Fco
Javier
Latasa

LA NUEVA ERA FINANCIERA: BLOCKCHAIN, SMART CONTRACTS & DEFI

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

LA NUEVA ERA FINANCIERA: BLOCKCHAIN, SMART CONTRACTS & DEFI

Autor: Francisco Javier Latasa Fernández-layos
Director: Ignacio Prieto Funes

MADRID | Abril 2022

La nueva era financiera: Blockchain, Smart Contracts & DeFi

Francisco Javier Latasa Fernández-layos
Universidad Pontificia Comillas (ICADE)

ABSTRACT

Así como el internet cambiaría para siempre los modelos de negocio prestablecidos, *blockchain* o cadena de bloques en español – base de datos distribuida entre participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí- desde su nacimiento en 2008, ha generado un nuevo modelo económico basado en la descentralización.

Esta tecnología ha proporcionado innumerables ventajas y oportunidades en la evolución del sistema financiero. No obstante, su nacimiento inesperado durante la crisis económica de 2008 ha supuesto una fuerte competencia para la banca tradicional.

Gracias a *blockchain* y a su desarrollo se ha llegado a generar una alternativa a las finanzas tradicionales centralizadas. En este trabajo se analiza su trayectoria, las implicaciones de su aparición y como ha sabido aplicar los fundamentos del sistema financiero tradicional y, sin necesidad de instituciones, intermediarios o autoridades centrales, generando alternativas financieras innovadoras para individuales e instituciones.

Ante el panorama expuesto, algunos expertos auguran la supresión de las entidades financieras tal y como las conocemos hoy en día. No obstante, la revisión bibliográfica y la actuación seguida por algunos individuos del sector sitúan un modelo híbrido como la optativa más probable. Esta investigación pretende colaborar en la comprensión de la tecnología, aportar una visión general de la situación financiera actual y futura tras la aparición de *blockchain*.

PALABRAS CLAVE: Blockchain, Bitcoin, Ethereum, Smart Contracts, DeFi, ERC-20, ERC-721, Decentralized finance Fintech, Flash loans, Flash swaps, Automatic Market

Maker, DEX, Decentralized Exchange, Cryptocurrency, Uniswap, MakerDAO, Compound, Ethereum, Aave, Yield protocol, Initial DeFi Offering, Yield farming

La nueva era financiera: Blockchain, Smart Contracts & DeFi

Francisco Javier Latasa Fernández-layos
Pontificia Comillas University (ICADE)

ABSTRACT

Just as the internet would forever change established business models, *blockchain*, since its birth in 2008, has generated a new economic model based on decentralization.

This technology has provided countless advantages and opportunities in the evolution of the financial system. However, its unexpected birth during the economic crisis of 2008 has brought strong competition for traditional banking.

Thanks to *blockchain* and its development, it has come to generate an alternative to traditional centralized finance. This paper analyzes its trajectory, the implications of its appearance and how it has been able to apply the fundamentals of the traditional financial system without the need for institutions, intermediaries or central authorities, generating innovative financial alternatives for individuals and institutions.

In view of the above, some experts predict the suppression of financial institutions as we know them today. However, a review of the literature and the actions of some individuals in the sector suggest that a hybrid model is the most likely option. This research aims to collaborate in the understanding of the technology, provide an overview of the current and future financial situation after the appearance of *blockchain*.

PALABRAS CLAVE: Blockchain, Bitcoin, Ethereum, Smart Contracts, DeFi, ERC-20, ERC-721, Decentralized finance Fintech, Flash loans, Flash swaps, Automatic Market Maker, DEX, Decentralized Exchange, Cryptocurrency, Uniswap, MakerDAO, Compound, Ethereum, Aave, Yield protocol, Initial DeFi Offering, Yield farming

Contents

Índice de ilustraciones

1. Introducción

En esta primera sección del trabajo, se explicará y justificará el por qué la elección de este tema: *blockchain, smart contracts* & DeFi. Posteriormente se enumerarán los objetivos de este trabajo.

a. Elección del tema y justificación

Vivimos en un mundo en constante transformación. En todos los ámbitos de nuestra vida, desde el plano profesional hasta el personal se precisa la constante actualización. En una mirada retrospectiva de 50 años, era inimaginable que un código pudiese ejecutar una operación y menos aún que este programa pudiese llegar a ser más eficaz y preciso que un experto con una larga trayectoria profesional. Esto mismo ha ocurrido en el campo financiero. Hoy en día, innumerables operaciones y transacciones se llevan a cabo sin la necesidad de ningún intermediario cuando antes era requisito indispensable la intervención de uno o varios profesionales. Las posibilidades que brinda la tecnología, de la mano de la criptografía ha generado lo que hoy conocemos como *blockchain* y sus derivados.

La tecnología *blockchain* se ha consolidado en los últimos años; comenzando como una idea un tanto anarquista que apostaba por la descentralización y apoyada por una minoría a consolidarse como una industria de hasta 3 trillones de dólares en 2021. Donde las principales instituciones han dado un giro en sus estrategias hacia el ecosistema *crypto* o cripto en español – ecosistema en el que se engloban las criptodivisas y actividades relacionadas con ellas- dejando atrás sus rechazos públicos y creando nuevas divisiones especializadas en este ecosistema.

Existe una gran expectación en torno a criptodivisas como Bitcoin así como a las *layers2* –protocolo que se construye sobre una *blockchain* ya existente- construidas en ecosistemas como el de Ethereum, donde la mayoría de proyectos de DeFi o finanzas descentralizas en español -estructura financiera descentralizada ejecutada sobre contratos inteligentes- están siendo desarrollados. Expertos afirman que *blockchain* transformará profundamente los sistemas de pago globales, la economía e incluso la política. Por otra

parte, profesionales de diversos sectores como las finanzas tradicionales o instituciones gubernamentales afirman que la industria *blockchain* es fundamentalmente defectuosa y carece de valor. “Personalmente, creo que Bitcoin tiene valor nulo” afirmó James Dimon, CEO de JP Morgan Chase en 2017. Más tarde, en 2018 con el lanzamiento de un sistema basado en *blockchain* por parte del banco de inversión más grande del mundo, cambiaría su postura “Me arrepiento de haber realizado ese comentario. *Blockchain* es real.” (Kim, 2018)

Las ofertas originales de criptomonedas ofrecen una alternativa a un sistema financiero dominado por los gobiernos y las instituciones centralizadas, como los bancos centrales. Su motivación principal fue el deseo de sustituir los sistemas financieros ineficientes y compartimentados por algoritmos inmutables, sin fronteras y de código abierto. Los parámetros de las monedas, como la inflación y el mecanismo de consenso, pueden ajustarse a través de su cadena de bloques subyacente para crear una variedad de propuestas de valor. (Abadi 2018) Una característica de *blockchain* es la posibilidad de diseñar productos *ad hoc* -a medida- en el que las necesidades de los clientes se satisfacen modificando los parámetros en función de cuales sean los objetivos del producto deseado. (Preukschat 2017)

En este trabajo se abordará desde el nacimiento de *blockchain* hasta los casos de uso de los smart contracts, con foco en DeFi. Con el fin de que el lector al finalizar la lectura haya desarrollado su conocimiento sobre *blockchain* y DeFi.

Mi formación académica especializada en las finanzas junto con mi pasión y posterior desarrollo en el mundo laboral por el sector tecnológico me han llevado a adentrarme en *blockchain.* La naturaleza descentralizada junto con el espíritu de comunidad permite que encontrar información de calidad para formarse esté al alcance de todo el que lo busca. Sin embargo, la industria está en pleno proceso de desarrollo y mantener actualizada esta información es responsabilidad de todos los participantes. Es por ello por lo que como inversor y alumno de la industria me propongo generar un Trabajo Final de Grado que sirva para dar a conocer, a aquel que lo desee, este ecosistema desde sus cimientos hasta el desarrollo de DeFi.

b. Objetivos de Investigación

Como se presentaba anteriormente, la industria, por su desarrollo reciente, presenta grandes campos de innovación que requieren constante actualización en cuanto a literatura académica se refiere. Con motivo de poder contribuir a la literatura en lo referente a *blockchain* y su influencia en el mundo financiero, este trabajo pretende analizar la historia y evolución en los últimos años, así como los casos de uso de los *smart contracts* que han dado lugar a soluciones como DeFi. Con el fin de que el lector al finalizar la lectura amplíe su conocimiento sobre las finanzas descentralizadas.

Se comenzará poniendo foco en los conceptos de *blockchain*, una base de datos descentralizada, verificable y ordenada. Para tener una mejor idea de qué es, se expondrá el contexto que dio lugar al nacimiento de Bitcoin. Analizando ésta, como la primera cadena de bloques con adopción.

Pasando a desarrollar el nacimiento de Ethereum; una implementación diferente de *blockchain*, centrada en aplicaciones descentralizadas. Se estudiarán casos de uso que se pueden construir sobre Ethereum. Poniendo especial foco en DeFi. En qué se diferencia de TradFi o finanzas tradicionales en español- en este grupo se encuentran todos los servicios financieros tradicionales centralizados- qué alternativas propone y a qué ciclo de adopción se enfrentan las finanzas tradicionales.

Este trabajo está dirigido a las personas que quieren aprender más sobre las soluciones de *blockchain*, haciendo un fuerte énfasis en las aplicaciones prácticas de Ethereum. Está dirigido tanto a personas con conocimientos técnicos como personas que desean explorar este ecosistema por primera vez.

2. Marco Teórico

a. Historia de blockchain

i. Tipos de blockchains

"Una *blockchain* no es diferente de una base de datos que se halla distribuida entre distintos participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente. En resumen, una *blockchain* funciona como una base de datos inmutable. Con la característica que permite que partes que carecen de confianza puedan tener consenso sobre la existencia, estado y evolución de una serie de factores compartidos. El consenso es precisamente la clave de un sistema *blockchain* porque es el fundamento que permite que todos los participantes puedan confiar en la información que se encuentra grabada." (Preukschat 2015)

Las soluciones basadas en *blockchain* son objeto de investigación institucional, especialmente en el sector financiero y gubernamental. Hay consenso en que las tecnologías sobre las que siguen operando estos sectores están obsoletas y necesitan desesperadamente una transformación para satisfacer las demandas modernas. *Blockchain* es una de las soluciones más valoradas para transformar estos sectores. Con casos como Blackrock, el gigante de la inversión presentó documentos ante la Securities and Exchange Commission (SEC) que muestran que quiere incluir los futuros de Bitcoin liquidados en efectivo como inversiones elegibles para dos de sus fondos. (Hansen 2021)

Aunque la mayor parte del trabajo de liquidación entre empresas comerciales podría automatizarse, las operaciones financieras correspondientes siguen realizándose manualmente, en parte debido a los requisitos legales y costumbre. Del mismo modo, los gobiernos mantienen múltiples registros, que exigen un proceso de conciliación largo y que demandan numerosos recursos. Por ello, se necesitan sistemas de registro automatizados que puedan sustituir a los actuales y crear un entorno unificado e interconectado.

Para comprender bien el alcance de esta tecnología, debemos conocer los elementos básicos que la componen:

- Los diferentes ordenadores que sustentan la red y que se comunican bajo el mismo protocolo se conocen como nodos.

- Se diferencia de un sistema centralizado en el que el control reside en una única entidad. No existe jerarquía entre nodos en las *blockchain*s públicas, en una privada, se puede establecer jerarquía en los nodos si así se desea.

- Operan bajo un protocolo estándar. Código según el cual los ordenadores que forman la red y funcionan como nodos, operan. Otorga un estándar común para definir la comunicación entre los ordenadores que componen la red.

- Red entre pares, o P2P. Los nodos se encuentran interconectados dentro de una red compartida.

Bitcoin es un sistema de moneda digital *peer-to-peer* basado en la tecnología *blockchain*. En su forma más simple, una cadena de bloques es un tipo de base de datos distribuida que está optimizada para procesar datos con prioridad en el tiempo, como las transacciones financieras. Las cadenas de bloques se distinguen de las bases de datos distribuidas convencionales de forma horizontal, como MySQL Cluster, MongoDB y Apache HBase, por su principal elemento de diseño: la seguridad integrada. Concepto que se desarrollará a continuación. (Kose 2022)

La seguridad de las cadenas de bloques hace que sea prácticamente imposible modificar o eliminar las entradas de la base de datos; además, este nivel de seguridad no es aplicado por una autoridad central (como es el caso de las bases de datos distribuidas bajo las que operan servicios de *cloud storage* como AWS), sino por el propio protocolo de la cadena de bloques. La naturaleza distribuida y descentralizada de las cadenas de bloques las convierte en una alternativa atractiva a las soluciones existentes utilizadas por las instituciones financieras. Las desventajas de las cadenas de bloques, como su confirmación de transacciones relativamente lenta y su limitada escalabilidad, son justificadas por el incremento en seguridad y la ausencia de un único punto de fallo, al estar distribuidas. En palabras de Nick Szabo, el inventor de los contratos inteligentes o *smart contracts*, "los controles financieros adecuados están descentralizados, gracias a una "cadena de bloques humana" de contables, auditores, etc. que comprueban el trabajo de los demás". Así, la automatización de esta cadena humana, manteniendo la descentralización intacta es un paso lógico. (Allison 2015)

En el caso ideal, el procesamiento de transacciones con *blockchain* satisface las siguientes propiedades (Bitfury 2015):

- Las transacciones deben ajustarse al estado actual del sistema: en el caso de las transacciones financieras, si el saldo de X es 99 dólares, no puede pagar a Y 100 dólares.

- Las transacciones deben estar autorizadas, es decir, sólo X debe tener acceso a realizar transacciones utilizando su nombre.

- Las transacciones deben ser inmodificables: una vez que la transacción ha entrado en el libro mayor, debe ser inviable modificar su información.

- Las transacciones deben ser definitivas: una vez que la transacción se registra en el libro mayor, revertir la transacción o borrarla es inviable.

- Resistencia a la censura: si una transacción se ajusta a un protocolo del libro mayor, se añade a la *blockchain*, sin bloqueos por parte de alguna entidad central.

Aunque generalmente hablamos de *blockchain*, conviene especificar, debe acompañarse de un adjetivo, de modo que podamos diferenciar entre *blockchain*s públicas o *blockchain*s privadas, por ejemplo.

Podemos clasificar las *blockchain*s en función a su acceso a los datos que almacenan. (Bitfury 2015):

- Una cadena de bloques pública es una *blockchain* en la que no hay restricciones para leer los datos, enviar y presentar transacciones.

- Una cadena de bloques privada es una *blockchain* en la que el acceso directo a los datos y el envío de transacciones está limitado a una lista predefinida de

entidades.

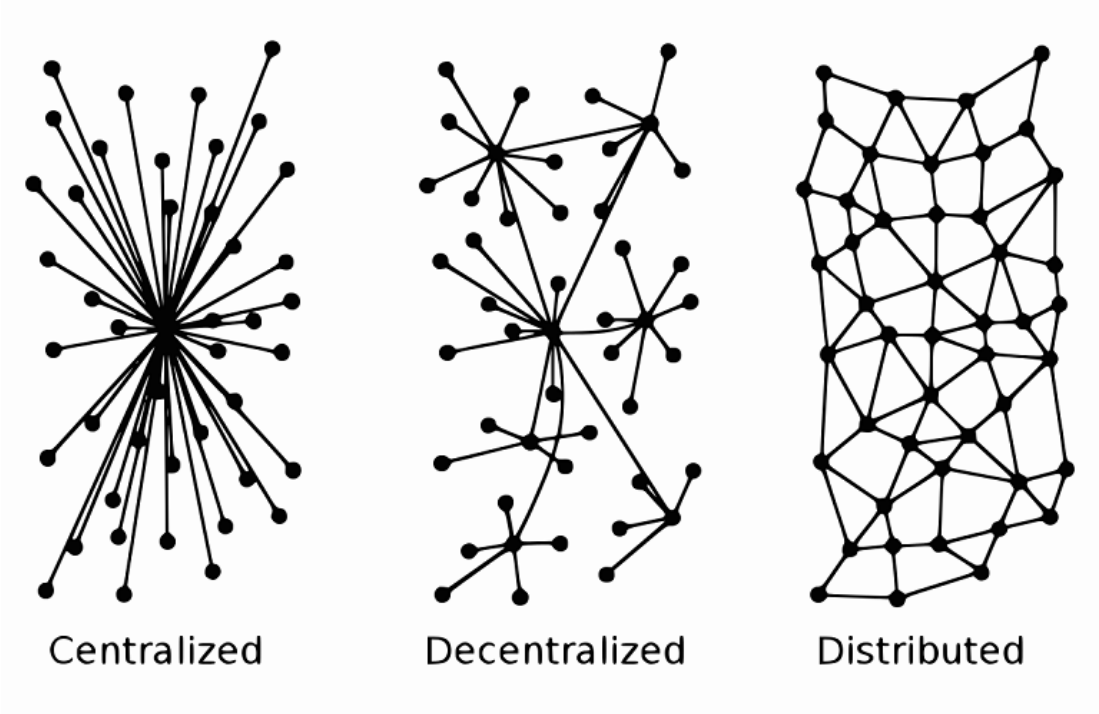
- Una *permisonless blockchain* o *blockchain* abierta es una cadena de bloques en la que no hay restricciones sobre las identidades de los procesadores de transacciones (es decir, los usuarios pueden crear bloques de transacciones). Cualquier persona con el equipo y conocimiento técnico necesario puede participar en el protocolo.

- Una *permissioned blockchain* es una cadena de bloques en la que el procesamiento de las transacciones se realiza por una lista predefinida de sujetos con identidades conocidas.

Los participantes de una *blockchain* privada operan sujetos al protocolo predeterminado por el creador de la red. Es por ello por lo que cadenas de bloques privadas pueden contar con mayor centralización sino total. Pues los nodos que componen la red podrían ser únicamente los creadores de ésta. Funcionando de manera más parecida a una base de datos, pero en la que la seguridad e inmutabilidad de los datos serían las principales ventajas. Es por ello por lo que muchas de las *blockchain*s privadas son referidas como *Distributed Ledger Techology* (DLT) pues funcionan como un libro mayor tradicional pero distribuida pues la base de datos está repartida en nodos.

