain*. Por ello, la tecnología de los contratos inteligentes está remodelando los procesos industriales y empresariales convencionales. Estos contratos inteligentes están integrados en plataformas *blockchain* que permiten se apliquen automáticamente los términos de un contrato sin la intervención de un tercero de confianza. Por ello, la explicación de para qué sirven estas plataformas de contratos inteligentes es que ofrecen a los desarrolladores interfaces sencillas para crear aplicaciones descentralizadas. Actualmente existen multitud de plataformas *blockchain* que pueden soportar contratos inteligentes. En este documento vamos a desarrollar tres de las principales: Ethereum, Cardano y Polkadot.

3.3.1 Ethereum

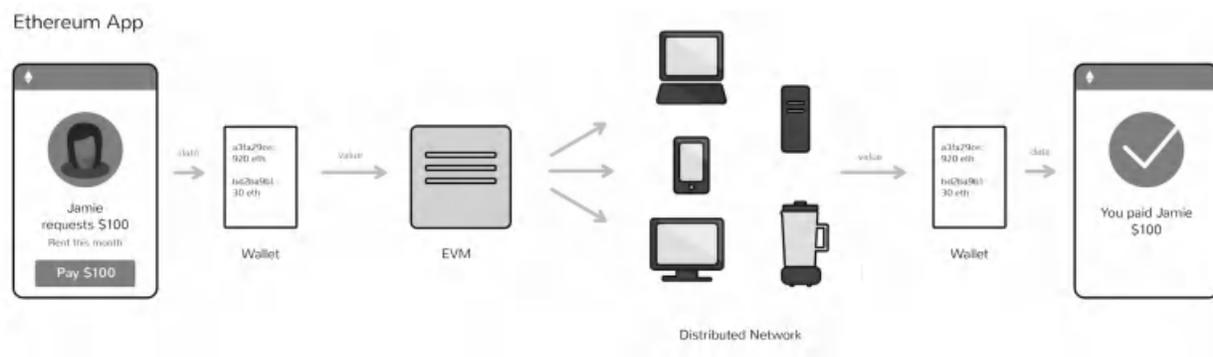
Es la segunda plataforma por capitalización de mercado, después de Bitcoin. Tiene características similares a éste, como la creación y desarrollo de una red pública de *blockchain* y el uso del mismo tipo de protocolo de consenso (*Proof of Work*). Ethereum representa una cadena de *blockchain* con un lenguaje completo que proporciona una capa abstracta, donde cualquiera puede crear sus reglas de propiedad, formatos de transacciones y funciones de la transición mediante la participación de los contratos inteligentes. El intercambio de valor es el principal uso de la tecnología *blockchain*, generalmente a través de su token nativo conocido como *ether*. Muchos de los desarrolladores están trabajando en la criptomoneda por su potencial a largo plazo y la visión de poder utilizar Ethereum para dar a los usuarios un mayor control de sus finanzas y datos en la web. Por ello, los desarrolladores pueden construir aplicaciones sin líderes, es decir, que los datos del usuario no puedan ser manipulados por los creadores del servicio. Ethereum fue propuesto en 2013 por su desarrollador Vitalik Buterin, quien, a los 19 años fue uno de los pioneros en expandir la tecnología *blockchain* sobre la que se creó el Bitcoin, para darle más casos de uso que transacciones monetarias. Los creadores de esta plataforma tenían como objetivo eliminar las terceras partes en internet como los que almacenan datos, transfieren hipotecas o llevan el control de diferentes instrumentos financieros. Finalmente, la plataforma vio la luz en 2015, convirtiendo la idea original en un proyecto real y funcional. La plataforma ha visto crecer exponencialmente tanto su

capitalización bursátil como el valor total de los activos en la red de Ethereum, llegando a una capitalización bursátil de más de 290.000 millones de dólares (Anexo I).

La red de Ethereum está compuesta de cuentas donde almacenar las criptomonedas, y cada cuenta tiene una dirección de 20 *bytes* y unas transiciones de estado. La red admite dos tipos de cuentas: las de propiedad externa (controladas por claves privadas) y las de contrato (controladas por códigos de contrato). Una cuenta de Ethereum se compone de cuatro campos: *nonce*, saldo *ether* (moneda utilizada en la red de Ethereum), *hash* y raíz de almacenamiento [*nonce*, saldo de *ether*, *hash* del código de contrato y la raíz de almacenamiento]. El *nonce* refleja el número de transacciones transmitidas desde una determinada dirección y se utiliza para garantizar que cada transacción sólo se procesa una vez. El saldo de Ethereum de una dirección es la cantidad de Wei que posee (Wei es la fracción más baja de Ethereum, siendo un Ethereum, igual a 10^{18} Wei). En cuanto al hash del código, éste es un identificador del almacenamiento del contrato, así como la raíz de almacenamiento es el identificador del almacenamiento del contrato]. La realización de las transacciones en la red es esencial, por ello podría definirse como el envío de un paquete de datos firmado desde una cuenta de propiedad externa. Cada transacción contiene el destinatario del mensaje, una firma que identifica al remitente, la cantidad de Ethereum que se va a entregar, un campo de datos opcional y los valores *startgas* y *gasprice*. Como cada transacción requiere un cierto número de cálculos, el campo *startgas* indica el número máximo de pasos de cálculo que puede tomar la transacción. Dado que los mineros reciben una mayor compensación si ejecutan una transacción con un *gasprice* más alto, el emisor debe seleccionar cuidadosamente los requisitos del *gasprice* (Vujičić,2018). Cada acción en una aplicación sobre la red de Ethereum, incluso tan pequeña como la publicación de un mensaje en una red de *micro-blogging*, cuesta una pequeña cantidad de *ether*. Con estas cuotas, los usuarios pueden acceder a una gran variedad de aplicaciones descentralizadas en la plataforma, pero no son gratuitas debido a que los recursos informáticos de Ethereum son limitados. A mayor número de usuarios, las tasas crecen debido a un mayor uso de la red. Por último, la plataforma de Ethereum permite emitir otras criptomonedas basadas en contratos inteligentes que implementan el estándar de creación de tokens conocido como ERC-20, el cual establece que tiene que consistir en 6 funciones y 2 eventos que describan la totalidad de la cuenta (transferencia y aprobación de la transacción) (Vitalik, 2013).

Para desplegar eficazmente una solución escalable, Ethereum está a punto de realizar una importante actualización de su protocolo para fundar Ethereum 2.0. Esta nueva versión no sólo aumentará la escalabilidad, sino que creará una arquitectura flexible para facilitar las demandas de la evolución de la industria. Ethereum 2.0 se basa en la noción de la fragmentación, donde la cadena de blockchain se divide en fragmentos y los subconjuntos de la cadena de bloques funcionarán de manera independiente procesando sus propias transacciones, para aportar mayor capacidad de procesamiento. También existirá una cadena principal llamada *Beacon Chain*, la cual se encarga de controlar el funcionamiento de la red y que todos operen de manera responsable (Cortes-Goicoechea, 2020). Cuando se complete la actualización, Ethereum cambiará de protocolo de consenso, y pasará a un consenso mediante *Proof of Stake* (PoS). Este cambio eliminará la minería y pasará al sistema de validadores, como ya se ha explicado anteriormente. Como se ha explicado anteriormente, el gráfico 5 propone un esquema general del funcionamiento de las transacciones en Ethereum. Un usuario envía una cantidad de dinero a través de su cartera virtual, que se incorpora a la blockchain tras ser confirmada por la *Ethereum Virtual Machine* (EVM). Esta *EVM* no es más que una maquina virtual que hace las funciones de ordenador y convierte los contratos inteligentes en instrucciones interpretables por el ordenador. Finalmente, el otro usuario recibe la cantidad propuesta de *ether*, tras consensuarse y aprobarse la transacción en la red de *blockchain*.

Gráfico 5: Funcionamiento de una aplicación en Ethereum



Fuente: Kuznetsov, 2017

3.3.2 Cardano

En segundo lugar, tenemos el ecosistema conocido como Cardano, el cual tiene su propia criptomoneda llamada ADA. Cardano es una plataforma *blockchain* basada en un protocolo de consenso de tipo Proof-of-Stake (PoS) de tercera generación llamado Ouroboros, siendo la primera que evoluciona desde una filosofía científica y con un enfoque impulsado por la investigación, garantizando un modelo único en el ecosistema *blockchain* (Kyayias, 2017). El equipo encargado de desarrollar esta plataforma es global, y está compuesto por destacados académicos e ingenieros de la comunidad criptográfica. La premisa de este proyecto es construir sobre la tecnología que soporta Ethereum, pero pretende mejorar la plataforma y los contratos inteligentes priorizando la seguridad, flexibilidad y escalabilidad. Su nacimiento se remonta al 2015, dando lugar a la creación de una red de *blockchain* de tercera generación, Bitcoin conforma la primera y Ethereum la segunda generación. Fue establecida por la firma de desarrollo de *blockchain* IOHK (Input Output Hong Kong) y liderado por su CEO Charles Hoskinson, co-fundador Ethereum y BitShares. Las principales ventajas en comparación con otras plataformas de *smart contracts*, es que está orientada hacia la investigación, contando con un equipo global de I + D. Cardano no es sólo una criptomoneda, sino que es una plataforma que puede ejecutar potencialmente aplicaciones financieras. Por ello, al comprar ADA, los inversores se benefician de dos aspectos del proyecto: El primero es que ADA es una criptomoneda tecnológica con un alto potencial, y en segundo lugar, el valor del sistema Cardano, es la suma de todos los proyectos que puedan utilizar su *blockchain* como plataforma (Aydinli, 2019). La blockchain de Cardano está separada en dos capas, la Capa de Liquidación de Cardano (CSL) y la Capa Computacional de Cardano (CCL), que convierte a Cardano en una plataforma con mayor potencial de desarrollo en el futuro que otros ecosistemas de contratos inteligentes. Por ejemplo, Ethereum ejecuta una arquitectura de una sola capa, lo que le produce una alta congestión en la red, lentitud en las transacciones y tasas por transacción altas. El funcionamiento de la red de Cardano tiene que ver con su infraestructura técnica que combina los diferentes nodos de la red, y sus interacciones relativas para formar un sistema unificado. Consiste en una colección de nodos (son los validadores y distribuidores de las transacciones que ocurren en la red de *blockchain*), que se comunican entre sí a través de un conjunto de mini-protocolos para permitir la comunicación entre los diferentes nodos (Hoskinson, 2017). Los *hard forks* son cambios importantes en el código fuente de una red de *blockchain* que conllevan cambios significativos, ya que anulan el protocolo anterior. La última actualización *hard forks* de Cardano

en mayo permitirá llevar la red a una nueva fase, llevando la red de Cardano a una nueva era conocida como fase Goguen. Esta fase permitirá a desarrolladores y creadores crear tokens customizados en la red, así como una mayor escalabilidad y aceptación de esta red en el ecosistema descentralizado (DeFi). La actualización promete eliminar las altas comisiones de la red, y crear una plataforma de contratos inteligentes que ofrezca características más avanzadas que cualquier protocolo desarrollado anteriormente. Esta actualización permitirá crear una plataforma estable y segura para la creación de aplicaciones descentralizadas (dApps) a nivel global.

3.3.3 Polkadot

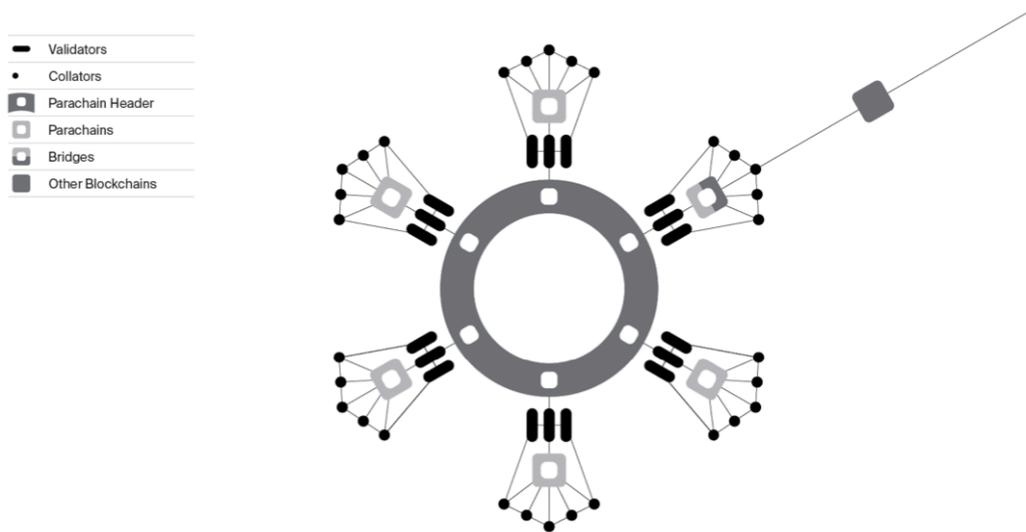
Otro de los proyectos que más atención ha logrado en el último año es Polkadot y su criptomoneda conocida como DOT. El fundador de este proyecto es Gavin Wood, uno de los desarrolladores principales de Ethereum que se separó para iniciar su propia trayectoria. En 2016, anunció la primera versión de su proyecto a través de un *whitepaper*. Este proyecto se puede definir como una multi-cadena heterogénea que se diferencia de las implementaciones anteriores en las redes *blockchain*. Éstas están centradas en crear una única red de *blockchain* con diferentes grados de generalidad en función de las aplicaciones potenciales que se puedan construir sobre ella. Sin embargo, Polkadot proporciona una cadena de transmisión como base para alojar multitud de estructuras de datos a nivel global. En otras palabras, la red de Polkadot puede considerarse como un conjunto de cadenas independientes (Ethereum, Cardano o Bitcoin) que procesan datos como en una cadena de transmisión. Además, su funcionamiento independiente le permite crear cadenas de *blockchain* para que se puedan implementar aplicaciones descentralizadas (dApps) y tokens sobre la red. Hay una característica esencial de Polkadot que se conoce como *sharding*, y consiste en la división de la cadena principal y la red, en varias subcadenas y subredes adjuntas a la misma. Estas estructuras son conocidas como paralelas o *parachains*, las cuales tienen un historial propio (su propia *blockchain*) y contiene una existencia de *tokens*, contratos inteligentes y nodos validadores. Por otra parte, existe la *Relay chain*, o cadena principal de Polkadot. Esta organización recoge la unión del historial de todas las redes de *blockchain* paralelas (*parachains*) y permite que se puedan ejecutar contratos inteligentes en paralelo y alcanzar una gran escalabilidad. Además, esta funcionalidad crea la posibilidad de crear puentes con otras blockchains (Ethereum) y servir de enlace para realizar operaciones conjuntamente. En su naturaleza criptográfica, Polkadot no ofrece soporte para albergar aplicaciones descentralizadas en su red, pero sus *parachains* son extensibles y modulares, por lo que tienen la capacidad de crear capas de abstracción y ejecutar