Las primeras *blockchain*s, como Bitcoin o Ethereum, nacieron con el objetivo de ser públicas (cualquier persona sin ser usuario puede consultar el *ledger*), abiertas (cualquier persona con conocimiento y equipo puede participar), descentralizadas (todos los nodos son iguales entre sí y no hay control sobre otro) y pseudónimas (se manteniene el anonimato personal, aunque se pueden rastrear las direcciones al ser *blockchain*s públicas). Sin embargo, hay casos específicos sobre *blockchains* públicas que han sido diseñadas expresamente para mantener el anonimato, como Monero. (William 2019)

Ilustración 1: Comparación gráfica de conexión entre nodos



Fuente: "*The Role of Blockchain Technology in Ensuring Digital Transformation for Businesses: Advantages, Challenges and Application Steps",* Kirbac, G. (2021)

La actitud general de las instituciones financieras hacia Bitcoin y otras *public permisionless blockchains* sigue siendo algo escéptica, mientras que la actitud es más inclusiva hacia las *private / permisionned blockchains.* Las principales razones por las que el sector financiero rechaza este tipo de *blockchains* son:

- Falta de control sobre los procesadores de transacciones (es decir, los mineros en el caso de Bitcoin). Numerosas jurisdicciones exigen que se revele la identidad de los procesadores de transacciones, lo que contradice directamente el protocolo de Bitcoin (cualquiera, desde el anonimato, puede minar mientras disponga de suficientes recursos computacionales). Según Craig Donaldson, director general de Metro Bank, "la ausencia de normas definitivas de cumplimiento financiero para los servicios de Bitcoin limita su potencial de crecimiento." (Fintech TV 2016)

- En relación con lo anterior. Preocupa la confidencialidad de los clientes. Al ser *blockchains* públicas que aún funcionando en anonimato permiten consultar las transacciones y si se dispone del conocimiento adecuado trazar las direcciones de éstas pudiendo llegar a descubrir la persona detrás de ellas.

- El sistema de consenso, en el caso de Bitcoin y Ethereum 1.0, *Proof of Work* o PoW en inglés, (Prueba de Trabajo) se omite en las *private blockchains*. Lo que permite que sean más baratas de operar y capaces de generar un mayor número de transacciones.

- Las *permissioned blockchains* son más eficaces a la hora de generar cambios y modificar el protocolo. Pues no se requiere consenso por parte de una mayoría de la red.

La tecnología *blockchain* permite, partiendo de la misma base, construir una *blockchain* privada, cerrada y en la que se establezca un KYC a los participantes. O incluso híbrida, que asuma características de la pública y la privada. Las características de las *blockchain*s privadas son: (Bitfury 2015)

- Como su propio nombre indica, son *blockchain*s privadas, solamente los participantes tienen acceso a consultar los datos en la *ledger*.

- Son cerradas, solamente las personas o entidades invitadas adquieren la condición de usuario. Dentro de ella, se puede determinar qué acciones le están permitidas a cada usuario, pudiendo determinar que únicamente ciertos usuarios puedan leer los datos de la *ledger* por ejemplo.

- Son distribuidas, el número de nodos de la red puede limitarse al número de participantes que se desee. Los participantes se comprometen a mantener la red. No significa que cada nodo necesite mantenerla, esta función puede estar asumida por la entidad que opera la red, como un banco.

- El nivel de anonimato queda abierto a deseo del creador de la red. Se puede

establecer que toda transacción que realice un usuario quede registrada y éste sea identificado, esto, por ejemplo, tiene sentido a nivel contable o fiscal.

ii. Bitcoin

Hay mucha expectación con Bitcoin y las criptomonedas. Los seguidores aseguran que Bitcoin alterará los sistemas de pagos, modelos económicos y la política. Por otro lado, los detractores a *crypto* claman que Bitcoin colapsará pues carece de fundamentos. Pero para entender qué es Bitcoin y por qué ha sido tan disruptivo, hay que entenderlo desde sus cimientos. Se comenzará explicando qué tecnologías previas inspiraron el nacimiento de Bitcoin.

El camino hacia Bitcoin está pavimentado con los restos de intentos anteriores. He extraído una lista de aproximadamente un centenar de sistemas de pago criptográficos notables del libro *"Bitcoin and Cryptocurrency Technologies*", incluyendo el dinero electrónico y la tecnología basada en tarjetas de crédito. Algunos son propuestas académicas, mientras que otros son auténticos sistemas que se han implementado y probado. Es probable que sólo haya un nombre en esta lista que reconozca, PayPal. Y es que PayPal ha sobrevivido porque supo alejarse rápidamente de su idea original de pagos criptográficos en dispositivos portátiles. (Narayanan 2016)

Ilustración 2: Listado de sistemas de pagos criptográficos

ACC	CyberCents	iKP	MPTP	Proton
Agora	CyberCoin	IMB-MP	Net900	Redi-Charge
AIMP	CyberGold	InterCoin	NetBill	S/PAY
Allopass	DigiGold	Ipin	NetCard	Sandia Lab E-Cash
b-money	Digital Silk Road	Javien	NetCash	Secure Courier
BankNet	e-Comm	Karma	NetCheque	Semopo
Bitbit	E-Gold	LotteryTickets	NetFare	SET
Bitgold	Ecash	Lucre	No3rd	SET2Go
Bitpass	eCharge	MagicMoney	One Click Charge	SubScrip
C-SET	eCoin	Mandate	PayMe	Trivnet
CAFÉ	Edd	MicroMint	PayNet	TUB
CheckFree	eVend	Micromoney	PayPal	Twitpay
ClickandBuy	First Virtual	MilliCent	PaySafeCard	VeriFone
ClickShare	FSTC Electronic Check	Mini-Pay	PayTrust	VisaCash
CommerceNet	Geldkarte	Minitix	PayWord	Wallie
CommercePOINT	Globe Left	MobileMoney	Peppercoin	Way2Pay
CommerceSTAGE	Hashcash	Mojo	PhoneTicks	WorldPay
Cybank	HINDE	Mollie	Playspan	X-Pay
CyberCash	iBill	Mondex	Polling	

Fuente: "*Bitcoin and Cryptocurrency Technologies*", Arvind Narayanan (2016)

Previo a la adopción de divisas, el trueque era la manera de intercambiar bienes, materiales y servicios entre personas. El contrato que se establecía entre las dos partes se denominaba permuta. Dado que no existe una tabla de cambios que asignase el valor a cada bien, servicio o material, se solía recurrir a la libre asignación de valor. Con lo que se delegaba en la capacidad de persuasión y confianza a través del entendimiento entre las dos partes.

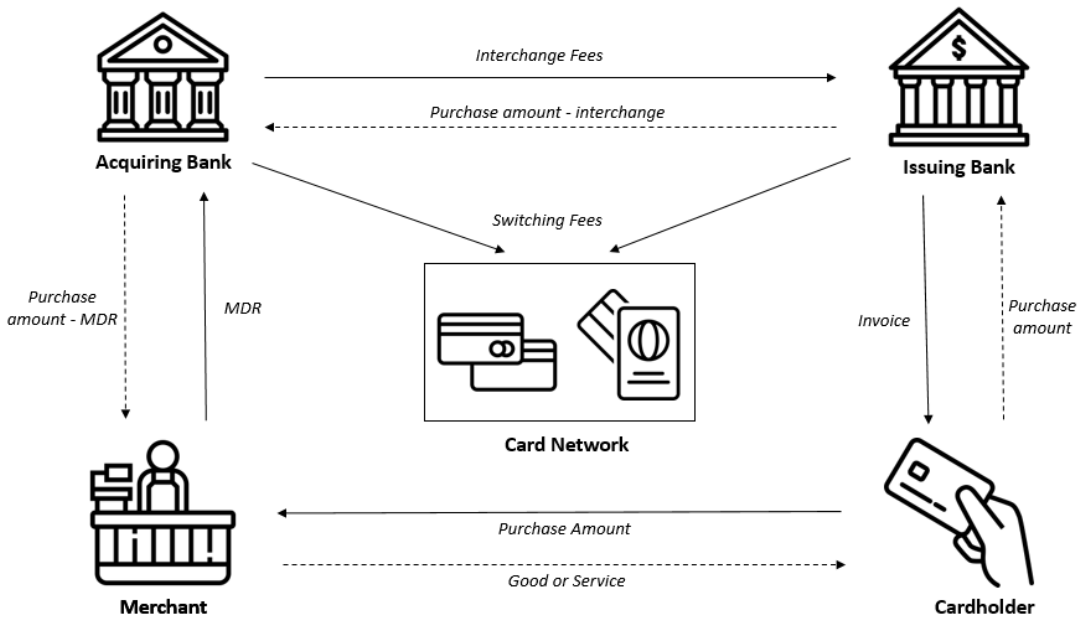
Eventualmente, según más bienes iban entrando al sistema, resultaba más difícil calcular el valor de cada. Esto, unido a la necesidad de encontrar otra persona que demandase lo que tu ofrecías y que ofreciese a cambio un bien, servicio o material de tu interés impulsaron el trueque a adoptar ciertos bienes comúnmente demandados que funcionaban de forma parecida a lo que hoy en día conocemos como divisas. Siendo en regiones el cacao, la sal (*salarium*, de ahí el término salario) o el oro. Siendo este último el percutor del fin del trueque como método de pago estándar.

El trueque no fomentaba la acumulación de riqueza. Los bienes intercambiados no eran fungibles y normalmente debían ser intercambiados al poco tiempo sino consumidos. Además del problema de coordinación previamente mencionado, alinear a dos personas cuyas necesidades y demandas coincidiesen en el mismo tiempo y espacio. Dos sistemas aparecieron para solucionar este problema de coordinación: efectivo y crédito.

Por una parte, el crédito permitía demandar un bien sin la necesidad de ser pagado en ese instante. Y el efectivo permitía intercambiar bienes teniendo un bien que facilitaba la tasación y la acumulación e intercambio. Aún, usando crédito, empleamos el efectivo para saber el monto a deber. Estas ideas son empleadas en muchos ámbitos, especialmente para intercambiar bienes en el ecosistema digital.

La tarjeta de crédito es el método de pago más utilizado en internet. Al realizar una compra con tarjeta, Amazon se encarga de procesar el pago a través del sistema. Un sistema en el que intervienen bancos y compañías emisoras de tarjetas de crédito, entre otros intermediarios.

Ilustración 3: Esquema de red de pago por tarjeta



Fuente: *"Introduction to Fintech"*, Tetyana B. (2022)

Por otra parte, métodos de pago como PayPal, funcionan como una arquitectura de intermediario. Es la compañía la que funciona como intermediario entre el comprador y el vendedor. Con la ventaja que el comprador solamente confía sus datos al intermediario. Quién al aprobar la transacción será el responsable de realizar el pago al vendedor. Esto da un valor añadido en seguridad al comprador en internet pues evita compartir sus datos con los diferentes vendedores. Pudiendo incluso pagar al vendedor sin necesidad de proveer identidad.

Dar los datos de nuestras tarjetas en la mayoría de los sitios web que compramos es el estándar. Pero en los primeros años de internet, los estándares de protocolos de encriptación estaban desarrollándose. Y no era común pagar directamente al vendedor ofreciéndole los datos de tu tarjeta. En esta época las arquitecturas de intermediario tenían mucho sentido y demanda. Hoy en día el comerciante no cobra inmediatamente, pero, sigue existiendo el riesgo de que el comprador genere una disputa y reclame su dinero a través de la compañía emisora de la tarjeta.

En los 90 hubo un sistema que competía con el sistema mencionado de arquitectura de intermediario. Este sistema se conocía como arquitectura SET. Evitaba que el vendedor tuviese acceso a tus datos sin la necesidad de inscribirte a un intermediario. Básicamente en SET, al comprar, el navegador manda los datos de tu transacción a una aplicación de compra en tu ordenador, donde junto con los datos de tu tarjeta, los encripta de un modo que solo el intermediario puede acceder a ellos. El intermediario desencripta tus datos y aprueba la transacción solamente si los datos de tu transacción concuerdan con los datos del vendedor.

SET fue desarrollado por VISA y MasterCard de la mano de Microsoft, RSA, IBM, Netscape y Verisign. Una de las compañías que utilizaba SET era CyberCash. Además de emplear este sistema, utilizaban dinero virtual, CyberCoin. El cual era empleado para realizar micropagos para acceder a ciertos servicios como lecturas de archivos. Por aquel entonces, el gobierno de los Estados Unidos restringía la exportación de servicios criptográficos a otros países, por ser considerado un arma de guerra. A pesar de esto, CyberCash consiguió permiso para operar pues su encriptación era considerada más difícil de extraer que de escribir desde cero. (Narayanan 2016)

SET no prosperó. El problema principal tenía que ver con los certificados. Un certificado es una forma de asociar de manera segura una identidad criptográfica, una *public-key*, con una identidad en la vida real. Conseguir un certificado requería un tedioso proceso. Bitcoin supo evitar este problema, evitando tener que certificar identidades en la vida real. En Bitcoin las *public-keys* son las identidades de las personas, no hace falta verificar su identidad en la vida real. (Narayanan 2016)

Así como comparamos crédito y efectivo anteriormente, podemos destacar que el efectivo tiene dos beneficios frente al crédito, de manera que presenta un mayor anonimato y permite transaccionar sin la necesidad de ser aprobado por un intermediario. Bitcoin, de distinta manera, provee anonimato en cierto modo (pues todas las transacciones se pueden consultar en la *blockchain*, rastrear y posteriormente asociar a una identidad si no se es precavido) y a la vez margina a los intermediarios gracias a su naturaleza descentralizada en la que es posible operar P2P. Funciona de una manera descentralizada en la que no hay un servidor central que la controle, de manera que lo hace más robusto a ataques, de la misma manera que el internet.

Los primeros esbozos de aplicar criptografía al dinero se remontan a 1983, de la mano de David Chaum. De manera similar a como funcionan los cheques bancarios, aplicó este mismo concepto, pero con firma digital. Para mantener el anonimato y solucionar el problema de *double-spending* -el gasto doble es la utilización completa o incluso la creación de transacciones falsas con el objetivo de atribuirse el uso legítimo de unas monedas para dos o más gastos distintos- rediseñó el proceso: el emisor desconocía el número de serie del cheque emitido, solo el beneficiario lo conoce, firmando el cheque a ciegas. O lo que se conoce como *blind signature*. Era el beneficiario el encargado de elegir un número de serie que no hubiese sido usado previamente. Pero este diseño requería de una autoridad central, como un banco, que certificase el proceso.

Cinco años más tarde, Chaum de la mano de los criptógrafos Fiat y Naor, trabajó en una moneda digital que pudiese operar desconectada de la red. El problema de *double-spending* se solventaba al comprobar el receptor de la transacción al conectarse a la red si era válida. De la misma manera que los cheques bancarios se comprueban con el banco más tarde para confirmar la disponibilidad de los fondos comprometidos en él.

El paso que dieron estos criptógrafos fue conseguir que toda moneda digital esté codificada a tu identidad, pero de manera que nadie es capaz de asociar una moneda con la identidad del que le pertenece.

Con el paso del tiempo este sistema fue perfeccionándose. Los criptógrafos Okamoto y Ohta publicaron el sistema de Merkle trees el cual permite subidividir las monedas. Este sistema será implementado en Bitcoin años más tardes por Satoshi Nakamoto. Así como el uso de *zero-knowledge proof* (capacidad de probar que información es cierta sin mostrarla) que serán utilizados posteriormente tanto en Bitcoin como en Ethereum y sus *layers2*. (Borde 2022)

En 1989, Chaum funda DigiCash, operaba con su propia moneda, eCash. Llegándose a implementar por bancos en Estados Unidos y Finlandia. Chaum era el propietario de varias de las patentes utilizadas en este sistema. Lo que generó rechazo por la comunidad a la hora de desarrollar la tecnología de Digicash.

Un grupo de criptógrafos se organizaron a través de Cypherpunks, lista a través de la cual, años más tarde, Satoshi publicaría el primer *white paper* -contenido escrito en el que se brindan datos y estadísticas sobre un tema específico- sobre Bitcoin. Estos criptógrafos desarrollaron una versión de eCash, a la que llamaron MagicMoney. Estaba basada en los mismos fundamentos que eCash, lo que violaba las patentes de Chaum pero teóricamente era solamente para uso experimental. Las transacciones se realizaban vía email. Era importante utilizar correo encriptado. Existían alternativas de correo encriptado con software como PGP. (Narayanan 2016)

Digicash no propsperó. No desarrolló el *network effect* -efecto red, en el que el consumo de una persona afecta directamente la utilidad de otra- requerido entre los comerciantes, además carecía de transacciones *user-to-user* (de usuario a usuario). La alternativa, compañías proveedoras de tarjetas de crédito como Mastercard, VISA o Discover. Bitcoin en cambio, no distingue de las transacciones entre identidades como comerciantes o usuarios. Lo que le hizo ganar popularidad previa a ser adoptada por comerciantes como estamos viendo en los últimos años. Pues la comunidad es capaz de impulsar su adopción transfiriendo entre usuarios.

En Digicash para obtener $1000 en eCash, necesitabas transferir $1000 de tu cuenta bancaria al banco que te hiciese de *exchange* – plataformas de intercambio de fiat a criptodivisas. En otro sistema, eGold, la moneda estaba respaldada por oro. Así lo hicieron otros proyectos más, hasta entonces el valor de la moneda digital estaba siempre respaldado por fiat o una *commodity*.

Para crear una moneda que sea independiente y capaz de adquirir valor real, tiene que ser escasa por naturaleza. Es por ello por lo que históricamente el oro se ha utilizado para respaldar fiat. En el ecosistema digital, una manera de lograr escasez es limitando el número de monedas que se puedan minar y creando un puzle matemático que haga que minar estas monedas requiera tiempo. Esta idea de desarrollar puzles computacionales se remonta a 1992 cuando los criptógrafos Dowrk y Naor idearon un sistema para evitar los correos con spam. Básicamente, tu ordenador debía resolver un puzle que solía comprender unos segundos. Esto no perjudicaba al usuario de a pie que enviaba pocos correos al día pero sí a los ordenadores empleados para enviar correos de forma masiva.