contratos inteligentes. La filosofía de esta plataforma es proporcionar una base sobre la que se puedan implementar otros protocolos de consenso y redes de blockchain, en una red mucho más segura. Adicionalmente, se pueden crear *parachains* que permiten la capacidad de desarrollar contratos inteligentes y ejecutarlos en la misma red, lo que facilita que el resto del sistema funcione normal evitando lentitud y colapsos generales (Wood, 2016). Para facilitar su funcionamiento, Polkadot ha creado esta nueva red con cuatro elementos principales.

- En primer lugar, en su red se encuentran los nodos “validadores”, que se encargan de verificar, validar y dar información sobre la red.
- En segundo lugar, hay un tipo especial de nodos llamados “nominadores”, los cuales se encargan de crear un vínculo seguro entre los validadores y el completo funcionamiento de la red de Polkadot.
- En tercer lugar, existen los nodos “clasificadores” que ayudan a los validadores a mantener actualizado el historial completo de las *parachains* a las que son asignadas. Mantienen toda la información necesaria para crear nuevos bloques en estas cadenas paralela, que luego será recopilada en el historial completo de la red de Polkadot.
- Por último, la estructura es mantenida por los nodos “pescadores”, que son nodos que buscan transacciones duplicadas u operaciones maliciosas dentro de la red a cambio de una recompensa (Burdges et al., 2020). Estas cuatro piezas combinadas permiten el funcionamiento de todo el sistema Polkadot, desde la generación y verificación hasta la validación y emisión de bloques dentro de las redes del ecosistema.

En el siguiente gráfico podemos encontrar un esquema de la red de Polkadot, en la cual se observa la estructura principal de la *Relay chain* y sus *parachains* dependientes e interconectadas entre sí.

Gráfico 6: Arquitectura de una red principal con sus respectivas blockchain paralelas



Fuente: Burdges et al., 2020

El protocolo de consenso que utiliza la red para establecer las transacciones se denomina *Nominated Proof of Stake* (NPoS), una versión particular del protocolo *Proof of Stake* (PoS). Su necesidad de mantener un constante número de validadores en función del número de *parachains*, permite que sea mucho más eficiente que un protocolo de *Proof of Work* (PoW) y más seguro que las formas convencionales de *Proof of Stake* (Ceballos & Stewart, 2020).

**Capítulo IV:
Casos de uso y
aplicaciones de un
ecosistema
descentralizado**

4. APLICACIONES DE UN ECOSISTEMA DESCENTRALIZADO

4.1 DeFi vs *Fintech*

Actualmente se puede clasificar a las finanzas en tres modelos diferentes con un objetivo común, ofrecer herramientas financieras para ayudar a las personas a gestionar sus finanzas e inversiones. Sin embargo, difieren mucho en la forma en cómo consiguen sus objetivos. Estos tres modelos de finanzas son las finanzas tradicionales, las *fintech* y por último las finanzas descentralizadas (DeFi). Las finanzas tradicionales son aquellas empresas que existen el sistema financiero actual, por lo que este trabajo se va a centrar en las diferencias entre las *fintech* y las aplicaciones descentralizadas (DeFi). En primer lugar, las *fintech* tratan de establecer un nuevo sistema de finanzas digitales que alcance más rápidamente a una la población y con un coste menor. La digitalización ha impactado fuertemente a la industria de servicios financieros, donde predominan como elementos clave la gestión de la información y la automatización de procesos para alcanzar la eficiencia. La evolución de las tecnologías financieras ha demostrado el enfoque general que tienen, desde relaciones empresa a cliente (B2C), de cliente a cliente (C2C) y de empresa a empresa (B2B) (Puschmann, 2017). Multitud de soluciones tecnológicas propuestas por *start-ups* del mundo *fintech* han sido adaptadas por grandes bancos e instituciones para acelerar su digitalización. Según Frame y White, el enfoque de innovación se basa en tres aspectos diferentes: el objetivo de la innovación, el nivel de innovación, y su enfoque (2014). Sin embargo, la aparición del Bitcoin, la llegada de Ethereum y todo el ecosistema descentralizado (DeFi) ha supuesto un desafío para el futuro de la innovación financiera. Para entender mejor en qué se diferencia una *fintech* de un proyecto descentralizado (DeFi), se pretende a continuación enumerar una lista con las diferencias.

- Una *fintech* es una entidad centralizada construida sobre un *software* y con un enfoque y desarrollo controlados. Sin embargo, una aplicación del ecosistema DeFi, está lanzada sobre una red de *blockchain* descentralizada.
- Los contratos en una *fintech* siguen el curso legal actual, mientras que, en un entorno descentralizado, el motor son los contratos inteligentes.
- En las *fintech* existen intermediarios entre el usuario y la empresa, creando una cadena burocrática en la toma de decisiones. En cambio, la DeFi no cuenta con una cadena ya que

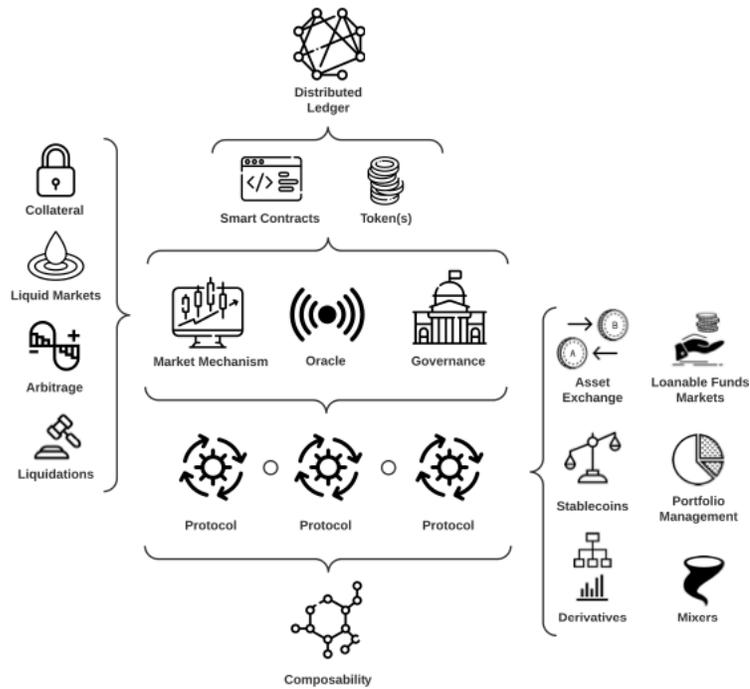
la decisión está en manos de los dos usuarios implicados, a través del protocolo de consenso.