Estos puzles computaciones deben tener varias propiedades: La primera es que cada puzle debe ser propio de ese email, es decir que el sistema no pueda ser replicado por el ordenador en otros puzles para futuros emails. Segunda, al recibir el correo la respuesta debe ser fácilmente comprobada sin necesidad de repetir el proceso. Tercera, cada puzle debe ser completamente independiente de los otros, la solución de un puzle no puede comprometer la solución de otro. Cuarta, la dificultad de los puzles debe ser actualizada de manera que con el incremento de capacidad computacional el diseño de los puzles se ajuste. (Dwork & Naor 1992)

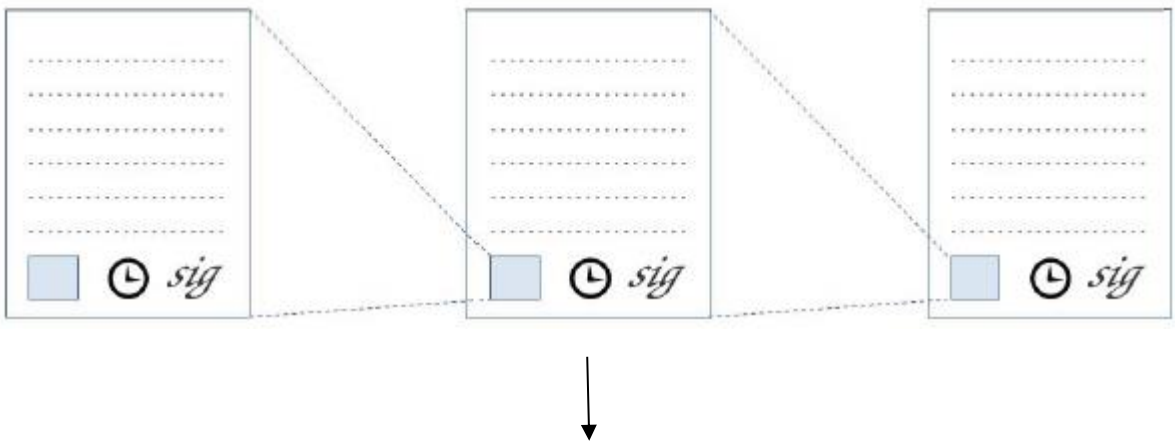
Bitcoin implementa un puzle computacional similar al desarrollado por Adam Black para HashCash. Conocido como *hash functions*. Estos son algoritmos que transforman cualquier *string* -secuencia de caracteres- de datos arbitrario en una serie de caracteres fijos. Bitcoin emplea el conocido SHA-256 (Secure Hash Algorithm). Los *hash* funcionan en una sola dirección, *one-way*, es decir podemos generar el hash partiendo de unos datos aleatorios pero es computacionalmente imposible a día de hoy revertir este proceso partiendo del hash para averiguar los datos iniciales. Si lo desea puede hacer sus propias pruebas aquí. Otro sistema similar es el RSA, desarrollado por Rivest and Shamir. En

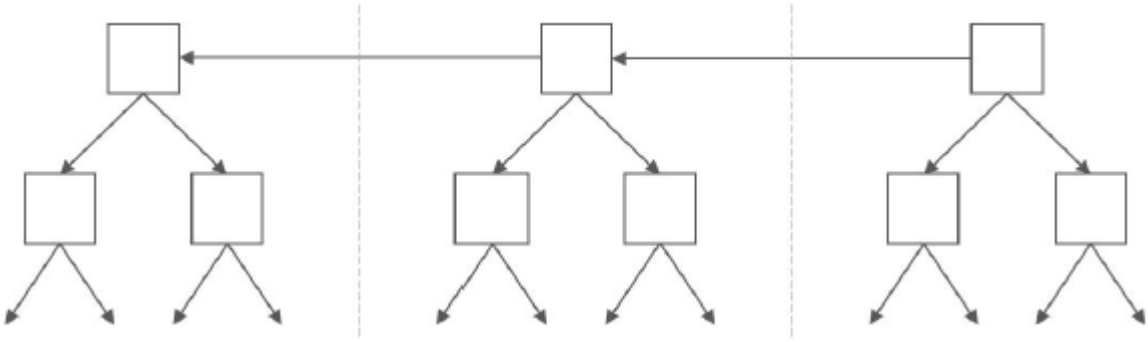
Hashcash el coste de resolver un número X de problemas se resume en el costo individual de resolver cada problema. Con el sistema RSA se pretende crear un gran coste fijo inicial pero un coste marginal bajo. De manera que minar la primera moneda cueste mucho en comparación con minar futuras monedas. (Rives, Shamir & Adleman 1977)

Otro componente fundamental en Bitcoin es *blockchain*: donde todas las transacciones quedan registradas de manera segura en un libro de cuentas abierto. Esta idea fue desarrollada en 1991 por Haber y Stornett. Su propuesta era desarrollar un método para guardar por orden temporal documentos digitales de manera inmutable. Lo que esto consigue es que cada certificado asegura que todo el historial de certificados previo está correcto y así de manera consecutiva. (Szostek 2020)

Para crear un certificado, el sistema relacionaba el *hash* con el certificado del documento previo, la hora y la firma. Más tarde se mejoró este sistema, en vez de coordinar los elementos de manera individual, se juntaban en bloques que posteriormente se unían formando una cadena. En cada bloque los documentos estaban de nuevo relacionados entre ellos, pero en un esquema en forma de árbol en vez de linear. Esto ahorraba la necesidad de comprobar que un documento apareciese en un momento particular en la historia del sistema. Esta estructura es la base sobre la que funciona la *blockchain* de Bitcoin. (Narayanan 2016)

Ilustración 4: Ilustración de hash pointer ineficiente vs eficiente

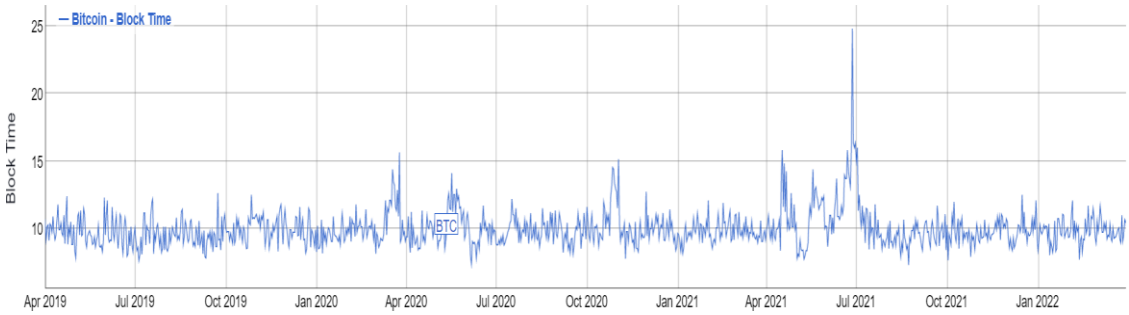




Fuente: "*Bitcoin and Cryptocurrency Technologies*", Arvind Narayanan (2016)

Bitcoin mejora este proceso en cuanto a la emisión de nuevos bloques. Basado en el protocolo de Hashcash. Esto le da a Bitcoin un extra en cuanto a seguridad. No necesita de servidores verificados, emplea a los denominados "mineros" quienes actúan como nodos no verificados. Cada minero se encarga de hacer seguimiento a los bloques. Cualquiera con una conexión activa a internet y poder computacional competente comparado al usado en ese momento por la red puede convertirse en minero. Resolver los puzles mencionados anteriormente, generando bloques. Bitcoin, a diferencia de este modelo no se basa en las firmas. Los bloques son creados aproximadamente cada 10 minutos. El *hashing algorithm* ajusta la dificultad en base al *hash rate*. La red Bitcoin tiene actualmente una tasa de hash de aproximadamente 190 EH/s, por lo que todos los mineros de la red están calculando el output de la función hash SHA-256 aproximadamente 190 quintillones de veces por segundo de media.

Ilustración 5: Bitcoin average block time



Fuente: "*Bitcoin Block Time"* Bitinfocharts: (2022)

En resumen, Bitcoin combina la idea de usar puzles computacionales para administrar la creación de nuevos bloques o BTC´s con la idea de crear un libro de cuentas abierto e inmutable en el que se soluciona el problema de *double-spending*.

Bitcoin se diferencia de propuestas similares como b-money o Bitgold creada por Nick Szabo en que en esas propuestas los puzles computaciones se emplean directamente para minar la divisa. En cambio, en Bitcoin, al solucionar el puzle, no obtienes BTC directamente, esa solución se utiliza para asegurar la red de *blockchain* y de manera indirecta te lleva a minar la divisa de Bitcoin (BTC) por un tiempo limitado. Bitcoin incorpora un mecanismo que ajusta automáticamente la dificultad de los puzles de manera periódica. A la vez, en estas propuestas no está claro que pasaría si la red es atacada y se desea realizar un cambio. En Bitcoin, el atacante debería ser capaz de resolver los puzles computaciones más rápidamente que el resto de la red. Lo que permite cuantificar la seguridad de la red, pues calculando la capacidad total de ésta se puede estimar cuantos recursos en cuanto a poder computacional necesitaría el atacante para lograr con éxito el cambio que desea realizar.

Recapitulación de cómo funciona una *blockchain* como Bitcoin. Una cadena de bloques es un mecanismo de almacenamiento de datos descentralizado y verificable. Se basa en la combinación de la criptografía de clave pública y el concepto nobel de *proof-of-work* o PoW:

> "Se trata de un protocolo en el que un comprobante demuestra a un verificador que ha realizado un determinado nivel de esfuerzo computacional en un intervalo de tiempo específico. Aunque no se ha definido como tal ni se ha discutido formalmente, la prueba de trabajo se ha propuesto como un mecanismo para varios objetivos de seguridad, incluyendo la medición del acceso al servidor, la construcción de cápsulas de tiempo digitales y la protección contra el envío de correo. spam y otros ataques de denegación de servicio." (Jakobsson 1999)

El proceso se divide en cuatro etapas (bit2me 2021):

- Primera etapa: El cliente o nodo establece una conexión con la red. En este punto,

la red le asigna una tarea computacionalmente costosa. Esta tarea debe ser resuelta a los fines de recibir un incentivo económico.

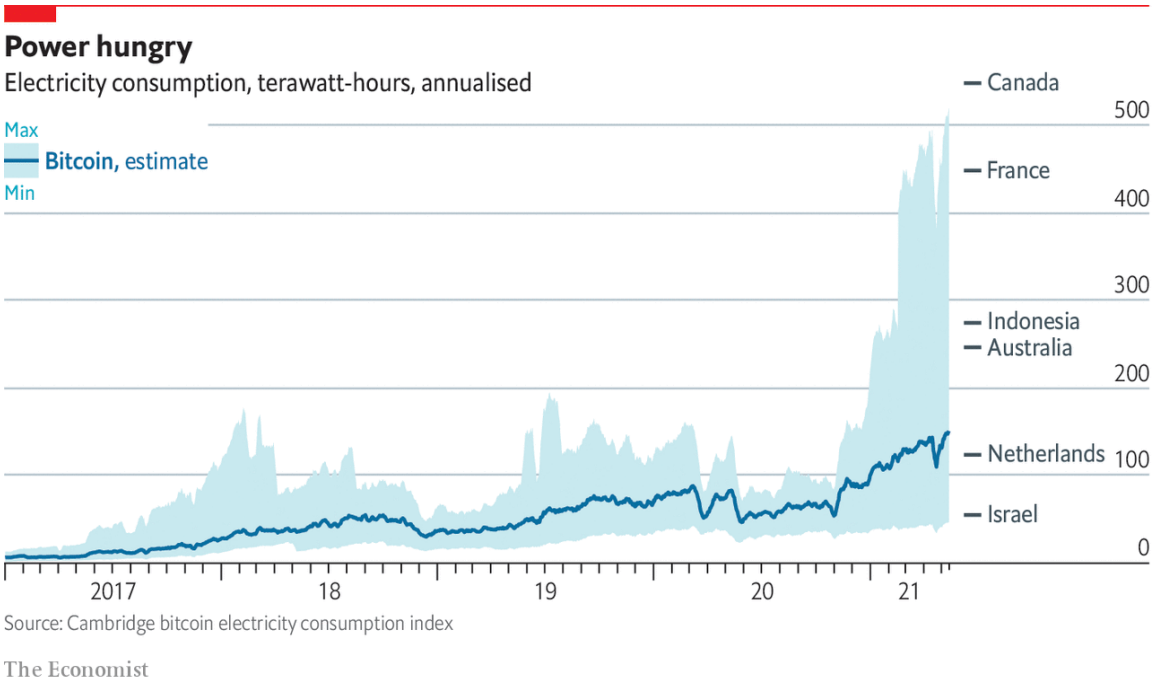
- Segunda etapa: Comienza la resolución del acertijo. Esto conlleva el uso de mucha potencia computacional hasta resolver el enigma entregado. Este proceso es el que recibe el nombre de minería.

- Tercera etapa: Una vez resuelta la tarea computacional, el cliente comparte esta con la red para su verificación. En este punto, se verifica rápidamente que la tarea cumpla con los requisitos exigidos. Si lo hace, se brinda acceso a los recursos de la red. En caso contrario, se rechaza el acceso y la solución presentada del problema. Es en este punto, donde se realizan las verificaciones de protección contra el doble gasto. Una protección que evita, que se presente más de una vez, una tarea ya asignada y verificada por la red.

- Cuarta etapa: Con la confirmación que la tarea ha sido cumplida, el cliente accede a los recursos de la red. Gracias a esto, recibe una ganancia por el trabajo computacional realizado.

Aunque este protocolo es muy seguro, resistente a ataques, adaptable a la tecnología y su software es fácil de implementar, el principal problema de *Proof of Work* es su consumo de energía. Para hacernos una idea, es comparable a todos los corredores de una maratón compitiendo por ser el primero en ganar la carrera computacional. Por la naturaleza de la competición, únicamente puede haber un ganador. Sin embargo, el resto de los participantes ha tenido que competir y por ende consumir energía. Cuantos más participantes tengamos en nuestro equipo, más posibilidades tendremos de ganar. Es por ello por lo que las compañías especializadas en minería de Bitcoin apuestan por el crecimiento de su infraestructura. Una alternativa es el auge de *mining pools* - espacio que le permite a los mineros trabajar de forma cooperativa para poder minar bloques de criptomonedas-, en las que mineros ponen sus recursos a disposición de la *pool* a la que pertenecen con el fin de hacer frente, de manera cooperativa, a la creciente dificultad de minar.

Ilustración 6: Gráfica índice de consumo de electricidad de Bitcoin



Fuente: "*Cambridge bitcoin electricity consumption index*" The Economist (2021)

Cada transacción en la cadena de bloques está firmada por el propietario legítimo del recurso que se negocia. Cuando se crean nuevas monedas (recursos), se les asigna un propietario. Este nuevo propietario puede entonces crear nuevas transacciones que envíen esas monedas a otros, simplemente incluyendo la clave pública del nuevo propietario en la transacción y firmándola con su clave privada. Esto crea una cadena verificable de transacciones; cada nueva transacción, con un nuevo propietario, apunta a la transacción anterior, con el propietario anterior.

Para garantizar el orden de estas transacciones y evitar el problema del doble gasto, las cadenas de bloques emplean *proof-of-work*. PoW es un proceso que establece un coste para agrupar las transacciones y añadirlas a la cadena de bloques en un orden determinado. Estas colecciones de transacciones se denominan bloques. (Jakobsson 1999)

Cada bloque de la cadena contiene una referencia a un bloque anterior, de ahí el nombre

de *blockchain*. Al hacer que la creación de bloques sea costosa y asegurar que cada nuevo bloque apunte al anterior, cualquier atacante que desee modificar el historial de transacciones de la cadena de bloques debe pagar el coste de cada bloque modificado. Debido a que los bloques apuntan a bloques anteriores, modificar un bloque antiguo requiere pagar el coste de todos los bloques posteriores, lo que hace que los cambios en los bloques más antiguos sean extremadamente caros. Al hacer que el coste de la creación de bloques sea computacional, una cadena de bloques aumenta la dificultad de modificar *blockchain*. En otras palabras, hay que gastar una cierta cantidad de energía de la CPU para crear nuevos bloques. Debido a que la potencia de la CPU depende en gran medida de los avances tecnológicos, es extremadamente difícil que una sola entidad maliciosa acumule suficiente potencia de CPU para superar al resto de la red. Un ataque práctico a una red basada en *blockchain* suele requerir que una sola entidad controle más del 50% de la potencia total de la CPU de la red. Cuanto mayor sea la red, más difícil. (Narayanan 2016)

Por su propia naturaleza, las transacciones pueden lograr algo más que la simple transferencia de recursos entre partes. De hecho, el acto de enviar puede describirse como un programa muy simple: el remitente genera un cálculo (transacción) que sólo puede realizarse si el receptor genera las entradas adecuadas en el futuro. En el caso de una transacción monetaria estándar, la entrada apropiada sería la prueba de propiedad del receptor. En otras palabras, el receptor puede gastar las monedas sólo después de establecer su propiedad. Cuando inicias una transferencia, debes demostrar que eres el propietario de la cuenta mediante un procedimiento de autentificación. Esto podría ser tan simple como un nombre de usuario y una contraseña para un sistema de banca en casa. En un banco, sería su tarjeta de identificación o de débito. Normalmente, estos procedimientos están integrados en el sistema, pero esto no tiene por qué ser así con las cadenas de bloques.

Es importante entender la propuesta de valor de Bitcoin, y puede ponerse en perspectiva evaluando la propuesta de valor de otros activos financieros. Consideremos el dólar estadounidense, por ejemplo. Solía estar respaldado por el oro antes de que se eliminara el patrón oro en 1971 bajo el mandato de Nixon. Ahora, la demanda de dólares proviene de: 1) los impuestos; 2) la compra de bienes estadounidenses denominados en dólares; y 3) el pago de la deuda denominada en dólares. En ninguno de estos tres casos se crea un

valor intrínseco, sino un valor basado en la red que es la economía estadounidense. La expansión o contracción de estos componentes de la economía estadounidense puede afectar al precio del USD (United States Dollar). Además, las perturbaciones de la oferta del USD ajustan su precio a un nivel determinado de demanda. La Reserva Federal (FED por sus siglas en inglés) puede ajustar la oferta de dólares a través de la política monetaria para alcanzar objetivos financieros o políticos. La inflación consume el valor del dólar, disminuyendo su capacidad de almacenar valor a lo largo del tiempo. Se podría temer una inflación galopante, lo que Paul Tudor Jones denomina "la gran inflación monetaria", que provocaría una huida hacia los activos resistentes a la inflación. El oro ha demostrado ser una exitosa cobertura contra la inflación debido a su oferta prácticamente limitada, a su utilidad concreta y a su fiabilidad general a nivel mundial. Sin embargo, dado que el oro es un activo volátil, su capacidad histórica de cobertura sólo se materializa en horizontes extremadamente largos. (Harvey, 2020)

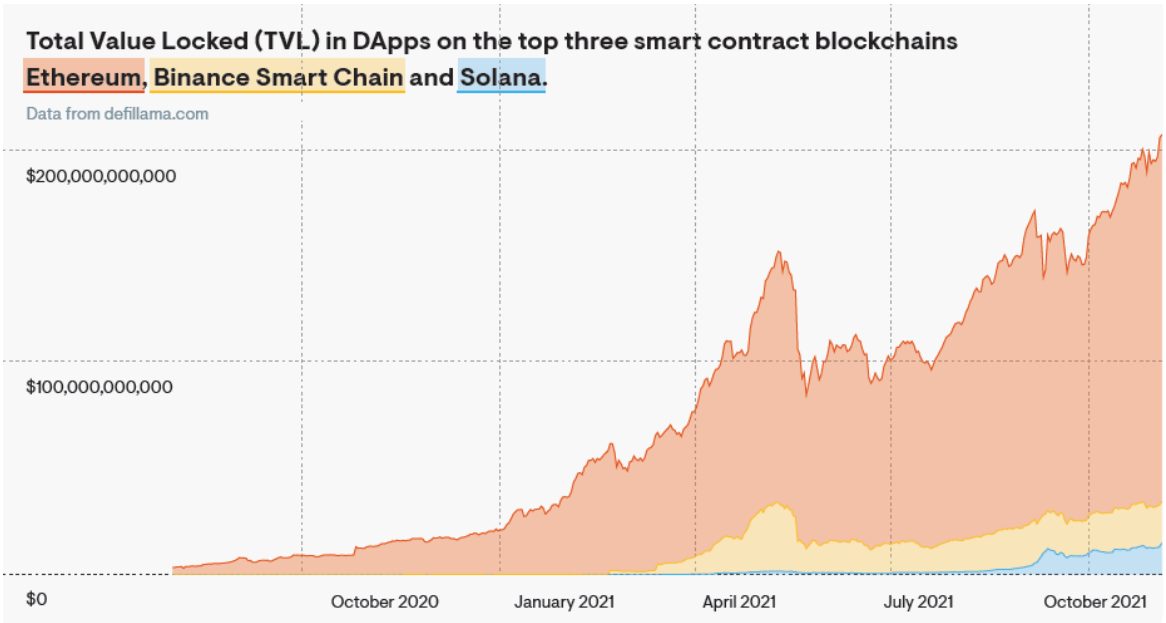
Bitcoin es un activo único. La oferta de Bitcoin está limitada a 21 millones de monedas. De ellas, 18,77 millones ya han sido "minadas". Esto significa que el 83% de todos los Bitcoins creados ya se han puesto en circulación en los 12 años siguientes a su creación. A principios de la década de 2030 -menos de una década después- se espera que se haya descubierto casi el 97% de Bitcoin. El 3% restante se creará a lo largo del próximo siglo, hasta 2140. A esto hay que añadir que muchos de los bitcoins minados son irrecuperables por sucesos como la pérdida de las *private-keys* que dan acceso a *cold wallets*. En un estudio realizado por Chainalysis, se estima que entre el 17% y el 23% del Bitcoin minado hasta la fecha se ha perdido. Estas cifras corresponden a entre 2,78 y 3,79 millones de BTC reales. (Chainalysis 2022)