- Las *fintech* usan instituciones bancarias y estructuras financieras tradicionales para ofrecer sus productos. El entorno descentralizado dispone de mayor libertad financiera ya que sólo necesitas una cartera digital para almacenar tus criptomonedas (Pep., 2021).

4.2 Casos de uso de la descentralización financiera

Los protocolos que existen en el ecosistema descentralizado DeFi, están categorizados según el tipo de operación que realizan. Por ello, en el gráfico 7 se pueden ver un esquema general de los diferentes tipos de aplicaciones y casos de uso que existen en un ecosistema descentralizado, que se explicarán más en detalle a continuación.

Gráfico 7: Visión general conceptual de los diferentes tipos de dApps



Fuente: Werner et al., 2021

4.2.1 Intercambio de activos en la red de blockchain

El primer caso de uso de protocolos descentralizados (DeFi) son las plataformas de intercambio descentralizadas conocidas como *decentralized exchanges* (DEX). Estos protocolos facilitan el intercambio sin custodia de activos digitales en la red de *blockchain*. No sólo no tienen la custodia de los activos, sino que liquidan todas las operaciones en la red de *blockchain*, garantizando la verificabilidad pública de todas las transacciones. Actualmente existen más de 109 plataformas de intercambio descentralizado y con un volumen medio de *trading* diario de 8 billones de dólares como se observa en la siguiente tabla.

Volumen de trading 24h (DEX)	Dominio del volumen (DeFi) vs Global	Visitas mensuales (DEX)
8.028.384.104 \$	4.5%	66.432.899

Fuente: CoinGecko, 8 de junio de 2021. Elaboración propia

También existen otras aplicaciones de intercambio de activos digitales centralizadas (existen 365) como Coinbase, Binance o Kraken, pero estas no están consideradas en el entorno DeFi debido a que carecen de una naturaleza descentralizada (CoinGecko, 2021). Existen varias generaciones de plataformas de intercambio descentralizadas, siendo la primera las plataformas de intercambio basadas en libros de órdenes. Similarmente a las bolsas tradicionales, los libros de órdenes recopilan un registro de todas las órdenes de compra y venta para un determinado activo, por lo que el precio vigente del mercado se ajusta con la diferencia de los precios de compra y venta. La siguiente generación de plataformas descentralizadas utiliza protocolos de bolsas de liquidez para determinar el precio de los activos digitales. Son de naturaleza *peer-to-peer* ya que estas plataformas ejecutan las órdenes directamente entre las carteras de los usuarios, en un proceso denominado *swap*. En esta categoría se clasifican por el valor total de los activos mantenidos en los contratos inteligentes de la plataforma o *total value locked* (TVL). Las principales plataformas son Mdex, Uniswap, PancakeSwap y Sushiswap (Lindsay et al., 2019).

4.2.2 Mercado de préstamos (PLFs) y pagos descentralizados

El préstamo y el endeudamiento de activos digital ocurre en la red de *blockchain* a través de protocolos de préstamos con contratos inteligentes (PLFs). Un agente puede pedir prestado directamente contra las reservas de un contrato inteligente si el mercado de ese token es suficientemente líquido. El coste del préstamo se determina por el tipo de interés que se cobra al

prestatario, determinado por el modelo de tipos de interés que tiene el mercado seleccionado. Suele haber dos tipos de préstamos: préstamos con sobre garantía y préstamos *flash*. En el primero, el prestatario deposita una garantía para cubrir el valor de la deuda, y que el valor de la garantía supere a la deuda. Esta colateralización asegura que, si el valor de la garantía en relación con la deuda cae, habría suficiente garantía para cubrirla. El segundo tipo son los préstamos *flash*, los cuales no requieren de garantía, pero requieren que el prestatario devuelva la cantidad total más los intereses al final de la misma transacción (Werner et al., 2021). MakerDAO es la principal aplicación para sistema de préstamos colateralizados, además de otros proyectos como Compound Finance, Aave y Dharma. Compound se parece a un tipo de fondo del mercado monetario, en el que ganas intereses con tus criptomonedas, mientras que Dharma te permite suscribir una deuda para obtener rendimientos de tu inversión. También hay aplicaciones descentralizadas de pagos como Flexa, que ofrece transacciones 100% seguras y evita cualquier tipo de fraude porque no necesita ninguna información privada y confidencial del cliente.

4.2.3 Criptomonedas estables

Estas monedas son criptoactivos que pretenden tener un precio estable en relación con una moneda objetivo, normalmente el dólar. Cabe mencionar que, por ejemplo, la criptomoneda denominada *USDT* no es considerada una moneda descentralizada porque utiliza terceros de confianza para operar. Hay una docena de criptomonedas estables, pero Dai creada por MakerDAO es la moneda más destacada, y cuenta con una capitalización de 8.200 millones de dólares (Defipulse, 2021). Los componentes principales son el colateral (almacén de valor principal de una criptomoneda estable), que puede ser *ether*. Luego están los agentes que desempeñan funciones como la absorción del riesgo, la gobernanza (mecanismo de parámetros que gobiernan el protocolo), emisión (protocolo que regula la emisión de monedas) y los oráculos (mecanismo para importar datos externos a la red de *blockchain*).

4.2.4 Yield Farming

Para los proveedores de liquidez que buscan maximizar los retornos, se pueden automatizar estos contratos en la red de *blockchain* a través de protocolos de contratos inteligentes, que sirven como fondos de inversión descentralizados. El funcionamiento de este proceso consiste en depositar los tokens en un contrato inteligente y bloquear esas criptomonedas para que generen intereses, así el rendimiento se genera a partir de estos intereses y recompensas de tokens. Algunos de los

protocolos más conocidos son Yearn Finance (es un protocolo que facilita el acceso de estrategias de *yield farming* y *liquidity mining*) (Rapoza, 2021).

4.2.5 Predicción de mercados

Los mercados de predicción son mercados bursátiles creados con el fin de negociar el resultado de determinados acontecimientos, por lo que los precios pueden indicar lo que los usuarios piensan y por ello, la probabilidad de que ocurra. El contrato de mercado es una opción binaria que se negocia entre 0 y 1 y expirará al precio de 0 o 100%. Por ejemplo, Augur es una plataforma descentralizada de predicción de mercados, que permite crear una predicción de mercado de cualquiera evento del mundo real. Utiliza un token ERC20 nativo (*REP*) para comerciar, y disputar los resultados del mercado o comprar tokens de participación, canjeables por el Ethereum recopilado inicialmente. Los usuarios comercian con el resultado de una determinada predicción, comprando y vendiendo las acciones en el mercado del evento. Finalmente, los usuarios con las acciones del resultado ganador pueden liquidar los contratos de Augur o vender sus acciones a otros usuarios (Peterson & Krug, 2016).