Las *wallets* son carteras digitales donde almacenar y gestionar las criptomonedas. Las *cold wallets* se caracterizan por estar desconectadas de *blockchain* y por tanto del Internet, por ende, las más seguras en cuanto a ataques. Ejemplos de empresas que las comercializan son Ledger o Trezor. Que sean físicas implica que hay un riesgo asociado a la pérdida del *hardware* así como de la *seed phrase* (conjunto de 12 a 24 palabras aleatorias que operan como clave para acceder a tu cartera) pero esta es necesaria en todo tipo de *wallets*. Por otro lado, están las *hot wallets, software* con conexión a internet, estas ofrecen acceso y gestión más rápida que las *cold wallets* pero son más propensas a sufrir ataques. Ejemplos de éstas son Exodus o Metamask

El algoritmo de Bitcoin asegura que el suministro de Bitcoin recién minado se mantiene constante en el tiempo, independientemente del número de mineros. Cada diez minutos se crea un bloque que contiene 6,25 Bitcoins desde agosto de 2021. De media, el número de bloques creados seguirá reduciéndose a la mitad cada 210.000 bloques minados, lo que es aproximadamente 4 años si tenemos en cuenta que cada bloque se mina a una media de 10 minutos. Hasta que en el año 2140 sólo se conceda 0,000000001 Bitcoin por bloque "minado". Por lo tanto, la recompensa de minar Bitcoin, así como el suministro se reduce con el tiempo. Este proceso se conoce como *halving*. Esta escasez generada, hace de Bitcoin un activo único. (Cong, Li & Wang 2018)

Como el objetivo de este trabajo es poner en perspectiva al lector del desarrollo de esta tecnología con el fin de entender qué propuestas ofrece, en concreto DeFi. No se le dedicará más espacio a Bitcoin, el cuál podría abarcar todo este trabajo. Se ha explicado su historia y tecnología, sin entrar a detalle, con el fin de que el lector tenga en este momento una idea a alto nivel del desarrollo y funcionamiento de Bitcoin. La escalabilidad de Bitcoin es limitada. Por lo que a fin de estudiar DeFi, se continuará con Ethereum, la segunda criptodivisa por capitalización de mercado en el momento de escribir este trabajo ($403 billion) y la *blockchain* sobre la que se están desarrollando la mayoría de los protocolos de DeFi.

Ilustración 7: TVL en dApps en las top tres smart contract blockchains



Fuente: *"The Elliptic 2022 DeFi report"* Elliptic (2022)

iii. Ethereum

Previamente, examinábamos de cerca qué son las cadenas de bloques y cómo ayudan a hacer posibles las transacciones distribuidas y verificables. Utilizamos Bitcoin como ejemplo de análisis por ser la primera criptomoneda que generó adopción y ser la inspiración sobre la que se fundarían el resto de las criptodivisas. Ethereum es, en cierto sentido, una extensión lógica de las aplicaciones de Bitcoin. Permite los *smart contract*s, que son códigos que viven en una cadena de bloques, pueden controlar activos y datos, y definir las interacciones entre los activos, los datos y los participantes de la red. La capacidad de los *smart contract*s define a Ethereum como una plataforma de *smart contract*s. Analizaremos como opera Ethereum y como da lugar al desarrollo de aplicaciones y ecosistemas enteros como el de DeFi.

Ethereum está pasando de *proof-of-work* (PoW) a un mecanismo de consenso llamado *proof-of-stake* (PoS) - *Proof-of-stake* es un tipo de mecanismo de consenso utilizado por las redes de *blockchain* para lograr consenso distribuido- sin embargo, conseguir un PoS correcto es un gran reto técnico y no es tan sencillo como usar PoW para alcanzar el consenso en toda la red. (Prashant 2022)

Requiere que los usuarios apuesten su ether -moneda nativa de Ethereum- para convertirse en un validador en la red. Los validadores son responsables de lo mismo que los mineros en el *proof-of-work*: ordenar las transacciones y crear nuevos bloques para que todos los nodos se pongan de acuerdo sobre el estado de la red.

Como especifica Ethereum en su página web, *proof-of-stake* viene con una serie de mejoras respecto al sistema de *proof-of-work* (Ethereum.org 2022):

- Mayor eficiencia energética: no es necesario utilizar mucha energía para minar bloques.

- Barreras de entrada más bajas, requisitos de hardware reducidos: no se necesita un hardware de élite para tener la oportunidad de crear nuevos bloques.

- Mayor inmunidad a la centralización, el *proof-of-stake* debería llevar a más nodos en la red.

- Mayor soporte para las cadenas de fragmentos- las cadenas de fragmentos proporcionan capas de almacenamiento adicionales, más económicas, para que las aplicaciones y las acumulaciones (o «rollups») almacenen datos-: una mejora clave para escalar la red Ethereum.

Anteriormente demostramos cómo las transacciones de Bitcoin son en realidad pequeños programas que cada nodo interpreta utilizando una simple máquina virtual *stack-based*.

En el caso de Bitcoin, esta máquina virtual está limitada intencionadamente. No es *Turing-complete* y está limitada en el número de operaciones que puede realizar. Sin embargo, Ethereum sí lo es.

Que Ethereum sea *Turing-complete* significa que es capaz de utilizar su base de código para realizar prácticamente cualquier tarea, siempre que tenga las instrucciones correctas, el tiempo suficiente y la capacidad de procesamiento. Ahora examinaremos cómo Ethereum amplía estos conceptos.

Aunque es fácil perderse en el mundo de las criptomonedas y los simples intercambios entre dos usuarios, existen otras numerosas aplicaciones para los cálculos distribuidos y seguros. Numerosas aplicaciones adicionales son posibles cuando se utiliza un sistema *Turing-complete* para los cálculos asociados a una cadena de bloques. Este es el *blockchain* de Ethereum.

Aunque Ethereum introduce cálculos generales en la cadena de bloques, mantiene el concepto de "moneda". Su moneda se llama "Ether" y, como cualquier otra criptomoneda, es un valor numérico que puede almacenarse en direcciones de cuentas y gastarse o recibirse como parte de transacciones o generación de bloques. Algunas transacciones requieren que los usuarios gasten ether. Se desarrolla el por qué a continuación.

Un lenguaje Turing-completo es aquel que es capaz de realizar cualquier computación.

En otras palabras, si algo tiene un algoritmo, puede expresarlo. Así, los *scripts* – secuencia de comandos - de Ethereum, denominados contratos inteligentes, son capaces de realizar cualquier cálculo. Las transacciones se utilizan para ejecutar cálculos. Esto requiere que cada nodo de la red realice cálculos. Cualquier máquina capaz de ejecutar un lenguaje completo de *Turing* se enfrenta a una única dificultad: el problema de *halting*. El problema de la interrupción consiste esencialmente en que ninguna máquina de Turing puede predecir por adelantado si un programa que ejecuta terminará (se detendrá) o continuará ejecutándose indefinidamente. En otras palabras, la única manera de determinar si un trozo de código se repite indefinidamente o no es ejecutándolo. Esto crea un problema importante para Ethereum: ningún nodo puede quedar atrapado en un bucle infinito mientras ejecuta un programa. Esto detendría efectivamente la evolución de la cadena de bloques y detendría todas las transacciones. Sin embargo, existe una solución.

Dado el coste de la computación, y el hecho de que los nodos que producen bloques son recompensados con ether (como es el caso de Bitcoin), la manera de limitar los cálculos es exigir ether para ejecutarlos. Así, Ethereum aborda el problema de los ataques de denegación de servicio distribuidos a través de *scripts* maliciosos o con errores que se ejecutan indefinidamente. Cada vez que se ejecuta un *script*, el usuario que lo solicita debe especificar una cantidad máxima de ether para gastar en él. El *script* consume ether durante su ejecución. Esto se consigue a través de la máquina virtual que los ejecuta. Si éste no puede completarse antes de que se le acabe el ether, se aborta. "Gas" es el término utilizado en Ethereum para referirse al ether asignado a un *script* como límite (como en la gasolina). El gas se refiere a la unidad que mide la cantidad de esfuerzo computacional requerido para ejecutar operaciones específicas en la red de Ethereum. Dado que cada transacción de Ethereum requiere recursos computacionales para ejecutarse, cada transacción requiere una tarifa. El gas es la tarifa requerida para llevar a cabo una transacción en Ethereum con éxito. Las tarifas de gas se pagan en la moneda nativa de Ethereum, ether (ETH). Los precios del gas se indican en gwei, que a su vez es una denominación de ETH - cada gwei es igual a 0,000000001 ETH (10-9 ETH). Por ejemplo, en lugar de decir que su gas cuesta 0,000000001 ether, puede decir que su gas cuesta 1 gwei. La propia palabra "gwei" significa "giga-wei", y equivale a 1.000.000.000 de wei. El propio wei (llamado así por Wei Dai, creador de b-money) es la unidad más pequeña de ETH. (Peyrott 2017)

Como el ether es un medio de intercambio, puede convertirse en otras monedas. Esto proporciona al ether una valoración de moneda del mundo real, similar a la de las monedas de Bitcoin.

Un componente fundamental de DeFi es una plataforma para *smart contract*s. Estas cadenas de bloques van más allá de una simple red de pagos, como Bitcoin, al permitir la creación de *smart contract*s que aumentan las capacidades de la cadena. Ethereum es el principal ejemplo de plataforma de *smart contract*s. El concepto es eficaz porque permite a los usuarios codificar con confianza reglas para cualquier tipo de transacción e incluso crear activos escasos con funcionalidad especializada. Numerosas cláusulas de los acuerdos comerciales tradicionales podrían trasladarse a un *smart contract*, que no sólo enumeraría, sino que haría cumplir esas cláusulas de forma algorítmica. Más allá de las finanzas, los *smart contract*s tienen aplicaciones en los juegos, la administración de datos y la gestión de la cadena de suministro, entre otros ámbitos.

-ERC-20, ERC-721 and ERC-1155

ERC-20 es uno de los estándares de contratos inteligentes más significativos en Ethereum, habiendo surgido como el estándar técnico para todos los *smart contract*s en la *blockchain* de Ethereum que implementan tokens fungibles.

El dinero físico y las criptomonedas son "fungibles", lo que significa que pueden comerciarse o cambiarse entre sí. Además, tienen el mismo valor: un dólar siempre vale otro dólar; un Bitcoin siempre es igual a otro Bitcoin.

Es un estándar API que rige como los tokens deben ser desarrollados. ERC-20 establece un conjunto uniforme de reglas que todos los tokens fungibles de Ethereum deben seguir. Como resultado, este estándar de tokens permite a los desarrolladores de todo tipo prever con precisión cómo interactuarán los nuevos tokens con el sistema Ethereum en general. El objetivo y la necesidad de los tokens ERC-20, es diseñar un estándar, para crear interoperabilidad y compatibilidad entre tokens y fomentar mejoras en el ecosistema de Ethereum. Esto gracias a que los tokens ERC-20 facilitan enormemente el trabajo de crear nuevos tokens. Esto simplifica y facilita las tareas de los desarrolladores, ya que pueden

seguir trabajando sin tener que rehacer de nuevo el proyecto cada vez que se libera un nuevo token, siempre que éste se atenga a las reglas.

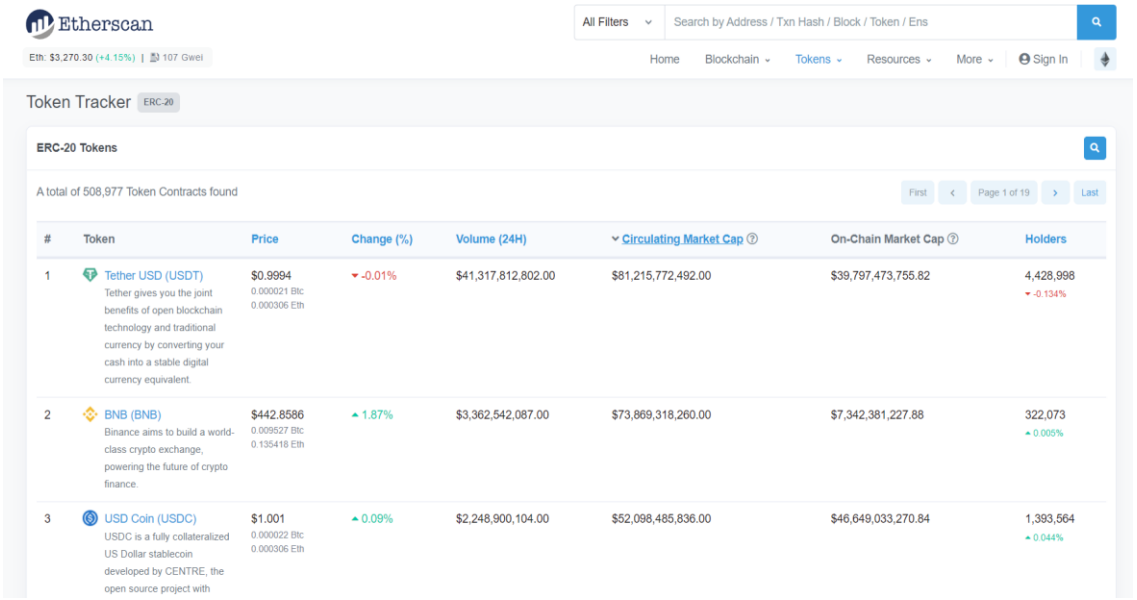
Ethereum permite crear su propia criptomoneda en la cadena de bloques con el estándar ERC-20. Este estándar, permite *mintear* -acuñar- tu propio token, éste puede ser fácilmente transferido entre carteras y vendido en los *exchanges* de criptodivisas con este estándar ERC-20. También es el estándar que nos va a permitir tener una venta de tokens en forma de ICO (Initial Coin Offering) -una empresa (o un proyecto de código abierto) recauda fondos vendiendo previamente el acceso a un producto o servicio posterior. (Li & Mann 2018)

Su creación fue propuesta por Fabian Vogelsteller y Vitalik Buterin, y aprobada el 19 de noviembre de 2015. La misma forma parte de los EIP de Ethereum, bajo la designación EIP-20 (Ethereum Improve Proposition o Propuesta de Mejora de Ethereum).

Las siglas ERC significan *Ethereum Requests for Comments* o Solicitud de Comentarios para Ethereum, mientras el número 20 proviene del EIP donde se describe. ERC-20 describe un estándar sobre las funciones y eventos que un *smart contract* de Ethereum puede implementar. (Ethereum.org 2022)

En la actualidad, los tokens ERC-20 son uno de los tokens más ampliamente utilizados en el mundo cripto. La cantidad de tokens ERC-20 creados es enorme, podemos comprobar en Etherscan que en la actualidad hay un total de +508.000 tokens.

Ilustración 8: Captura del listado de tokens ERC-20 en Etherscan



Fuente: Etherscan.io (2022)

Como explica Bit2Me en su artículo sobre ERC-20, estos tokens fueron diseñados con la motivación, principalmente, de crear un sistema de capacidad múltiple. Todo ello bajo una interfaz estándar reutilizable por otras aplicaciones: desde monederos hasta *exchanges* descentralizados. Todo ello bajo un API (abreviatura de Application Programming Interfaces, en español significa interfaz de programación de aplicaciones) que le garantiza a los desarrolladores las siguientes ventajas (Bit2Me 2021):

- Uniformidad en la programación. La API es estándar y estable lo que facilita la tarea de programar usando la misma. Esto facilita la tarea creativa de los programadores a la hora de crear nuevo software basado en las capacidades de Ethereum.

- Reduce la complejidad de la programación. Dado que la API es sencilla, emplearla reduce la complejidad del software creado para usarla. Esto se traduce en una mejor lectura, seguridad y auditabilidad del código escrito.

- Soporte para múltiples lenguajes de programación y mejoras en la

portabilidad. Dado que la API de los tokens es libre, es posible programar en ella en distintos lenguajes de programación. Ello facilita enormemente la capacidad de crear software específico. Algunos de los lenguajes soportados para esta tarea son Solidity, JavaScript, C, C++, Python, Java y Go.

- Menor complejidad en la comprensión de cada tipo tokens implementado. Esto gracias a que todos estarán basados en los mismos principios de funcionalidad.

- Mayor seguridad, en especial gracias a funciones como token *allowance* - permiten que una tercera parte tenga derecho a realizar una transacción de una determinada cantidad de nuestros tokens asociados a nuestra dirección.

- Menor riesgo de romper contratos, al no tener impedimentos, ni incompatibilidades. Esto gracias a que la API es estable, los cambios introducidos en ellas mejoran la misma, pero nunca romperán la compatibilidad.