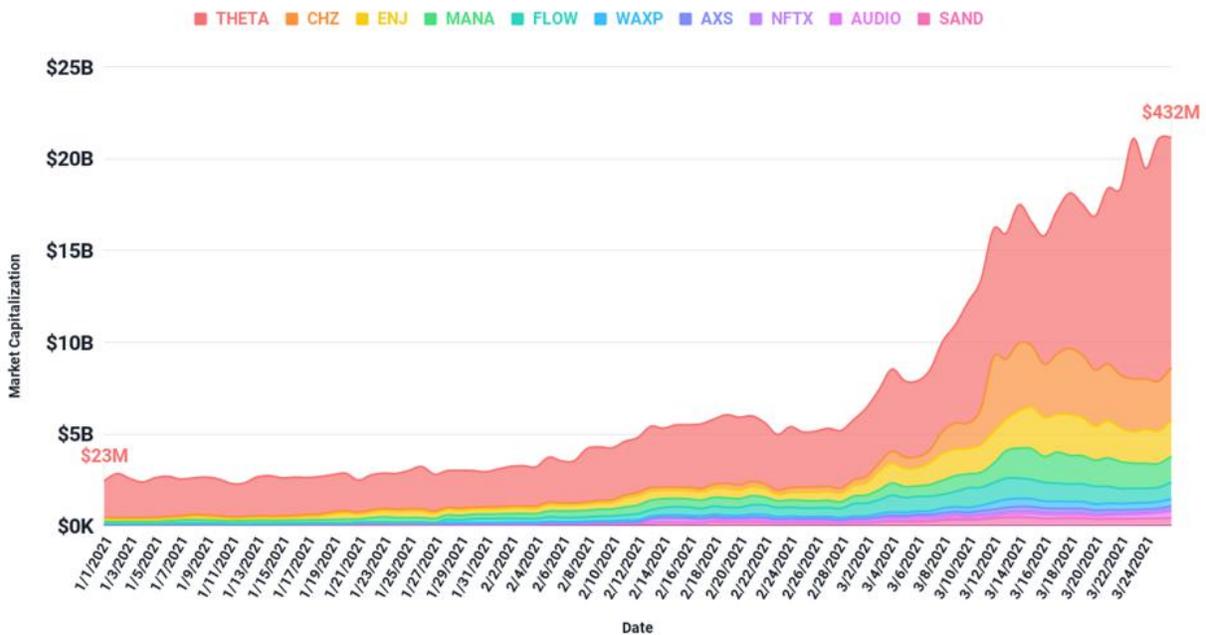
4.2.6 Servicios de custodia (*E-wallets*)

La gestión de activos o servicios de custodia es un sector que está en alza. Se trata de aplicaciones digitales sobre la red de *blockchain* que custodian activos digitales, para permitir poner el dinero de los usuarios en contratos inteligentes y gestionar diferentes criptomonedas. Las aplicaciones como MetaMask permiten crear una cuenta de uso en redes *blockchain* como Ethereum, manteniendo su acceso privado a través de unas contraseñas que el usuario posee. Permiten cambiar entre diferentes redes de *blockchain* para tener acceso a varias y reflejar los balances correctos de cada red de *blockchain* (Lee, 2019).

4.2.6 Tokens No Fungibles (NFTs)

Existe una categoría de activos virtuales basados en *blockchain* conocido como tokens no fungibles que han generado gran interés entre los inversores y son descritos como el futuro del arte digital. A efectos de definición, un token no fungible puede verse como una unidad de información digital (token) que se almacena en una red de *blockchain* y no es intrínsecamente intercambiable con otros activos digitales. Estos tokens adquieren valor debido a la escasez. Los NFTs son óptimos para su uso en aplicaciones descentralizadas (dApps) para crear y permitir la creación de artículos digitales únicos para coleccionar. Los NFTs se pueden negociar en plataformas de intercambio, siendo cada uno único y con un precio determinado (Chochan, 2021). A finales de marzo, el valor de mercado había crecido en más de 1.785%, con precios de venta de algunos de los NFTs más reconocidos de alrededor de los 70 millones de dólares (Young, 2021). En el siguiente gráfico se puede comprobar el aumento de la capitalización de los NFTs durante el año 2021.

Gráfico 8: Capitalización de mercado de los tokens no fungibles (NFTs)



Fuente: Young, 2021

4.3 Análisis de las principales aplicaciones descentralizadas (dApps)

Aunque ya se han destacado algunos proyectos según la categoría a la que pertenecen, en esta parte se pretende estudiar las seis aplicaciones descentralizadas (DeFi) que actualmente lideran el mercado, para ver en qué consisten y conocer cómo han ido desarrollándose a lo largo de los años: Uniswap, Maker, Aave, Compound, InstadApp y Flexa.

4.3.1 Uniswap

Es la principal plataforma descentralizada para intercambios de criptomonedas digitales, con más de un 14,5% de dominio sobre todo el ecosistema descentralizado (Coingecko, 2021). Es un protocolo de *trading* descentralizado que ejecuta una serie de contratos inteligentes en la *blockchain* de Ethereum, garantizando liquidez para millones de usuarios y cientos de aplicaciones establecidas sobre la red *blockchain* de Ethereum. En realidad, es una plataforma creadora de mercado automatizada (AMM) que reúne la liquidez necesaria para ponerla a disposición de los operadores según un algoritmo. Su tercera versión introduce numerosos cambios como incorporar más *pools* de liquidez a cada par de criptomonedas y mejorar el control sobre el rango de precios, aumentando la liquidez total de la plataforma. También dispone de comisiones más flexibles y un protocolo de gobernanza más flexibles. Su token de gobernanza es conocido como (UNI), y permite la propiedad compartida de la comunidad de Uniswap, así como participar en el sistema de gobernanza que guíe la plataforma en el futuro (Adams, 2018).

4.3.2 Maker

Es el protocolo encargado de la criptomoneda estable (DAI), que tienen una naturaleza descentralizada y respaldada por activos colaterales para tener un valor anclado al dólar estadounidense. Es un proyecto de código abierto basado en la red de *blockchain* de Ethereum y que consta de un token de gobernanza llamado MKR, por el cual los usuarios que poseen este token gestionan el protocolo Maker y los riesgos de DAI para garantizar su valor. El protocolo Maker permite crear DAI y es una de las aplicaciones financieras descentralizadas más grandes de la red de Ethereum. La característica principal de DAI es que evita la volatilidad de su precio y por ello se ha convertido en una pieza esencial de muchos proyectos descentralizados sobre Ethereum. Es una reserva de valor, que puede utilizarse como un medio de intercambio descentralizado y como unidad de cuenta, además de mantener su valor por los activos que guarda como colateral, y basados en Ethereum que se depositan en el protocolo Maker. (Bogoni, 2019)

4.3.3 Aave

Aave es un protocolo de liquidez de código abierto y no custodiado para ganar intereses sobre los ahorros y el préstamo de activos. Los precios dentro de la plataforma de Aave se definen con un algoritmo en función de la demanda y oferta de los activos, siendo como Uniswap, un mercado automatizado de activos (AMM). Pretende que sus usuarios puedan invertir dinero en *pools* para crear liquidez y crear una plataforma global capaz de ofrecer préstamos con diferentes colaterales y políticas de funcionamiento. Su carácter descentralizado y la seguridad de la plataforma, la posicionan como una aplicación descentralizada (dApp) con mucho potencial para el futuro (Meegan, 2010). Como *ether* no es compatible con el token estándar ERC-20, ya que éste se definió a posteriori, *ether* no se puede comerciar directamente en plataformas descentralizada y para lograrlo se transforma el *ether* en un token ERC-20 denominado wETH.