El ERC-721 (Ethereum Request for Comments 721), propuesto por William Entriken, Dieter Shirley, Jacob Evans, y Nastassia Sachs en enero de 2018, es un estándar de tokens no fungibles que implementa una API para tokens dentro de los *smart contract*s. (de Figuereido 2021)

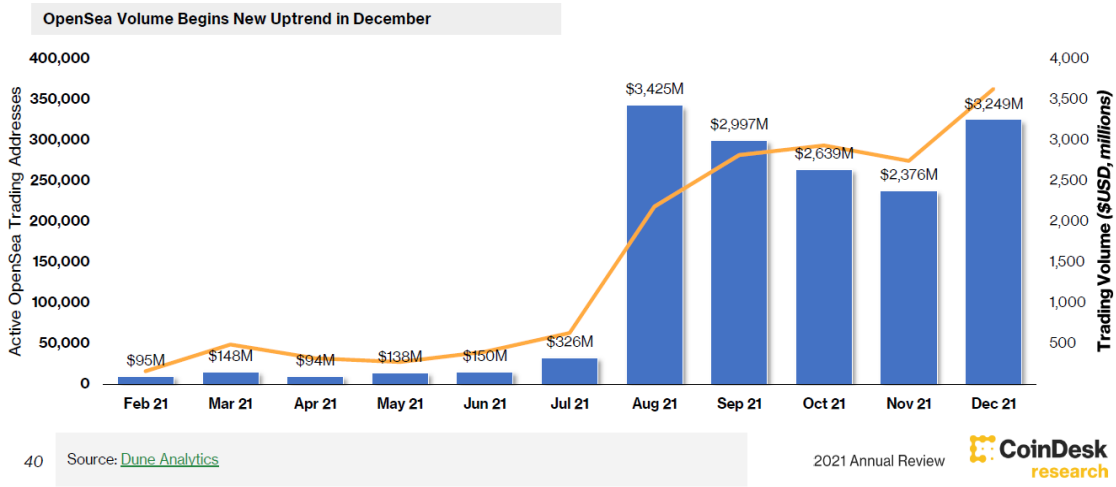
ERC-721 es un estándar abierto y gratuito que describe cómo construir tokens no fungibles o únicos en la *blockchain* de Ethereum. Más conocidos por sus siglas en inglés NFT´s (non-fungible tokens) Mientras que la mayoría de los tokens son fungibles (los token son idénticos), los tokens ERC-721 son todos únicos.

Un token no fungible (NFT) se utiliza para identificar en la *blockchain* un activo o identidad de forma única. Este tipo de token es perfecto para ser utilizado en plataformas que ofrecen artículos coleccionables, llaves de acceso, billetes de lotería, como prueba de afiliación a un club… Los *use cases* son aplicables a todos los sectores. Este tipo especial de token tiene unas posibilidades increíbles, por lo que merece un estándar adecuado, el ERC-721. El valor de un token ERC-721 se puede definir por su rareza, así como por propiedades particulares. (de Figuereido 2021)

El ERC-721 define una interfaz mínima que debe implementar un *smart contract* para permitir la gestión, la propiedad y el comercio de tokens únicos. No impone un estándar para los metadatos de los tokens ni restringe la adición de funciones suplementarias. Proporciona funcionalidades como transferir tokens de una cuenta a otra, obtener el saldo actual de tokens de una cuenta, comprobar el propietario de un token específico y también el suministro total del token disponible en la red. Además de esto, también tiene otras funcionalidades como aprobar que una cantidad de tokens de una cuenta pueda ser movida por una cuenta de terceros. Si un *smart contract*s implementa los siguientes métodos y eventos puede llamarse un ERC-721 Non-Fungible Token Contract y, una vez desplegado, será responsable de llevar el control de los tokens creados en Ethereum. (Ethereum.org 2021)

Los NFT´s fueron los responsables de la mayor parte de la adopción de Ethereum durante 2021, ya que artistas, atletas y celebridades se sumaron en el espacio, otorgando gran visibilidad a la industria. Después de alcanzar 633 millones de dólares en volumen de operaciones durante la primera mitad del año, el volumen de operaciones de OpenSea -principal *marketplace* de NFT´s- superó los 3.000 millones de dólares tanto en agosto como en diciembre. Con un total de $8.26 billones (americanos) en volumen durante el cuarto cuatrimestre. (Coindesk 2021)

Ilustración 9: OpenSea NFT trade volume



Fuente: *"2021 Annual Review"* CoinDesk (2021)

El token ERC-1155 es un nuevo tipo de token estándar dentro de Ethereum con capacidad

para cambiar el panorama de las dApps -*descentralized applications* o aplicaciones descentralizadas- dentro de esta *blockchain*, gracias a su capacidad "multitoken" y a un nuevo número de funciones diseñadas para proporcionar una mejor experiencia de usuario y programación.

Como se comentaba anteriormente, Ethereum implementa tokens estándares para facilitar el desarrollo de *smart contract*s. Uno de los últimos estándares lanzados por Ethereum es el ERC-1155.

Con este estándar, Ethereum, habilita a este tipo de token a funcionar a modo de custodio de otro tipo de tokens como el ERC-721 o ERC-20. Esto además habilita a este nuevo estándar de token a funcionar al mismo tiempo bajo los estándares de ERC-721 y ERC-20.

El token ERC-1155 se describe en una EIP (Propuesta de Mejora de Ethereum), más concretamente en la EIP-1155, de la que deriva su nombre. Este estándar fue desarrollado por Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet y Ronan Sandford. (EIPS Ethereum.org 2018)

Ethereum solventa con este estándar, problemas de los estándares mencionados previamente. Por ejemplo, en ERC-20, son numerosos los casos tanto de novatos como de expertos que han perdido sus criptodivisas por equivocarse en la dirección de envío, al ser esta irreversible, son irrecuperables. Incluso Vitalik Buterin, el mismo fundador de Ethereum, realiza transacciones de comprobación antes de transferir cripto entre *wallets*.

Por el otro lado, los tokens ERC-721 son conocidos por sus limitaciones a la hora de transferirlos entre cuentas. Cada token ERC-721 debe ser transferido en transacciones individuales. No pudiendo enviar, por ejemplo, un lote de cinco NFT´s en una única transacción. Lo que conlleva un elevado coste en comisiones de envío, entre otros factores, debido a la congestión de la red. Otra ineficiencia de estos tokens es el proceso de autentificación que siguen para verificar el estado de tu token dentro de la red a la que pertenece. Así que, si tu NFT pertenece a una colección de 100.000 tokens no fungibles, el sistema debe mandar una transacción a toda la red para trazar el NFT sobre el que se

ha solicitado la comprobación.

A esto debemos añadir que los estándares ERC-20 y ERC-721 son incompatibles entre sí. De hecho, los contratos son tan distantes que añadir una funcionalidad para conectarlos es una tarea abrumadora que, casi con toda seguridad, tendría un impacto negativo en la red, provocaría posibles fallos y daría lugar a elevadas comisiones.

Esto es crítico porque muchas dApps utilizan ambos tipos de tokens, y como resultado de esta limitación, la lógica de su funcionamiento se vuelve más compleja. Si un único *smart contract* pudiera gestionar todo, sería significativamente más fácil de programar, más seguro y menos complejo de diseñar.

ERC-1155 se ha creado como puente, bajo el mismo *smart contract*, entre los dos estándares explicados anteriormente. Bajo el mismo *smart contract*, ahora podemos transferir una mayor cantidad de ERC-721 (NFT´s) y generar ERC-20 por ejemplo. Con ello descongestionamos la red y ahorramos en comisiones de envío.

Otra funcionalidad dentro del token ERC-1155 es la capacidad de integrar la funcionalidad del ERC-165 (conocida como, Standard Detection), todo dentro del mismo sistema. De este modo, el token ERC-1155 es capaz de detectar la interfaz del token y adaptar su comportamiento en función de la misma. Esto es especialmente útil debido a la naturaleza multitoken del ERC-1155 y simplifica el diseño de las aplicaciones.

Quizá una de las características más prometedoras del token ERC-1155 sea la transferencia segura de tokens. Para ello, el *smart contract*s estándar ERC-1155 incluye una función que verifica que la transacción se ha llevado a cabo, y si no, la revierte para devolver el control de los tokens a su emisor. Esto es crucial para la adopción de cripto, si el fin es que sea utilizada en el día a día por el público general sin conocimientos sobre la tecnología, se debe afrontar que fallos en las transacciones se pueden cometer y proteger al usuario con iniciativas como las de Ethereum son un gran paso de cara a hacer *crypto* más *user-friendly*. Pues ni el UX (experiencia de usuario) ni el UI (interfaz de usuario) de *crypto* a día de hoy están adaptados para el público general.

b. Smart Contracts

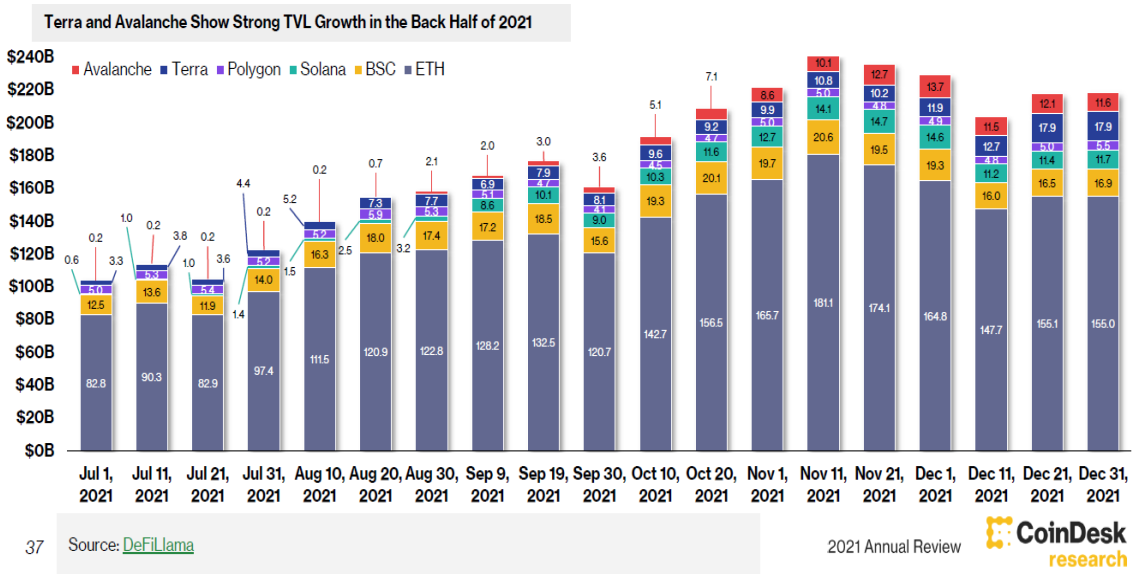
El potencial de los *smart contracts* o contratos inteligentes en español -contratos programables que se ejecutan automáticamente cuando se cumplen unas condiciones predefinidas- ha generado un considerable debate y discusión en el sector de los servicios financieros. (Ethereum.org 2022)

Los contratos inteligentes, que se basan en la tecnología *blockchain* o de libro mayor distribuido (DLT por sus siglas en inglés), han sido aclamados como la panacea para resolver una serie de problemas asociados a los contratos financieros tradicionales, que simplemente no están diseñados para la era digital. (Peyrott 2017)

La dependencia de los documentos físicos provoca retrasos e ineficiencias, así como un mayor riesgo de error y fraude. Aunque los intermediarios financieros mejoran la interoperabilidad del sistema financiero y reducen el riesgo, aumentan los gastos generales y los requisitos de cumplimiento. (Preukschat 2017)

Aunque hay otras *blockchain*s que utilizan *smart contract*s como Avalanche, Polygon, Solana, Binance Smart Chain o Terra, el estudio se centrará en Ethereum pues es el ecosistema sobre el que la mayor parte de proyectos de DeFi se están desarrollando. La adopción de DeFi incrementó en el último cautrimestre de 2021 en $17.85 billion en TVL (Total Value Locked) -valor global de los criptoactivos depositados en DeFi.

Ilustración 10: Crecimiento en TVL de las principales blockchains



Fuente: "*CoinDesk 2021 Annual Review"* CoinDesk (2021)

El componente central de Ethereum son sus *smart contract*s. Son capaces de codificar cualquier algoritmo. Los contratos inteligentes pueden almacenar cualquier tipo de datos y realizar cualquier tipo de cálculo. Incluso pueden invocar otros contratos inteligentes. Esto hace a Ethereum, extraordinariamente flexible a la hora de desarrollar soluciones.

La adopción de los contratos inteligentes dará lugar a una reducción de los riesgos, de los costes de administración y de los servicios, y a unos procesos empresariales más eficientes en los principales segmentos del sector de los servicios financieros. Estos beneficios se acumularán como resultado de los avances tecnológicos, el rediseño de procesos y los cambios fundamentales en los modelos operativos, ya que todos ellos requieren que un grupo de empresas comparta un entendimiento común del contrato entre las partes comerciales. Los consumidores se beneficiarán de productos más competitivos, como los ofrecidos por DeFi, así como de procesos simplificados que eliminan muchas de las molestias asociadas a la experiencia del cliente moderno. (Preukschat 2017)

Este contexto de sistema fragmentado e ineficiente ayuda a explicar por qué *blockchain* y los contratos inteligentes están generando tanto interés. En su forma más simple, los contratos inteligentes son contratos que también pueden realizar algunas de las funciones

del contrato. Y cuando estos contratos inteligentes se despliegan en una *blockchain* o libro mayor distribuido, adquieren permanencia e inmutabilidad. (Capgemini 2020)

Según Ethereum.org un *smart contract* es simplemente un programa que se ejecuta en la *blockchain* de Ethereum. Es una colección de código (sus funciones) y datos (su estado) que reside en una dirección específica en la *blockchain* de Ethereum. (Ethereum.org 2022)

Los *smart contracts* son un tipo de cuenta de Ethereum. Esto significa que tienen un saldo y pueden enviar transacciones a través de la red. Sin embargo, no son controlados por un usuario, sino que se despliegan en la red y se ejecutan según lo programado. Las cuentas de usuario pueden entonces interactuar con un ellos enviando transacciones que ejecutan una función definida en el *smart contract*. Éstos pueden definir reglas, como un contrato normal, y aplicarlas automáticamente a través del código. Éstos no pueden ser eliminados por defecto, y las interacciones con ellos son irreversibles. (Ethereum.org 2022)

Un aspecto fundamental del funcionamiento de los *smart contract*s en Ethereum es que cada uno de ellos tiene su propia dirección de *blockchain*. En otras palabras, el código del contrato no está contenido en las transacciones que lo utilizan. (Capgemini 2020)

Como se explica en "Intro to Ethereum" a diferencia de Bitcoin, Ethereum utiliza un algoritmo diferente para determinar qué bloques deben añadirse a la cadena de bloques válida. Mientras que el *blockchain* de Bitcoin es siempre la cadena más larga de bloques válidos, Ethereum utiliza un protocolo llamado GHOST (de hecho, una variación del mismo). (Peyrott 2017)

El protocolo GHOST permite integrar en la cadena de bloques los bloques antiguos, es decir, los bloques calculados por otros nodos pero descartados porque otros han calculado bloques más nuevos, reduciendo así la potencia de cálculo desperdiciada y aumentando los incentivos para los nodos más lentos. Además, permite una confirmación más rápida de las transacciones: mientras que los bloques de Bitcoin suelen crearse cada diez minutos, los de Ethereum se crean en segundos. Se ha debatido mucho sobre si este protocolo supone una mejora con respecto al protocolo de Bitcoin, mucho más sencillo y

de "cadena más larga", pero este debate está fuera del tópico de este trabajo. Por el momento, este protocolo parece funcionar con éxito en Ethereum. (Peyrott 2017)

Como se explicaba anteriormente, un aspecto importante de cómo funcionan los *smart contract*s en Ethereum es que tienen su propia dirección en la cadena de bloques. En otras palabras, el código del contrato no se lleva dentro de cada transacción que hace uso de él. Esto se convertiría rápidamente en algo difícil de manejar. En su lugar, un nodo puede crear una transacción especial que asigna una dirección a un contrato. Esta transacción también puede ejecutar código en el momento de la creación. (Ethereum.org 2022)

Después de esta transacción inicial, el contrato pasa a formar parte de la cadena de bloques para siempre y su dirección nunca cambia. Cuando un nodo quiere llamar a alguno de los métodos definidos por el contrato, puede enviar un mensaje a la dirección del contrato, especificando los datos de entrada y el método que debe llamar. El contrato se ejecutará como parte de la creación de nuevos bloques hasta el límite de gas o finalización. Los métodos del contrato pueden devolver un valor o almacenar datos. Estos datos forman parte del estado de la *blockchain*. (Ethereum.org 2022)

Los *smart contract*s se implementan utilizando Ethereum Virtual Machine, que se instala en cada nodo. Aunque es extremadamente potente, Ethereum Virtual Machine funciona a un nivel lo suficientemente bajo como para que no sea conveniente programarla directamente (como la mayoría de los *Virtual Machines*). Por ello, se han desarrollado varios lenguajes de escritura de contratos. Solidity es el más popular de ellos.

Solidity es un lenguaje de programación similar a JavaScript que fue creado específicamente para el desarrollo de los *smart contracts* de Ethereum. El compilador de Solidity convierte este código en bytecode de Ethereum Virtual Machine, que luego puede enviarse como una transacción a la red de Ethereum y se le asigna su propia dirección.

Para entender mejor Solidity, se extra este ejemplo de Intro to Ethereum:

Ilustración 11: Ejemplo código en Solidity

```
pragma solidity ^0.4.2;

contract OwnerClaims {

    string constant public defaultKey = "default";

    mapping(address => mapping(string => string)) private owners;

    function setClaim(string key, string value) {
        owners[msg.sender][key] = value;
    }

    function getClaim(address owner, string key) constant returns (string) {
        return owners[owner][key];
    }

    function setDefaultClaim(string value) {
        setClaim(defaultKey, value);
    }

    function getDefaultClaim(address owner) constant returns (string) {
        return getClaim(owner, defaultKey);
    }

}
```

Fuente: "*Introduction to Ethereum and smart contracts*", Sebastian E. Peyrott (2017)

Se trata de un simple contrato de reclamación de propietarios. Un contrato de reclamación de propietario es un contrato que permite a cualquier propietario de una dirección registrar datos de valor clave arbitrarios. La naturaleza de la cadena de bloques certifica que el propietario de una determinada dirección es el único que puede establecer reclamaciones en relación con esa dirección. En otras palabras, el contrato de reclamaciones del propietario permite a cualquiera que quiera realizar transacciones con una de sus direcciones comprobar sus afirmaciones. Por ejemplo, puede crear una afirmación llamada "correo electrónico" que permita a cualquiera que desee hacer negocios con usted obtener su dirección de correo electrónico. Esto es ventajoso porque una dirección de Ethereum no está asociada a una identidad (o dirección de correo electrónico), sino a su

clave privada. (Peyrott 2017)

El contrato es lo más sencillo posible. Para empezar, está la palabra clave del contrato, que indica el comienzo de un contrato. A continuación, está *OwnerClaims*, el nombre del contrato. Hay dos tipos de elementos en un contrato: variables y funciones.

Hay dos tipos de variables: las constantes y las variables escritas. Las constantes son inmutables. Sin embargo, las variables escritas almacenan el estado en la cadena de bloques. Estas variables, y nada más, se utilizan para almacenar el estado de la cadena de bloques.

Las funciones son fragmentos de código capaces de leer o modificar el estado. Además, las funciones de sólo lectura se marcan en el código como constantes y no requieren gas para ejecutarse. Por otro lado, las funciones que cambian el estado consumen gas, ya que las transiciones de estado deben codificarse en nuevos bloques de la cadena de bloques (y su producción cuesta trabajo). La persona que llama recibe los valores devueltos por las funciones.