4.3.4 Compound

Compound es una aplicación descentralizada de blockchain basado en Ethereum que establece mercados monetarios, los cuales son grupos de tokens con diferentes tipos de interés derivados de un algoritmo, que establece los precios en función de la oferta y la demanda. Los usuarios interactúan directamente con el protocolo de una forma descentralizada, cobrando o pagando (según sea proveedor o prestatario) un determinado tipo de interés flotante, sin tener que negociar ningún término, interés o garantía. Tiene un balance transparente y que es público para todos, además posee un registro de las transacciones y de todo el histórico de tipos de interés. Aplicaciones descentralizadas o plataformas con tokens pueden utilizar el protocolo Compound para generar una fuente de monetización y rendimientos incrementales con sus saldos (Leshner, 2019).

4.3.5 InstaDApp

Esta aplicación es un proyecto interesante desarrollado sobre la *blockchain* de Ethereum, que da acceso a actividades de gestión de activos y conecta varios protocolos descentralizados, permitiendo a sus usuarios interactuar con una multitud de servicios financieros. Por ejemplo, MakerDAO, Compound o Uniswap. Los usuarios y desarrolladores pueden gestionar su cartera DeFi y pueden aprovechar todo el potencial de las finanzas descentralizadas. Permite agregar e interactuar con diferentes protocolos en la misma aplicación: prestar y pedir prestado, intercambiar tokens u apalancar el capital propio. Todas las transacciones dentro de la aplicación se realizan a

través de contratos inteligentes, y se necesita una aplicación de monedero digital como MetaMask para poder utilizar su interfaz (Moncada et al, 2020).

4.3.6 Flexa

Es una red de pagos instantáneos que cuenta con protocolos de seguridad para evitar el fraude de activos digitales. Utiliza una cartera habilitada para la aplicación, y sus usuarios pueden gastar una gran variedad de criptomonedas, tokens ERC20 u otros puntos de recompensa, de forma instantánea, privada y sin comisiones. Su estructura es descentralizada, con el token (AMP) como núcleo de la red, y asegura todos los pagos en tiempo real. Además, este protocolo permite que se confirmen transacciones de otros activos digitales subyacentes y se liquiden (Abdal & Lesueur, 2019).

En la siguiente tabla se puede observar un resumen de las aplicaciones descritas anteriormente, con características principales como el valor total bloqueado de cada protocolo, su token principal para el uso de la plataforma y la cadena *blockchain* donde se encuentra.

Gráfico 9: Resumen de las principales aplicaciones descentralizadas

Logotipo	Aplicación	Valor Total Bloqueado (TVL)	Token Principal	Blockchain
	Uniswap	6.020.000.000 \$	ETH	Ethereum
	Maker	7.860.000.000 \$	WETH	Ethereum
	Aave	11.680.000.000 \$	WETH	Multichain
	Compound	7.090.000.000 \$	WETH	Ethereum

	InstaDapp	4.930.000.000 \$	DAI	Ethereum
	Flexa	1.200.000.000 \$	AMP	Ethereum

Fuente: Coingecko 8 de junio de 2021. Elaboración propia

Capítulo V: Conclusiones del trabajo

5. CONCLUSIONES DEL TRABAJO

La descentralización financiera tiene el potencial para crear un nuevo ecosistema de aplicaciones de servicios financieros: se espera que su crecimiento y desarrollo continúen en el futuro: si se analizan los datos históricos de la evolución y el crecimiento de los ecosistemas, se puede comprobar el potencial y progresiva adopción de estas tecnologías por la población. El ecosistema DeFi ha crecido exponencialmente en 2021 hasta sobrepasar los 100.000 millones de dólares de activo depositados. El número de direcciones Ethereum únicas se han disparado en el último año, desde los 130 millones de cuentas el 1 de enero de 2021 hasta los 146 millones de direcciones únicas contabilizadas el 1 de abril (Anexo III). Sin embargo, al ser DeFi un sector en crecimiento, se puede comprobar que sólo 1,75 millones de direcciones únicas usaban al menos un protocolo DeFi. Aun así, esa cifra representa un crecimiento del 50% en el último trimestre y un incremento diez veces superior desde el último trimestre de 2020. Ese aumento de usuarios ha permitido una rápida evolución de muchas plataformas, tanto en volumen como en tamaño. El volumen de intercambio de activos digitales en plataformas descentralizadas (DEX), pasó de aproximadamente 25.000 millones de dólares en el mes de diciembre de 2020, a 63.000 millones de dólares en marzo de 2021. Con todo esto, es muy probable que el valor total depositado (TVL) crezca en el futuro cuando el mercado reconozca todas estas mejoras del ecosistema. El crecimiento de valor de los activos DeFi está fuertemente vinculado a que sus fundamentos tienen cada vez más solidez y no sólo se incrementan por una mayor aceptación hacia los activos digitales. Con la tecnología blockchain como elemento disruptivo, la descentralización está llamada a devolver la privacidad y la confianza a los usuarios y permitir que los individuos pertenezcan en un futuro, a un ecosistema público, transparente y con total seguridad.

Las aplicaciones descentralizadas pueden facilitar la inclusión financiera en países en vías de desarrollo: el problema de acceso a los servicios financieros está relacionado con países en desarrollo y aquellas personas que no forman parte del sistema bancario. Sin embargo, en muchos países desarrollados se encuentran muchas personas sin servicios bancarios, que pueden aprovecharse de la oportunidad que brinda la tecnología *blockchain* y el ecosistema DeFi. La posibilidad de ofrecer servicios bancarios descentralizados permite que un usuario con únicamente un teléfono móvil e internet pueda acceder a multitud de servicios financieros. El problema es que la mayoría de la población desconoce el sector y que hay muchas plataformas que son difíciles de

usar por la necesidad de utilizar una carteras virtuales o plataformas de intercambio descentralizados. Se necesita que las instituciones pongan el foco en diseñar políticas de descentralización, y establecer la ruta para facilitar el acceso a DeFi por parte de la población.

Las aplicaciones descentralizadas no pretenden desbancar a las finanzas tradicionales: el auge de DeFi puede servir potencialmente para llamar la atención de las instituciones establecidas. Las aplicaciones financieras que se ofrecen en un entorno descentralizado y el sistema financiero tradicional, no son incompatibles. Las soluciones DeFi pueden estar representadas en las estructuras centralizadas de fintech, e incluso grupos como la Chicago DeFi Alliance ven en las soluciones DeFi una vía para salir de la recesión causada por el coronavirus, así como un posible camino para futuros desarrollos financieros. Esto se podría acelerar si las instituciones tradicionales se abren más a este sector y en la medida de lo posible, muestran más flexibilidad en su cooperación.