En nuestro contrato, la variable propietaria es un mapa, también conocido como matriz asociativa o diccionario. Asocia una clave con un valor. La clave en este caso es una dirección. En Ethereum, las direcciones sirven como identificadores de las cuentas normales (que suelen ser gestionadas por los usuarios) o de otros contratos. Cuando el propietario de una dirección decide presentar una reclamación, nos interesa el mapeo entre la dirección y la reclamación. De hecho, no estamos mapeando una dirección a una reclamación, sino a una colección de valores-clave que comprenden una colección de reclamaciones (en forma de otro mapa). Esto es ventajoso porque el propietario de una dirección puede querer revelar varios detalles sobre sí mismo a otros. En otras palabras, los propietarios de direcciones pueden querer hacer públicas su dirección de correo electrónico y su número de teléfono móvil. Podrían lograrlo creando dos reclamaciones: una bajo la clave "correo electrónico" y otra bajo la clave "teléfono".

Como el contrato deja que cada propietario decida qué entradas crear, los nombres de las claves se desconocen de antemano. Por ello, existe una clave especial "por defecto", para

que cualquier lector que no esté familiarizado con las claves disponibles reconozca al menos una reclamación. En realidad, esta clave también está ahí por otra razón: Solidity hace imposible devolver grandes cantidades de datos desde las funciones. En otras palabras, devolver todas las reclamaciones asociadas a una dirección en una sola llamada de función no es trivial. De hecho, el tipo de mapeo carece de una operación de iteración (aunque se puede codificar una si es necesario), lo que hace imposible determinar qué claves están contenidas en un mapeo. (Solidity 2022)

Un aspecto por estudiar de los protocolos de cadena de bloques es su aislamiento del mundo más allá de su libro de contabilidad. Es decir, la cadena de bloques de Ethereum sólo tiene autoridad sobre lo que ocurre en la cadena de bloques de Ethereum, no sobre lo que ocurre a su alrededor. Si nuestro *smart contract* está programado para actuar en base a lo que ocurra en el mundo real, debemos proporcionar esta información a nuestro *smart contract*. Esta restricción restringe las aplicaciones a los contratos y tokens nativos de Ethereum, reduciendo la utilidad de la plataforma, y se conoce comúnmente como el problema del oráculo. Un oráculo es cualquier fuente de datos que reporta información externa al *blockchain* en el contexto de las plataformas de *smart contracts*. Construir un oráculo que pueda hablar con autoridad sobre los datos fuera de la cadena y al mismo tiempo ser de confianza es un problema por resolver. Numerosas aplicaciones requieren el uso de un oráculo, y las implementaciones varían en su grado de centralización. (Chainlink 2021)

Los oráculos se implementan en una variedad de aplicaciones DeFi. Una estrategia común es que una aplicación albergue su propio oráculo o se conecte a un oráculo existente a través de una plataforma de confianza.

Un proyecto en el ecosistema *crypto* que trata de dar solución a este problema es Chainlink, una plataforma basada en Ethereum, está diseñada para abordar el problema del oráculo mediante la agregación de fuentes de datos. El artículo técnico de Chainlink describe un sistema basado en la reputación no implementado. Los oráculos son, sin duda, un problema de diseño no resuelto y una barrera para que DeFi alcance una utilidad más allá de su propia cadena aislada. (Chainlink 2021)

c. DeFi

Cuando los costes son elevados, la innovación surgirá para capitalizar las ineficiencias. Sin embargo, la innovación puede ser frenada por una poderosa capa de intermedios.

La infraestructura financiera heredada ha limitado las oportunidades de crecimiento y ha exacerbado la desigualdad de oportunidades. Alrededor de 1.700 millones de personas en todo el mundo no están bancarizadas. Las pequeñas empresas, incluso las que tienen una relación bancaria, a menudo deben recurrir a una financiación de alto coste, como las tarjetas de crédito, porque no pueden optar a la financiación de préstamos a través de la banca tradicional. Los altos costes también afectan a los minoristas, que pierden un 3% por cada transacción con tarjeta de crédito. Desde cualquier punto de vista, estos costes totales para las pequeñas empresas son enormes. Como resultado, la inversión disminuye y el crecimiento económico se ralentiza. Las finanzas descentralizadas, o DeFi, son una alternativa frente al sistema actual y ofrecen una serie de soluciones potenciales a los problemas inherentes a la infraestructura financiera tradicional. Aunque existen numerosas iniciativas de *fintech*, las que incorporan la infraestructura bancaria existente tienen más probabilidades de ser transitorias. Las iniciativas que emplean métodos descentralizados -en concreto, la tecnología *blockchain*- son las que tienen más posibilidades de definir el futuro financiero. (Kraken 2021)

Descentralized Finance – DeFi – (Finanzas descentralizadas en español) hace referencia a la evolución de las finanzas tradicionales, sistemas financieros centralizados, a finanzas *peer-to-peer* habilitadas por *blockchains* como la de Ethereum. Desde su nacimiento en 2013 y lanzamiento en 2015, Ethereum combina el código abierto y la infraestructura financiera de Bitcoin, con una funcionalidad mayor y más flexible gracias a la introducción de los *smart contracts*. De esta manera los intermediarios financieros centralizados son sustituidos por aplicaciones descentralizadas o dApps. Con el objetivo de solucionar los cinco principales problemas de las finanzas tradicionales: control centralizado, acceso limitado, ineficiencia, falta de interoperabilidad y opacidad. (Harvey & Santoro 2020)

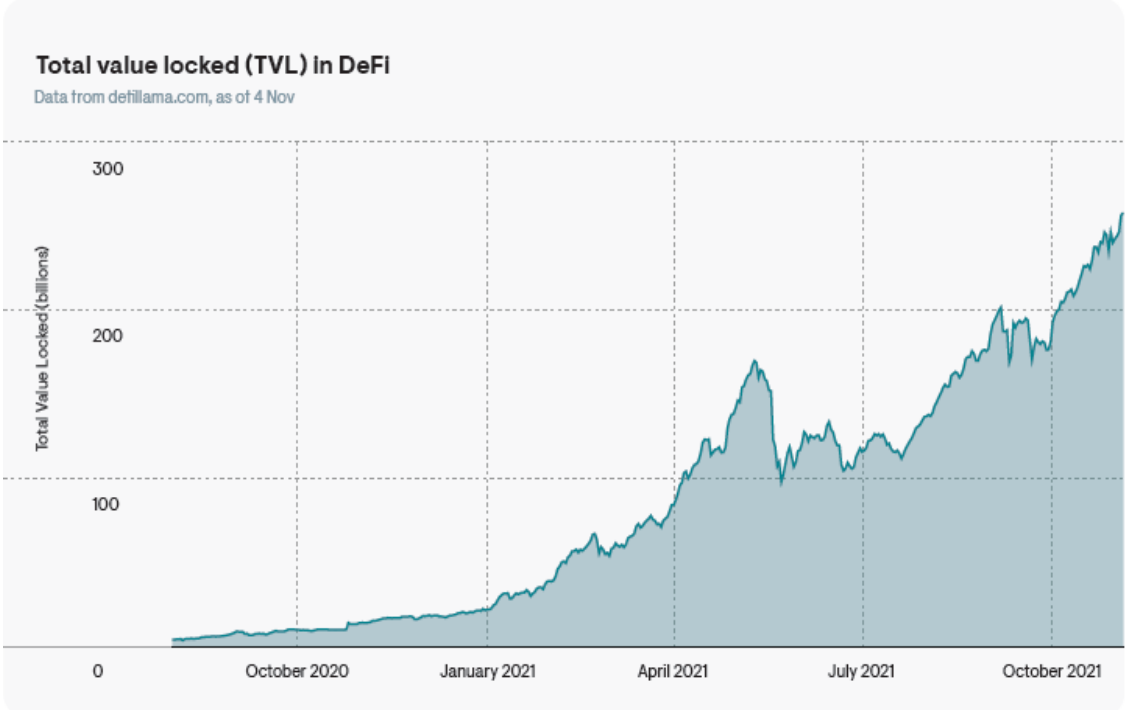
DeFi utiliza la tecnología *blockchain* para desarrollar y combinar bloques de código abierto en sofisticados productos financieros con mínima fricción y máximo valor para los usuarios. DeFi es fundamentalmente un mercado de aplicaciones financieras descentralizadas que ofrecen productos financieros como el intercambio, el ahorro, los préstamos y *tokenization*- proceso de sustitución de un elemento de datos sensibles por uno que no es sensible, es decir que no tiene valor explotable-. Estas aplicaciones se benefician de los efectos de red asociados a la combinación de productos DeFi, atrayendo así una parte creciente de la cuota de mercado del ecosistema financiero tradicional. (Zetzsche, Arner & Buckley 2020)

DeFi ha emergido como el sector más activo en el ecosistema *crypto*. Con un amplio rango de casos de uso para instituciones, particulares y desarrolladores.

Bitcoin fue originalmente concebido en 2008 como una alternativa para suprimir intermediarios financieros. Daba acceso a cualquier persona a un sistema de pagos sin la necesidad de terceros del tipo de un banco. Sin embargo, Bitcoin no ha conseguido establecerse como método de pago principal hoy en día en parte por sus problemas de escalabilidad, volatilidad y su limitada funcionalidad. Los sistemas de pago constituyen solamente una parte de un sistema financiero. El intercambio y *lending* de Bitcoin sigue controlado por entidades centrales, de manera similar al sistema financiero tradicional. (Harvey & Santoro 2020)

En los últimos dos años el panorama DeFi ha proliferado, con dApps ofreciendo *descentralized lending & borrowing, exchange, asset management, margin trading, payment products,* derivados*, insurance, margin trading* y similares han ido ganando tracción. En especial en las nuevas formas de invertir como son *staking* y *yield farming.* El valor total bloqueado o TVL por sus siglas en inglés, ha aumentado de $500 millones en noviembre de 2019 a $247 billones en noviembre de 2021. (Elliptic 2022)

Ilustración 12: TVL en DeFi



Fuente: "*The Elliptic 2022 DeFi Report*" Elliptic (2022)

Total Value Locked o TVL hacer referencia al valor total de activos cripto depositados en protocolos de DeFi. Ha emergido como una métrica crucial para analizar este sector en la industria crypto. TVL incluye todas las criptodivisas depositadas en funciones como *staking*, *lending* o *liquidity protocols*. Cabe destacar que este valor no refleja el *yield* que se espera de estos depósitos. Únicamente, el valor actual de éstos.

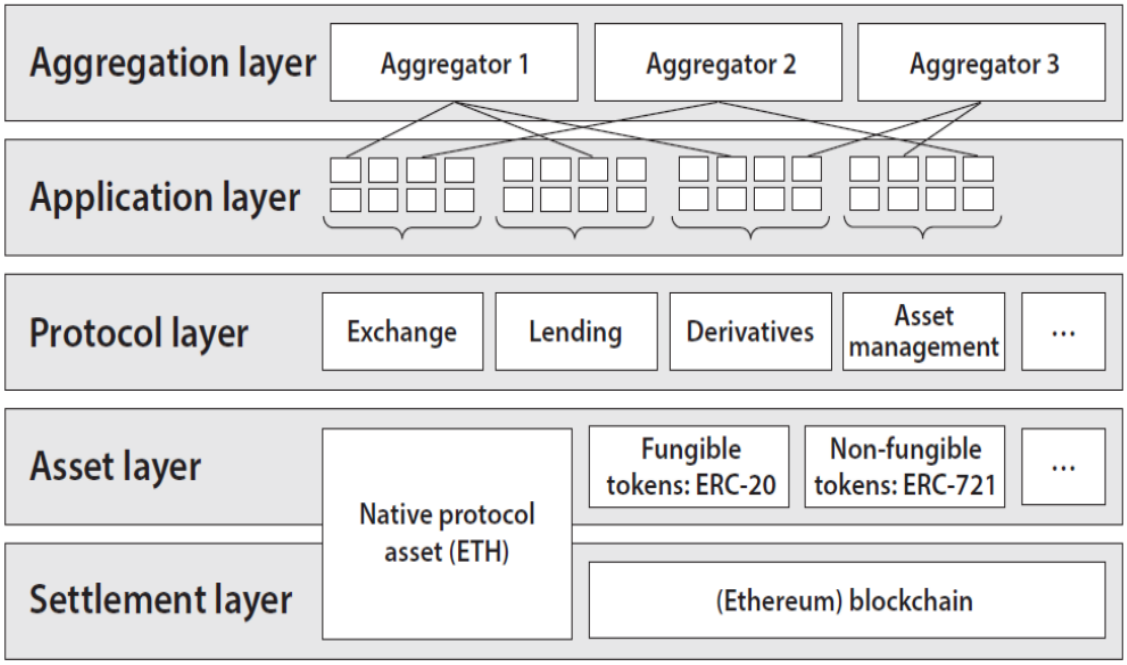
El TVL de un proyecto no cambia únicamente como resultado de nuevos depósitos o retiros. Cambia constantemente al ritmo del valor en dólares de todas las criptomonedas. Una parte, o incluso la totalidad, de los depósitos de un protocolo DeFi pueden estar denominados en el token nativo del protocolo. Cuando el token nativo del protocolo se aprecia en valor, el TVL del protocolo aumenta proporcionalmente. (Elliptic 2022)

Los inversores pueden utilizar la TVL para determinar si el token nativo de un proyecto DeFi se valora adecuadamente. La capitalización de mercado del token puede ser alta o

baja en comparación con el TVL del proyecto. Cuanto más extrema sea la relación, más sobrevalorado o infravalorado parecerá el token.

DeFi ha otorgado a los usuarios una mejor manera de generar y operar con *passive income*. Los *centralized exchanges* (CEX) eran anteriormente la única manera de operar con *digital assets* -activo digital. Esto traía consigo inconvenientes para el usuario como el control sobre las *private keys "not your keys, not your crypto"* (haciendo referencia al control del *exchange* sobre el acceso a tu *wallet*), los parámetros de trading, información del usuario y la seguridad del fondo. Además, no había manera de generar *passive income* sobre tu porfolio, siendo la exposición a la fluctuación del *asset* en el mercado la única manera de incrementar el valor de tu porfolio.

Ilustración 13: DeFi Stack



Fuente: "*Introduction to Fintech*" Tetyana B. (2022)

El auge de DeFi mantiene el espíritu de confianza de las criptomonedas, reformando un ecosistema estancado que había sucumbido al control centralizado. La introducción de intercambios descentralizados (*decentralized exchanges* o DeX) basados en el modelo de

creador de mercado automatizado (AMM) fue un avance significativo. Esto niveló el campo de juego al permitir el comercio sin restricciones al estilo de las criptomonedas, con total anonimato y una rápida liquidación.

Los *centralized exchanges* han mantenido su ventaja debido a su facilidad de uso y a las herramientas profesionales de negociación, ambas integradas en la interfaz de negociación basada en el libro de órdenes. Aunque la negociación descentralizada ha crecido en popularidad en los últimos años, se trata de un proceso completamente diferente al de los libros de órdenes de *centralized exchanges* que a día de hoy siguen siendo las plataformas líderes para los usuarios como "*on-ramp*" para convertir fiat a crypto. (Elliptic 2022)

Los incentivos desempeñan un papel fundamental a la hora de promover los comportamientos deseados (incentivos positivos) y desalentar los indeseables (incentivos negativos) de los usuarios en los sistemas criptoeconómicos, incluido DeFi. Aunque el término "incentivo" es bastante amplio, nuestra discusión se centrará en los pagos directos de tokens o *fees*. Examinaremos dos tipos distintos de incentivos: los *staked* y los directos. Los incentivos *staked* se aplican al saldo de tokens en la custodia de un *smart contract*. Los incentivos directos están disponibles para los usuarios del sistema que no tienen un saldo en custodia. (Harvey & Santoro 2020)

Los mecanismos del contrato especifican el origen de los fondos de recompensa y el destino de las comisiones. Los fondos de recompensa pueden ser emitidos a través de la inflación o *minting* (minar, pero en sistema de consenso PoS) y pueden ser custodiados en el *smart contract*s. Los fondos extraídos como comisión pueden ser *burn*ed (un mecanismo puede iniciar una quema para reducir la oferta de un token en particular y así ejercer una presión al alza sobre su precio) o retenidos en la custodia del *smart contract*. Además, los fondos de recompensa pueden distribuirse directamente a los participantes de la plataforma o recaudarse a través de una subasta para pagar una deuda.

Los *staking rewards* son un tipo de incentivo positivo en el que un usuario recibe una bonificación en su saldo de tokens a cambio de su inversión en el sistema. Existen numerosos verticales para la personalización de los incentivos: (Harvey & Santoro 2020)

- Requisitos de apuesta opcionales:
    - Umbral mínimo entre todos los saldos apostados.
- Opciones de remuneración:
    - Remuneración fija o “pro-rata” (proportionally)
    - Tipo de token idéntico al apostado o un tipo de token distinto

El protocolo Compound recompensa a los usuarios por apostar sus saldos mientras se encuentran en posición de préstamo o de crédito. Estas recompensas se pagan en un token separado (COMP), que se financia con COMP custodiados y tiene un suministro fijo, y se aplican a pro-rata a todos los saldos apostados.

Otro protocolo, denominado Synthetix paga las recompensas de las apuestas en su token nativo, SNX, el token del protocolo de suministro limitado. Las recompensas, están financiadas por la inflación, y sólo se emiten si el usuario cumple con un cierto nivel de garantía.

Las recompensas directas son incentivos positivos que vienen en forma de pagos o tarifas por las acciones del usuario. Todas las interacciones de Ethereum comienzan con una transacción, que se inicia con una cuenta de propiedad externa. Independientemente de si está controlada por un usuario humano o por un *bot* fuera de la cadena, una *externally owned account* (EOA) está (críticamente) fuera de la cadena, y por tanto la supervisión autónoma del mercado es prohibitiva (cuesta gas) o técnicamente imposible. Como resultado, ninguna transacción se produce automáticamente en Ethereum a menos que se inicie deliberadamente. (Harvey & Santoro 2020)

El ejemplo clásico de una transacción que debe iniciarse es cuando una posición de deuda colateralizada se convierte en subcolateralizada. Este caso de uso no da lugar automáticamente a una liquidación; el EOA debe hacerlo. Para este y otros casos de uso,

los EOA suelen ser compensados directamente por la iniciación del contrato. Después, el contrato evalúa las circunstancias y liquida o actualiza el contrato si todo es como se espera.

Un *keeper* es un tipo de EOA que es recompensado por realizar una acción dentro del protocolo DeFi u otra dApp. Un *keeper* es compensado en forma de una tarifa plana o un porcentaje de la acción incentivada. Con los incentivos adecuados, el seguimiento autónomo puede ser *off-chained*, lo que resulta en economías robustas y nuevas oportunidades de beneficio. Además, las recompensas de los *keepers* pueden estructurarse como una subasta para garantizar la competencia y el mejor precio. Las subastas de *keepers* son extremadamente competitivas, ya que los datos del sistema son casi totalmente públicos. Las recompensas directas para los *keepers* tienen la consecuencia no deseada de inflar los precios del gas como resultado de la competencia por estas recompensas. Es decir, el aumento de la actividad de los poseedores provoca un aumento de la demanda de transacciones, lo que hace subir el precio del gas. (Harvey & Santoro 2020)

Las tasas suelen utilizarse para financiar las características del sistema o de la plataforma. Pueden programarse como fijas o en porcentaje, dependiendo del incentivo deseado. Las tasas pueden imponerse directamente o acumularse sobre los saldos *staked*. Las comisiones acumuladas deben ir acompañadas de un saldo *staked* para garantizar que sean pagadas por el usuario. Dado que las cuentas de Ethereum son pseudónimas y anónimas -todo lo que se sabe de un usuario de Ethereum es el saldo de su cartera y las interacciones con varios contratos de Ethereum. Esto puede consultarse en Etherscan-, la imposición de comisiones es un reto para el diseño. Si el *smart contract* es accesible a cualquier dirección de Ethereum, la única manera de garantizar la ejecución fuera de la cadena o la intervención legal es que todas las deudas estén respaldadas por una garantía transparente y ejecutable. Debido a las dificultades que plantea el anonimato, otros mecanismos, como la reputación, no son sustitutos adecuados de los saldos *staked*. (Wharton 2021)

Los *swaps* no son más que el intercambio de un tipo de token por otro. La principal ventaja de realizar el *swap* en DeFi es que no es custodiado. Los fondos pueden

mantenerse en un *smart contract* que incluya derechos de retirada que pueden ser ejercidos en cualquier momento antes de la finalización del *swap*. Si el canje no tiene éxito, todas las partes conservan la custodia de sus fondos. El intercambio sólo tendrá lugar si todas las partes están de acuerdo y cumplen las condiciones de intercambio, que se hacen cumplir mediante el *smart contract*. Si alguna condición no se cumple, la transacción se cancela automáticamente. Un intercambio descentralizado (DEX) es una plataforma que permite el intercambio de tokens no custodiados en Ethereum. Hay dos mecanismos principales de liquidez para el DEX: *order-matching* y un creador de mercado automatizado o AMM por sus siglas en inglés. (Harvey & Santoro 2020)

La conciliación del libro de órdenes es una estrategia de cobertura en la que todas las partes deben acordar el tipo de cambio. Los creadores de mercado pueden presentar ofertas y demandas a un DEX y permitir a los tomadores que ocupen las cotizaciones al precio negociado de antemano. Hasta que la oferta es aceptada, el creador de mercado se reserva el derecho de retirarla o de actualizar el tipo de cambio en respuesta a las cambiantes condiciones del mercado. (KPMG 2021)

Dado que cada actualización requiere una transacción en la cadena, el enfoque de la correspondencia de órdenes es costoso e ineficiente. Una ineficiencia fundamental de la casación de órdenes es que ambas partes deben estar dispuestas y ser capaces de intercambiar al tipo de cambio acordado para que la operación se ejecute. Este requisito impone limitaciones a un gran número de aplicaciones de *smart contract*s en las que la demanda de liquidez de intercambio no puede depender de la disponibilidad de una contraparte. Una alternativa de vanguardia es un Creador de Mercado Automatizado (AMM). (KPMG 2021)

Un Creador de Mercado (AMM) es un *smart contract* que mantiene activos en ambos lados de un par comercial y cotiza un precio de compra y venta continuamente. El contrato actualiza el tamaño del activo detrás de los precios de oferta y demanda basándose en las compras y ventas ejecutadas y utiliza esta relación para definir su función de fijación de precios. Además, el contrato puede considerar datos más complejos que sólo el tamaño relativo de la oferta y la demanda a la hora de determinar el precio. Desde el punto de vista del contrato, el precio debe ser neutral al riesgo, es decir, debe ser independiente de

si el contrato se compra o se vende. (KPMG 2021)

Un AMM "ingenuo" podría utilizar una relación de precios fija para determinar el valor relativo de dos activos. Cuando el precio de mercado de los activos varía, el activo más valioso se retira del AMM y se arbitra en otra bolsa donde se negocia a precio de mercado. El AMM debe tener una función de fijación de precios que pueda converger con el precio de mercado de un activo, de forma que la compra de un activo del par de negociación se encarezca a medida que disminuya la relación del activo con los demás activos del contrato. (Harvey & Santoro 2020)

Las principales ventajas de un AMM son su disponibilidad constante y la ausencia de la necesidad de una contraparte tradicional para ejecutar una operación. Estas disposiciones son fundamentales para el desarrollo de *smart contract*s y DeFi porque garantizan que un usuario pueda intercambiar activos en cualquier momento y a cualquier hora si es necesario. Dado que el usuario conserva la custodia de sus fondos hasta que se complete la operación, no hay riesgo de contrapartida. Además, la *composoble liquidit*y es una ventaja, ya que permite a cualquier contrato de intercambio aprovechar la liquidez y los tipos de cambio de otro contrato de intercambio. (Harvey & Santoro 2020)

Una de las desventajas de un AMM es el concepto de *impermanent loss*, que se refiere a la dinámica de coste de oportunidad que existe entre la oferta de activos para el intercambio y la tenencia de los activos subyacentes para beneficiarse del movimiento de los precios. La pérdida es transitoria, ya que puede recuperarse si el precio vuelve a su nivel inicial. (Elliptic 2022)

El *impermanent loss* se produce cuando el contrato está estructurado para vender el activo que se aprecia y comprar el activo que disminuye. La independencia de la trayectoria es una propiedad crítica del *impermanent loss*. En este caso, da igual que uno o cien operadores consuman toda la liquidez. Independientemente de la cantidad de operaciones o de su dirección, el tipo de cambio final y las relaciones de los activos contratados dan lugar a la misma pérdida temporal. Debido a la independencia de las rutas, la pérdida temporal en los pares de operaciones con precios asociados se minimiza (pares de reversión media). En consecuencia, los pares de negociación de *stablecoins* son muy

atractivos para los AMM. (Elliptic 2022)

La excesiva volatilidad es una debilidad crítica de las criptodivisas. Esto crea dificultades para los clientes que quieren utilizar aplicaciones DeFi pero carecen de la tolerancia al riesgo requerida para una criptodivisa volátil como ETH. Las *stablecoins*, un nuevo tipo de criptodivisa, han surgido para solucionar este problema. Las *stablecoins* están diseñadas para preservar la paridad con un determinado activo, como el dólar estadounidense o el oro. Las *stablecoins* ofrecen a los inversores la estabilidad necesaria para participar en una variedad de aplicaciones DeFi y permiten una solución nativa de la criptodivisa para liquidar las participaciones en criptoactivos más volátiles. El tipo más común de *stablecoin* es el que está colateralizado por dinero en efectivo. Estas están garantizadas por una reserva fuera de la cadena del activo subyacente. Normalmente, están en manos de una empresa o conjunto de empresas externas que se someten a auditorías periódicas para garantizar la existencia de la garantía. Tether es la mayor *stablecoin* respaldada por fiat que a fecha de escritura de este trabajo tiene una capitalización de mercado de $81.7 billion (en billones americanos) y es la tercera criptodivisa por capitalización de mercado, detrás de Bitcoin con una capitalización de mercado de $857 billion y Ethereum con $393.6 billion. (Coingecko 2022)

El modelo AMM hace posible el comercio utilizando *pools* de liquidez, o colecciones de tokens de criptomonedas, a través de un algoritmo que establece los precios de los tokens en función de la proporción cambiante de tokens suministrados. Los creadores de mercado, o proveedores de liquidez (LP), son los que proporcionan liquidez a las *pools* en forma de activos digitales. A cambio, se les compensa con comisiones de negociación proporcionales a la cantidad de liquidez aportada inicialmente. Para acceder a una *pool*, hay que destacar que se debe proveer de una cantidad idéntica por token. Es decir, para una pool de BTC/USDT se debe proveer $1000 de cada. (KMPG 2021)

Las *flash loans* son una de las revoluciones de DeFi más interesantes. Una *flash loan* es específica de DeFi, amplía significativamente ciertas formas de financiación. En las finanzas convencionales, un préstamo es un instrumento financiero utilizado para transferir eficazmente el dinero sobrante de una persona o entidad que pretende emplearlo (prestamista) a una persona o entidad que necesita fondos para financiar un proyecto o

consumir (prestatario). El tipo de interés aplicado durante la vida del préstamo compensa al prestamista por suministrar el dinero y asumir el riesgo de impago. El tipo de interés suele ser mayor cuanto más largo es el plazo del préstamo, ya que el prestamista se expone a un mayor riesgo de impago del prestatario. (Harvey & Santoro 2020)

La inversión de la noción implica que los préstamos a corto plazo son menos arriesgados y, por tanto, exigen menos compensación al prestamista. Un préstamo *flash* es un préstamo a corto plazo que se devuelve en la misma transacción. Un préstamo *flash* es análogo a un préstamo de un día para otro en las finanzas tradicionales, excepto que la devolución es necesaria durante la transacción y se hace cumplir por el *smart contracts*.

Para entender cómo funcionan los préstamos *flash* es necesario comprender bien las transacciones de Ethereum. Una condición en la transacción es crítica: si el préstamo no se devuelve con el interés requerido al final de la transacción, todo el procedimiento vuelve al estado en el que estaba antes de que el dinero saliera de la cuenta del prestamista. En otras palabras, o bien el usuario utiliza con éxito el préstamo para el fin previsto y lo devuelve íntegramente a lo largo de la transacción, o la transacción fracasa y todo se reinicia como si el usuario nunca hubiera pedido dinero prestado.

Los préstamos *flash* están prácticamente exentos de riesgo de contraparte y de duración. Permiten a un individuo beneficiarse de oportunidades de arbitraje o refinanciar deudas sin comprometer la seguridad. Esta habilidad permite a cualquier persona del mundo acceder a posibilidades que tradicionalmente exigen un gasto importante de financiación. Es un ejemplo de producto financiero que no es posible en el ámbito de las finanzas tradicionales.

La deuda y el préstamo son quizás los procesos financieros más críticos en DeFi, y más ampliamente, en las finanzas convencionales. Por un lado, estos procesos proporcionan un medio eficaz para asignar el capital de forma efectiva, aumentar la exposición al riesgo de retorno y estimular el crecimiento económico. Por otro lado, un endeudamiento excesivo puede crear inestabilidad en el sistema, provocando importantes contracciones económicas y de mercado. Estos beneficios y peligros se potencian en DeFi debido al entorno hostil e interconectado en el que operan las contrapartes.

Cualquier préstamo con un plazo superior a cero días (préstamo *flash*) debe estar respaldado por una cantidad igual o superior de garantías. Los requisitos de garantía impiden contractualmente que una contraparte incumpla. Los mecanismos sin garantía aumentan el peligro de que los fondos sean robados por una contraparte, especialmente en un sistema abierto y anónimo como Ethereum. Un peligro asociado a la excesiva *collateralization* - el uso de un activo valioso para garantizar un préstamo- es que la garantía adquiere un valor inferior al del préstamo, lo que da lugar a una ejecución con pocas posibilidades de recuperación. Por ello, los tipos de garantía más variables exigen mayores ratios de *collateralization* para compensar este riesgo. (Harvey & Santoro 2020)

Se ha descrito anteriormente el procedimiento de liquidación; ahora se profunizará en él. Para evitar la liquidación, es fundamental que la deuda esté lo suficientemente *overcollateralized* – colateral excede valor del préstamo- como para que la volatilidad moderada de los precios no ponga en peligro el valor de la garantía. Normalmente, los *smart contract*s especifican un nivel mínimo de *collateralization* por debajo del cual se puede liquidar la garantía y cerrar la posición. La garantía puede subastarse o venderse directamente en un DEX, normalmente a través de un AMM, a precio de mercado.

Dado que las posiciones en la *blockchain* de Ethereum no pueden liquidarse automáticamente, se requiere un incentivo. A menudo, el incentivo es en forma de un porcentaje pagado a un guardián externo capaz de liquidar la posición y cobrar la recompensa. Cualquier garantía sobrante se devuelve al titular original de la posición. Como incentivo más fuerte, el sistema puede, en algunas situaciones, dejar toda la garantía restante en manos del depositario. Debido a la gran penalización por la liquidación y a la volatilidad de la mayoría de los tipos de garantías, las plataformas suelen permitir a los usuarios completar sus garantías para mantener unos buenos ratios de *collateralization*.

Los préstamos colaterales y el ajuste de la oferta de tokens tienen una implicación intrigante: la *collateralization* puede utilizarse para respaldar el valor de un token sintético. El token sintético es un activo financiero generado y financiado por la deuda, definida como la necesidad de reembolsar el token sintético para mantener la propiedad. (Harvey & Santoro 2020)

En “DeFi and the future of Finance”, Campbell R. Harvey expone los 5 problemas que DeFi resuelve frente a las finanzas tradicionales: ineficiencia, acceso limitado, opacidad, control centralizado y falta de interoperabilidad. (Harvey & Santoro 2020)

El primero de los cinco puntos débiles de las finanzas tradicionales es la ineficiencia. DeFi permite realizar transacciones financieras con enormes cantidades de activos y una fricción mínima, lo que normalmente impondría un importante coste organizativo a las finanzas tradicionales. DeFi produce *smart contract*s reutilizables en forma de aplicaciones descentralizadas (dApps) destinadas a realizar una transacción financiera específica. Estas dApps son accesibles a cualquier usuario que necesite ese tipo de servicio específico, por ejemplo, para ejecutar una opción de venta, independientemente del tamaño de la transacción. Dentro de los límites del *smart contract* y de la *blockchain* en la que se ejecuta la aplicación, el usuario puede esencialmente ser autosuficiente. En el caso de la DeFi basada en Ethereum, cualquiera que pague la tarifa plana, que suele ser de aproximadamente 15 dólares para una transferencia y de 25 dólares para una función de la dApp como el apalancamiento contra la garantía, puede utilizar los contratos. Una vez establecidos, estos contratos prestan sus servicios de forma casi continua, con unos gastos de organización casi nulos.

Los *keepers* son actores externos que reciben una compensación directa por prestar un servicio a los protocolos de DeFi, como la supervisión de las posiciones para asegurarse de que están adecuadamente garantizadas o la activación de cambios de estado para diversas actividades. Para garantizar que las ventajas y los servicios ofrecidos por una dApp tengan un precio adecuado, las recompensas de los *keepers* suelen diseñarse como una subasta. Al garantizar que los clientes paguen el precio de mercado por los servicios que necesitan, la competencia pura y abierta añade valor a los sistemas DeFi.

Los *forks* son otra noción que fomenta la eficiencia. En el contexto del código abierto, un *fork* es una copia y reutilización del código que incluye mejoras o modificación. Esto fomenta la competencia a nivel de protocolo y da lugar al desarrollo de la mayor plataforma de *smart contract*s posible. No sólo el código de la *blockchain* de Ethereum es abierto y *forkable*, sino también cada dApp de DeFi desarrollada sobre Ethereum. Si alguna de las aplicaciones DeFi es ineficiente o no es óptima, el código puede ser

rápidamente clonado, mejorado y reimplantado a través de un *fork*. *Forking* y sus beneficios asociados son el resultado de la naturaleza abierta de DeFi y de las cadenas de bloques.

El segundo de los puntos débiles de las finanzas tradicionales es el acceso limitado. Incluso los consumidores que tienen acceso a servicios financieros en las finanzas tradicionales, como cuentas bancarias, hipotecas y tarjetas de crédito, no tienen acceso a los productos financieros con los precios más competitivos y las condiciones más favorables; estos productos y estructuras están restringidos a las grandes instituciones. DeFi ofrece a cualquier usuario el acceso a la totalidad de su infraestructura financiera, independientemente de su riqueza o ubicación geográfica.

El *yield farming* compensa a los usuarios por apostar capital o implementar un sistema con pagos inflacionarios o basados en contratos. Estos beneficios pueden pagarse en el activo subyacente que el usuario posee o en un activo separado, como un token de gobernanza. Esto está disponible para todos los usuarios. Un usuario puede apostar cualquier cantidad, por mínima que sea, y obtendrá un pago proporcional. A través del token emitido, un usuario de un protocolo que produce un token de gobernanza se convierte en propietario parcial de la plataforma.

La tercera desventaja de la financiación convencional es su opacidad. A través de la naturaleza abierta y contractual de los acuerdos, DeFi resuelve este problema. Se examinará cómo los *smart contract*s y la *tokenization* pueden aumentar la transparencia de DeFi.

Las partes pueden estudiar de forma independiente los contratos para comprobar si las disposiciones son satisfactorias y eliminar cualquier incertidumbre sobre lo que ocurriría cuando interactúen bajo las condiciones del contrato. Esta apertura mitiga significativamente la posibilidad de responsabilidad legal y proporciona comodidad a los participantes más pequeños que, en el contexto actual de la banca convencional, pueden ser explotados por las contrapartes más grandes aplazando o incluso cancelando sus obligaciones en virtud de un acuerdo financiero. Aunque el usuario promedio no comprende el código del contrato, puede sentirse seguro debido a la naturaleza de código

abierto de la plataforma y al conocimiento de la multitud. DeFi, en general, mitiga el riesgo de contraparte y, por lo tanto, permite una serie de eficiencias no disponibles en la financiación tradicional.

Al ceder el poder a protocolos abiertos con características transparentes e inmutables, DeFi subvierte este control centralizado, latente en las finanzas centralizadas. La tasa de inflación de una dApp de DeFi, por ejemplo, puede ser controlada por una comunidad de interesados o incluso por un algoritmo programado. Si una dApp incluye poderes a nivel de administrador, todos los usuarios los conocen, y cualquier usuario puede construir fácilmente un equivalente menos centralizado.

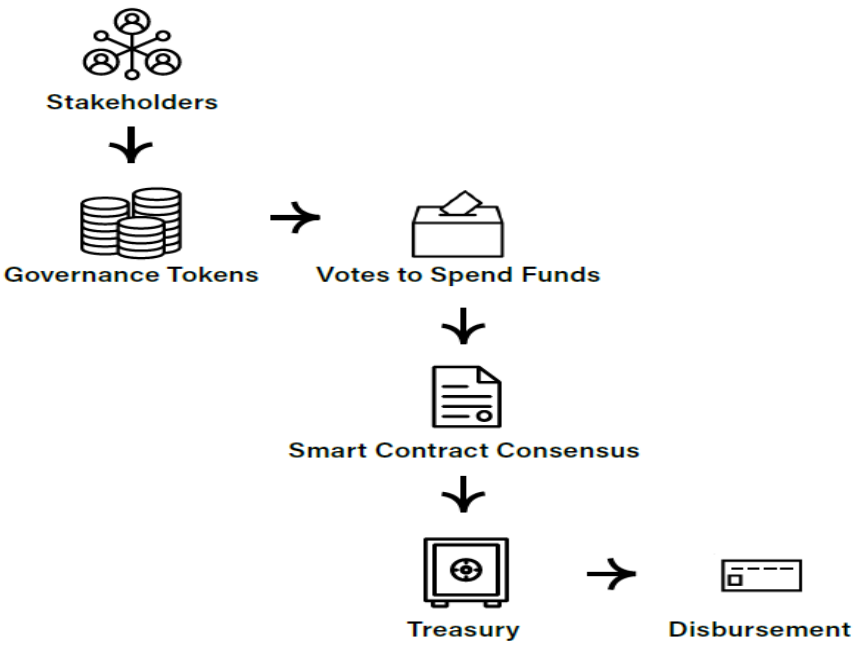
Debido a la cultura de código abierto de *blockchain* y a la naturaleza pública de todos los *smart contract*s, los defectos e ineficiencias de un proyecto DeFi pueden ser fácilmente encontrados y "*forkeados*" por usuarios que copien y arreglen el proyecto problemático. Como resultado, DeFi busca crear protocolos que incentiven a las partes interesadas de forma orgánica, manteniendo un equilibrio saludable. Gracias a *blockchain*, un nuevo diseño organizacional de control descentralizado ha surgido, las DAO.