Las finanzas descentralizadas han llegado para quedarse: por primera vez en la historia, se está desarrollando un sistema financiero a gran escala, sin intermediarios. En la actualidad, las aplicaciones DeFi no pueden competir en términos de seguridad, velocidad y facilidad de uso con las soluciones financieras tradicionales. Pero DeFi ha producido aplicaciones reales y operativas que ya han conseguido atraer miles de millones de capital. Esos recursos se utilizarán para desarrollar en el futuro aplicaciones más competitivas y fáciles de usar. Por ello, DeFi tiene el potencial de convertirse en una de las industrias más importantes de blockchain si la tecnología se desarrolla adecuadamente, especialmente si se resuelven las dificultades de escalabilidad.

6. BIBLIOGRAFÍA

Aave. (2021). Aave whitepaper. <https://aave.com>

Abdat, M., & Lesueur, R. S. (2019). Value Propositions in the Cryptocurrency Ecosystem: A Stakeholder Analysis (Master's thesis, Handelshøyskolen BI).

Arias, F. G. (2012). El proyecto de investigación. Introducción a la metodología científica. 6ta. Fideas G. Arias Odón.

Adams, H. (2018). Uniswap Whitepaper. <https://uniswap.org/docs>.

Aste, T. (2016). The fair cost of Bitcoin proof of work. Available at SSRN 2801048.

Aydinli, K. (2019). Performance Assessment of Cardano.

Benston, G. J. (1976). SMITH Jr.; Clifford W. A Transactions Cost Approach to the Theory of Financial Intermediation. *The Journal of Finance*, 31(2), 215-231.

Burdges, J., Cevallos, A., Czaban, P., Habermeier, R., Hosseini, S., Lama, F., ... & Wood, G. (2020). Overview of polkadot and its design considerations. arXiv preprint arXiv:2005.13456.

Buterin, Vitalik. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform." 2013. <http://ethereum.org/ethereum.html>.

Bogoni, G. (2019). Cryptocurrencies stabilization systems: a focus on the MakerDAO case

Cevallos, A., & Stewart, A. (2020). Validator election in nominated proof-of-stake. arXiv preprint arXiv:2004.12990.

Chaudhry, N., & Yousaf, M. M. (2018, December). Consensus algorithms in blockchain: Comparative analysis, challenges, and opportunities. In *2018 12th International Conference on Open-Source Systems and Technologies (ICOSST)* (pp. 54-63). IEEE.

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13, e00151.

Chohan, U. W. (2021). Decentralized Finance (DeFi): An Emergent Alternative Financial Architecture. Critical Blockchain Research Initiative (CBRI) Working Papers.

Chohan, U. W. (2021). Non-Fungible Tokens: Blockchains, Scarcity, and Value. Critical Blockchain Research Initiative (CBRI) Working Papers.

Christensen, R. (2020) MakerDAO Whitepaper. <https://www.makerdao.com/en/whitepaper>

Coingecko. (2021). <https://www.coingecko.com/en/exchanges>

Cortes-Goicoechea, M., Franceschini, L., & Bautista-Gomez, L. (2020). Resource Analysis of Ethereum 2.0 Clients.

DeBank, (2021). DeFi Wallet for Ethereum Users. (n.d.). https://debank.com/ranking/locked_value

Defipulse. (2021). <https://defipulse.com/>

DeFi Report Q1 2021. (n.d.). <https://consensys.net/reports/defi-report-q1-2021-es>

Edwards, F. R., & Mishkin, F. S. (1995). *The decline of traditional banking: Implications for financial stability and regulatory policy* (No. w4993). National Bureau of Economic Research.

Fairfield J (2014) Smart contracts, Bitcoin bots, and consumer protection. *Wash Lee L Rev Online* 71:35–299

Frame WS, White LJ (2014) Technological change, financial innovation, and diffusion in banking. Federal Reserve Bank of Atlanta & Leonard N. Stern School of Business, Department of Economics, NY

Haber, S., & Stornetta, W. S. (1990, August). How to timestamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.

Hoskinson, C. (2017). Cardano Whitepaper. <https://cardano.org>

Huberman, G., Leshno, J., & Moallemi, C. C. (2019). An economic analysis of the bitcoin payment system. *Columbia Business School Research Paper*, (17-92).

Jeppsson, A., & Olsson, O. (2017). Blockchains as a solution for traceability and transparency.

- Katona, T. (2021). Decentralized Finance: The Possibilities of a Blockchain “Money Lego” System. *Financial and Economic Review*, 20(1), 74-102.
- Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference* (pp. 357-388). Springer, Cham.
- Kuznetsov, M. (2017). Ethereum 101. <https://www.coindesk.com/learn/ethereum-101/how-to-use-ethereum>
- Lafourcade, P., & Lombard-Platet, M. (2020). About blockchain interoperability. *Information Processing Letters*, 161, 105976.
- Larimer, D. (2013). Transactions as proof-of-stake. <https://cryptochainuni.com/wp-content/uploads/Invictus-Innovations-Transactions-As-Proof-Of-Stake.pdf>
- Lee, W. M. (2019). Using the metamask chrome extension. In *Beginning Ethereum Smart Contracts Programming* (pp. 93-126). Apress, Berkeley, CA.
- Leshner, R., & Hayes, G. (2019). Compound: The money market protocol. White Paper.
- Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. The decentralized financial crisis. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 1–15. IEEE, 2020.
- Lin, L. X., Budish, E., Cong, L. W., He, Z., Bergquist, J. H., Panesir, M. S., ... & Zhang, S. (2019). Deconstructing decentralized exchanges. *Stanford Journal of Blockchain Law & Policy*.
- Litvack, J., Ahmad, J., & Bird, R. (1998). Rethinking decentralization in developing countries. The World Bank.
- Meegan, X., & Koens, T. (2010). Lessons Learned from Decentralised Finance (DeFi). https://new.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2.0.pdf

Moncada, R., Ferro, E., Favenza, A., & Freni, P. (2020). Next Generation Blockchain-Based Financial Services. In Euro-Par 2020: Parallel Processing Workshops (Vol. 12480, p. 30). Nature Publishing Group.

Peterson, J., & Krug, J. (2015). Augur: a decentralized, open-source platform for prediction markets. arXiv preprint arXiv:1501.01042.

Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org>

Napoletano, E., & Schmidt, J. (2021). Decentralized Finance Is Building A New Financial System. *Forbes*. <https://www.forbes.com/advisor/investing/defi-decentralized-finance/>.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183-187.

Oleksiuk, A. (2021, Abril 21). How to Make Smart Contracts Work for the Insurance Industry: Intellias Blog. <https://www.intellias.com/how-to-make-a-smart-contract-work-for-the-insurance-industry/>

Panda, S. K., Elngar, A. A., Balas, V. E., & Kayed, M. (Eds.). (2020). Bitcoin and Blockchain: History and Current Applications. CRC Press.

Pep. (2021, May 17). ¿Qué es DeFi o Finanzas Descentralizadas? Retrieved from <https://academy.bit2me.com/que-es-defi-o-finanzas-descentralizadas/>

Martino, P., Bellavitis, C. and DaSilva, C. (2020). Cryptocurrencies and entrepreneurial finance. *The Economics of Cryptocurrencies*, pages 51–56.

Popescu, A. D. (2020). Decentralized Finance (DeFi)—The Lego of Finance. *Social Sciences and Education Research Review*, 7(1), 321-348.

Popescu A. D. (2020). Transitions and concepts within decentralized finance (defi) space. *Research Terminals in the social sciences*, page 40.

Puschmann, T. (2017). *Fintech. Business & Information Systems Engineering*, 59(1), 69-76.

Rapoza, K. (2021). DeFi ‘Yield Farming’: How to Get DeFi Yield, And Why Invest In It. <https://www.forbes.com/sites/kenrapoza/2021/06/06/defi-yield-farming-what-is-it-how-should-you-invest-in-it/?sh=7a539f0f2193>.

Real Academia de la Lengua Española. Diccionario RAE 2021. <https://www.rae.es>

Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, 8(2), 23-29.

Schär, F. (2021). Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review*.

Sunyaev, A. (2020). Distributed ledger technology. *In Internet Computing* (pp. 265-299). Springer, Cham.

Swanson T (2015) Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Work Pap

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc."

Szabo, Nick. "Smart Contracts." 1994. <http://www.fon.hum.uva.nl>

Szabo, Nick. "The idea of smart contracts." 1997. <https://nakamotoinstitute.org/the-idea-of-smart-contracts/>

Szabo N (1997) Smart contracts: formalizing and securing relationships on public networks. *First Monday* 2(9). doi:10.5210/fm.v2i9.548

T. Limited, (2016). “Tether: Fiat currencies on the bitcoin blockchain,”. <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>

Vujičić, D., Jagodić, D., & Randić, S. (2018, March). Blockchain technology, bitcoin, and Ethereum: A brief overview. In 2018 17th international symposium infoteh-jahorina (infoteh) (pp. 1-6). IEEE.

Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). SoK: Decentralized Finance (DeFi). *arXiv preprint arXiv:2101.08778*.

Whitaker, A. (2019). Art and blockchain: A primer, history, and taxonomy of blockchain use cases in the arts. *Artivate*, 8(2), 21-46.

Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White Paper.

Williams-Grut, O. (2018, Enero 01). The 11 biggest ICO fundraises of 2017. <https://www.businessinsider.com/the-10-biggest-ico-fundraises-of-2017-2017-12>

Yan Chen and Cristiano Bellavitis. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, 13:e00151, 2020.

Young, J. (2021, March 29). NFT Market Rages On: NFTs Market Cap Grow 1,785% In 2021 as demand explodes. <https://www.forbes.com/sites/youngjoseph/2021/03/29/nft-market-rages-on-nfts-market-cap-grow-1785-in-2021-as-demand-explodes/?sh=2262aa947fdc>

Zheng Z., Xie S., Dai H.N., Wang H. (2016) Blockchain Challenges and Opportunities: A Survey. Work Pap

Zhen, Y., Yue, M., Zhong-yu, C., Chang-bing, T., & Xin, C. (2017, Julio). Zero-determinant strategy for the algorithm optimize of blockchain PoW consensus. In 2017 36th *Chinese Control Conference (CCC)* (pp. 1441-1446). IEEE.

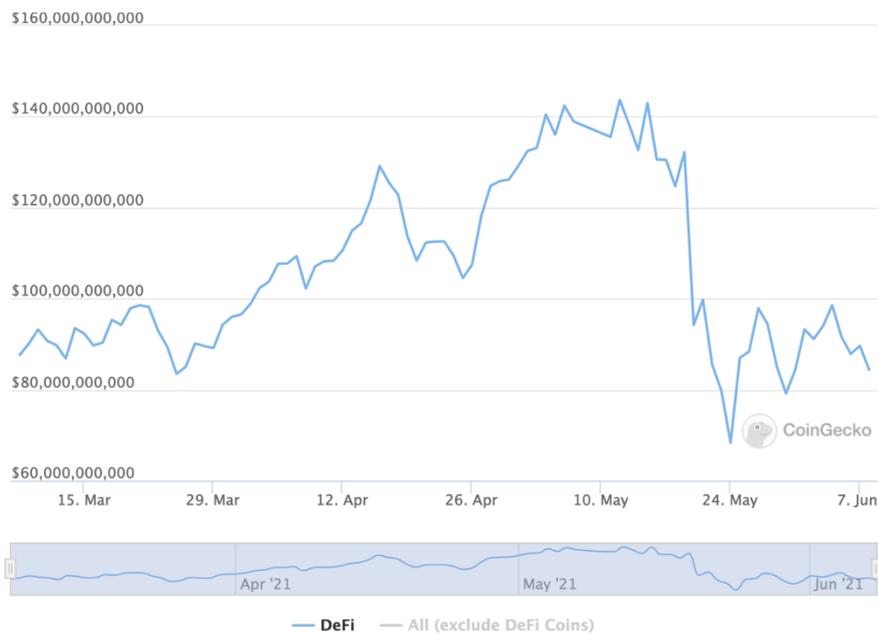
7. ANEXOS

Anexo I: Datos de capitalización y TVL de Ethereum

Capitalización bursátil DeFi	Capitalización bursátil ETH	Valor Total Bloqueado
82.479.876.856 \$	293.491.074.574 \$	102.198.448.310 \$

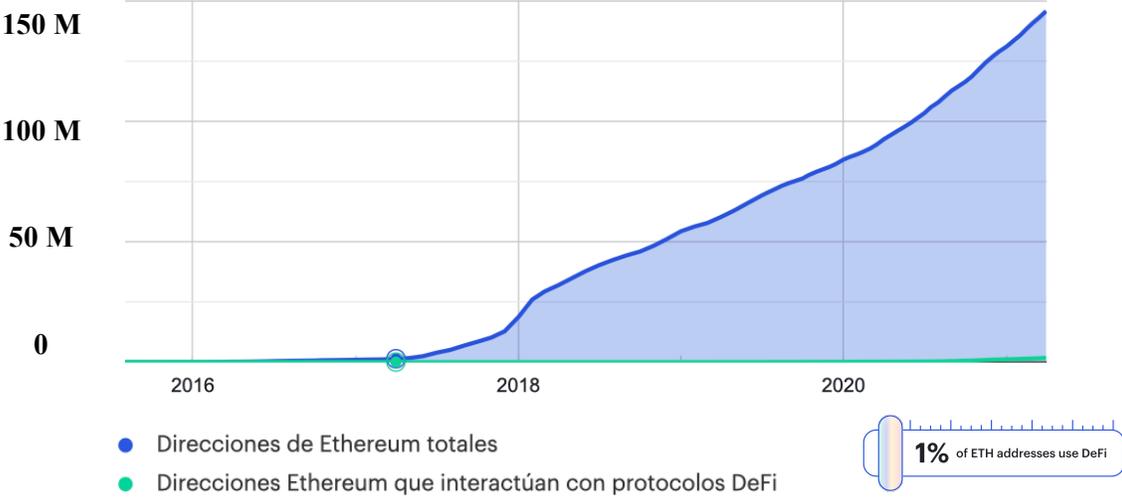
Fuente: Coingecko, 8 de junio de 2021. Elaboración propia

Anexo II: Crecimiento del ecosistema DeFi a lo largo de 2021



Fuente: Coingecko, 8 de junio de 2021

Anexo III: Direcciones Ethereum que interactúan con protocolos DeFi



Fuente: DeFi Report Q12021