Una Organización Autónoma Descentralizada (DAO) es un tipo de entidad nativa de Internet en la que sus miembros la controlan y administran de forma colaborativa. Considere una DAO como una fundación informal, en la que la organización recauda fondos a través de una variedad de donaciones y vota sobre cómo gastarlos. Las DAO mantienen sus propias tesorerías, que suelen estar protegidas mediante un monedero con varias firmas. Este monedero prohíbe el uso no autorizado de los activos compartiendo la clave secreta entre numerosos individuos, lo que les obliga a colaborar para desbloquear el dinero. Las propuestas y los métodos de votación regulan la toma de decisiones en una DAO, asegurando que todo el mundo dentro de la empresa tenga la misma voz en el proceso de gobierno. Este procedimiento permite a los usuarios votar sobre las decisiones críticas de gestión de recursos de la DAO, como el patrocinio de una colección de arte NFT, desarrollo de un nuevo protocolo DeFi o la compra de un campo de golf. Además, desarrolla un sentido de comunidad entre los miembros mientras trabajan por objetivos comunes. La pertenencia a las DAO se establece normalmente mediante instantáneas de la cartera, que capturan la dirección de la cartera de criptodivisas de un interesado con el

fin de establecer que el individuo o la empresa en cuestión posee los tokens de gobernanza relacionados con la DAO. (Kraken 2022)

El *smart contract* de una DAO es su base. Es decir, un contrato escrito de forma condicional que establece las regulaciones de la DAO mientras se mantiene el control de los fondos de ésta. En una cadena de bloques, los *smart contract*s se componen de un código informático autoejecutable que impone condiciones y acciones predefinidas. Permiten a las partes anónimas llevar a cabo transacciones y acuerdos de confianza sin la necesidad de un arbitraje de terceros. Una vez que el *smart contract* de la DAO está activo en la *blockchain*, sólo puede ser alterado por el voto mayoritario de los titulares de tokens de la DAO. Si un actor hostil intenta retirar fondos de la tesorería, comportarse de forma maliciosa o cambiar el contrato de alguna manera, las restricciones especificadas codificadas en el código informático bloquearán estos actos. Si se abusa del contrato, la naturaleza de código abierto del *smart contract*s implica que todos y cada uno de los usuarios podrán ver las acciones del atacante. (Kraken 2022)

Ilustración 14: Estructura de gobernanza en una DAO



Fuente: "*A community built in code"* by Kraken Intelligence (2021)

Volviendo a los problemas que DeFi resuelve. La falta de interoperabilidad es otro de los problemas que DeFi soluciona frente a las finanzas tradicionales. Una vez que se haya establecido una arquitectura básica para, por ejemplo, crear un activo sintético, se podrán aplicar los protocolos adicionales que permitan el préstamo y el empréstito. Una capa superior permitiría aplicar el apalancamiento a los activos prestados. A medida que surjan nuevas plataformas, esta compatibilidad podrá ampliarse en un número creciente de direcciones.

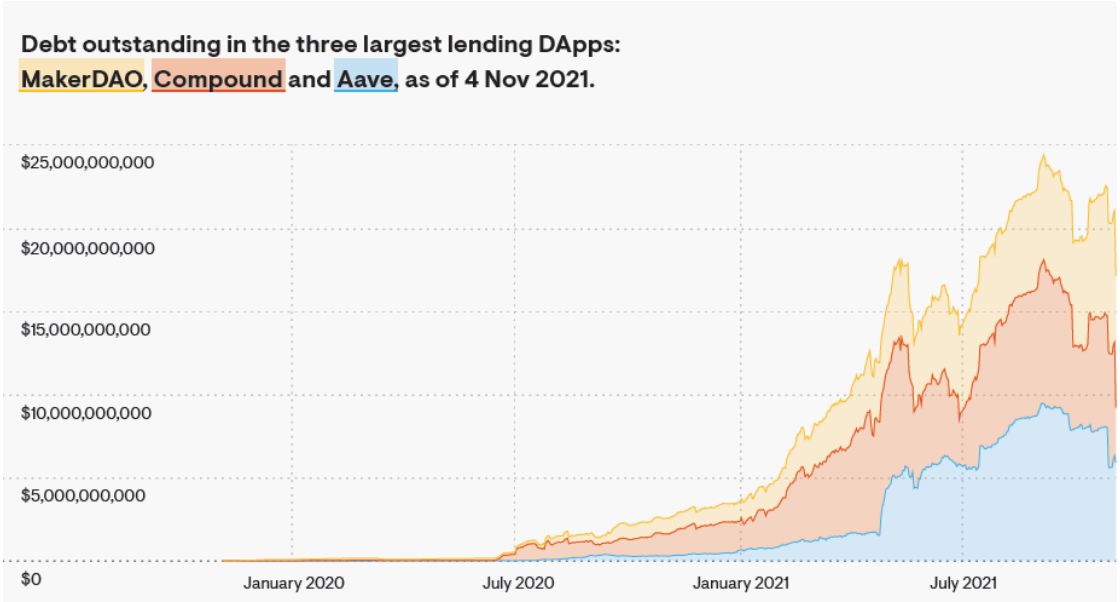
Gracias a las interfaces comunes de DeFi, las aplicaciones pueden acceder directamente a los activos de otros y reorganizarlos, así como subdividir las posiciones según sea necesario. Los Legos de Finanzas Descentralizadas (DeFi) son bloques de construcción, cada uno con su propia funcionalidad, que se pueden integrar para construir un protocolo con múltiples funciones. Mediante la *tokenization*, DeFi tiene el potencial de aumentar la liquidez en activos históricamente ilíquidos. Un uso sencillo sería generar acciones fraccionarias de un activo unitario, como una acción. Este enfoque puede ampliarse para permitir la propiedad fraccionaria de recursos preciosos, como pinturas raras. Los tokens pueden utilizarse como garantía para cualquier otro servicio DeFi, incluyendo el apalancamiento o la negociación de derivados. (Harvey & Santoro 2020)

La *tokenization* de activos físicos, como los bienes inmuebles o los metales preciosos, es más difícil que la de los activos digitales, ya que factores prácticos como el mantenimiento y el almacenamiento no pueden aplicarse mediante código. La *tokenization* también se ve limitada por las restricciones legales entre jurisdicciones; sin embargo, no se debe subestimar el beneficio de la *tokenization* segura y contractual para la mayoría de los casos de uso. (Harvey & Santoro 2020)

Dentro de DeFi podemos diferenciar numerosos sectores según la funcionalidad del protocolo. Hay dApps que encajan en múltiples, dependiendo del producto que ofrecen. A pesar de que en DeFi hay otras *blockchain*s desarrollando protocolos, como Polkadot, continuaremos desarrollando sobre la *blockchain* de Ethereum por ser la más popular y sobre la que más proyectos de DeFi se están desarrollando en el momento de escribir este trabajo.

Cada protocolo da para un trabajo específico, con lo que me centraré en resumir uno de los protocolos de DeFi que más adopción ha tenido en los últimos años, Aave, en concreto sus *flash loans*

Ilustración 15: Deuda en las tres principales dApps



Fuente: "*The Elliptic 2022 DeFi Report*" Elliptic (2022)

La mejor manera de describir Aave es como un sistema de grupos de préstamos o *lending pools*. Los participantes depositan los fondos que desean prestar, reunidos en un fondo común de liquidez. Los prestatarios pueden entonces extraer de esos fondos cuando piden un préstamo. Estas fichas pueden negociarse o transferirse como desee el prestamista. (Aave 2020)

El protocolo Aave permite la creación de mercados totalmente nuevos. Cada mercado se compone de una colección distinta de grupos de tokens, cada uno con su propia oferta y tipo de interés de préstamo. La ventaja de establecer un mercado distinto es que los tokens apoyados por el mercado funcionan como garantía exclusivamente en ese mercado y no tienen efecto en otros mercados, disminuyendo el riesgo de correlación.

Aave opera actualmente en dos mercados distintos. El primero es para tokens ERC-20 como USDC, ETH y DAI como activos. El segundo es exclusivo para los tokens del *exchange* descentralizado Uniswap (LP). Por ejemplo, cuando un usuario deposita una garantía en un mercado Uniswap, recibe un token LP que representa su propiedad en el mercado. Para obtener más beneficios, los tokens LP pueden colocarse en el mercado Uniswap de Aave.

Pero lo que más atracción ha generado, son las *flash loans* que ofrece Aave. Un préstamo *flash* es un préstamo a corto plazo que se devuelve en la misma transacción. Si el préstamo no se devuelve con los intereses requeridos al final de la transacción, todo el proceso vuelve a la condición en la que estaba antes de que el dinero saliera de la cuenta del prestamista. En otras palabras, o bien el usuario utiliza con éxito el préstamo para el fin previsto y lo devuelve íntegramente a lo largo de la transacción, o la transacción fracasa y todo se reinicia como si el usuario nunca hubiera pedido dinero prestado. (Aave 2020)

Las *flash loans* están prácticamente exentas de riesgo de contraparte y de duración. Sin embargo, siempre hay un peligro asociado a los *smart contract*s. Un ejemplo reciente es lo ocurrido con el *airdrop* -desarrolladores otorgan tokens gratuitamente a las carteras que ellos consideren oportunas con el fin de promover o recompensar a los usuarios por el uso del protocolo- de los gigantes de los NFT´s, Yuga labs, los creados del Ape Yacht Club. Realizaron un airdrop en el que otorgaban su nuevo token (APE) a cualquier propietario de un NFT de esta colección. En el *smart contract* no se especificaba desde cuando debía uno ser propietario del NFT para reclamar estos tokens. Mediante una *flash loan* un individuo pidió prestado cinco de estos NFT´s que no habían reclamado sus tokens aún. En el mismo *smart contract*, solicitó los tokens, lo que le otorgó la capacidad de reclamar alrededor de $1.1 millones en APE coin, los envío a su *wallet*, vendió y envío los beneficios a otras *wallets*, devolviendo los NFT´s como se establecía en la *flash loan*. Generando instantáneamente una venta a precio de mercado. En la comunidad hay un debate activo sobre hasta qué punto "*code is law"* pues son unos cuantos los casos en los que individuos aprovechan *bugs* en el código para realizar este tipo de acciones. Pero no se profundizará en este debate. (Crypto Times 2022)

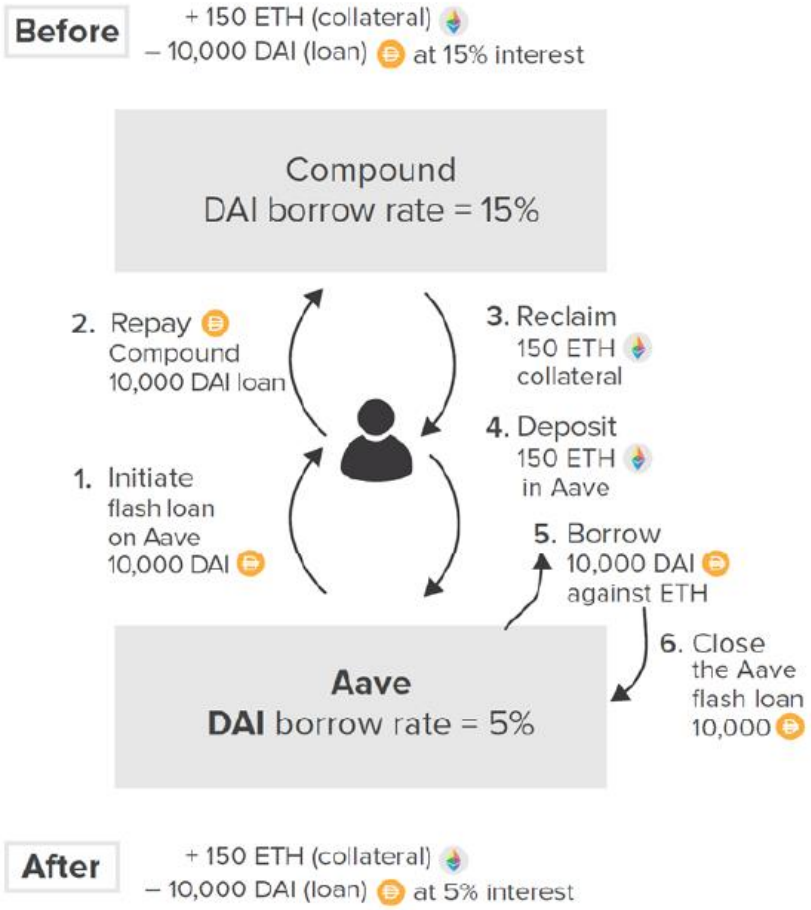
Retomando Aave. Para ejecutar un préstamo *flash*, Aave cobra una comisión de 9 puntos

básicos (pb) sobre el importe del préstamo. La comisión se paga al pool de activos y da un impulso a los rendimientos de la inversión de los proveedores, ya que cada uno posee una parte proporcional del pool. Un uso fundamental de los préstamos *flash* es que permiten a los consumidores obtener fondos rápidamente para refinanciar sus participaciones. Esta característica es fundamental para DeFi, tanto como componente básico de la infraestructura como elemento de una gran experiencia de usuario (UX). Del cual el ecosistema *crypto* tiene todavía mucho recorrido por mejorar su experiencia de usuario, como se mencionó previamente, pues a día de hoy requiere cierta habilidad para operar en él.

Se utilizará un ejemplo para explicar Aave. Supongamos que el precio de ETH es de 200 DAI (token ERC-20 que funciona como *stablecoin*). Un usuario suministra 100 ETH en Compound (otro protocolo de DeFi) y toma prestados 10.000 DAI para apalancarse y comprar otros 50 ETH, que el usuario también suministra a Compound. Se asume que el tipo de interés del préstamo en DAI en Compound es del 15%, pero sólo en Aave es del 5%. El objetivo es refinanciar el préstamo para aprovechar el tipo más bajo ofrecido en Aave, lo que es análogo a la refinanciación de una hipoteca, un proceso largo y costoso en las finanzas centralizadas. (Harvey & Santoro 2020)

Una opción es deshacer manualmente cada operación en Compound y volver a realizar ambas operaciones en Aave para reconstruir la posición apalancada, pero esta opción es un derroche en términos de comisiones de cambio y de gas. La acción más fácil es sacar un préstamo *flash* de Aave por 10.000 DAI, utilizarlo para pagar la deuda en Compound, retirar los 150 ETH completos, volver a abastecer a Aave, y activar una posición de préstamo normal de Aave (al 5% TAE) contra esa garantía para pagar el préstamo *flash*. Este último enfoque salta efectivamente los pasos de intercambiar ETH por DAI para deshacer y revertir el apalancamiento. (Harvey & Santoro 2020)

Ilustración 16: Esquema funcionamiento flash loan en Aave



Fuente: "*DeFi and the Future of Finance"* by Harvey, C. (2020)

Como se expuso en el ejemplo anterior, un préstamo *flash* utilizado para refinanciar una posición permite a las aplicaciones de clientes DeFi que permiten a los usuarios mover una posición apalancada con un solo clic de una dApp a otra.

Una invención exclusiva de Aave es el préstamo a tipo "estable". El término "tipo estable" se utiliza deliberadamente por "tipo fijo". Un prestatario puede elegir entre un tipo variable y un tipo estable corriente. El tipo de oferta es siempre variable, ya que sería difícil financiar un tipo de oferta fijo en determinadas situaciones, como por ejemplo si todos los prestatarios abandonan el mercado. Los proveedores siempre ganan la suma de los pagos de intereses de los préstamos estables y variables, menos los costes

de la plataforma.

El tipo estable no es un tipo fijo, ya que es modificable durante los periodos de fuerte restricción de liquidez y puede refinanciarse a un tipo inferior si las condiciones del mercado lo permiten.

La demanda de DeFi se ha multiplicado a lo largo del año, con aplicaciones como Aave, Maker y Curve, todas ellas con más de 20.000 millones de dólares en criptoactivos. Las aplicaciones más populares siguen desplegando *cross-chain* -tecnología que mejora la interconexión entre las redes de blockchain al permitir el intercambio de información y valor- lo que hace que los servicios sean más accesibles gracias a la reducción de las tasas de transacción y, en última instancia, atrae nuevas fuentes de capital e ingresos. (Coindesk 2021)

3. Conclusiones

Blockchain y en concreto DeFi ha crecido a un ritmo imparable en los últimos años, pero para poder triunfar, la estrategia es coexistir con las finanzas tradicionales para ello se enfrente a varios retos.

Hay un aspecto base que une a todo el mundo financiero, independientemente de la supervisión reglamentaria o de los activos bajo gestión (AUM): El riesgo. La gestión del riesgo en DeFi tiene varias dimensiones. Esto implica el almacenamiento seguro de las claves privadas, que se suelen guardar en Módulos de Seguridad de Hardware (HSM) o tecnología de custodia de Multi-Party Computation (MPC), o con custodios cualificados.

La siguiente capa de la pirámide es el cumplimiento de la normativa o *compliance*, un riesgo y un reto al que todavía no se enfrenta el ecosistema *crypto*, aunque la creciente supervisión reglamentaria será sin duda primordial en los próximos meses y años: en Europa, Asia y EE.UU., las instituciones tienen que cumplir la normativa.

El siguiente nivel de la pirámide incluye la mejor ejecución: garantizar que los activos puedan adquirirse y enajenarse con amplia liquidez, y que los márgenes se mantengan ajustados y bajos. El acceso a DeFi debe estar al alcance de todos. Para eso se concibió.

El *reporting* constituye el cuarto nivel de la pirámide, que incluye una variedad de nuevos retos para el mundo institucional: Un nuevo mundo financiero da lugar a nuevos retos, desde los *airdrops* hasta los tokens de gobernanza. Por ejemplo, *el yield farming* de forma activa en DeFi conlleva la creación de complejas estrategias de negociación que incluyen la apuesta de tokens de recompensa. Estas posiciones generan ganancias de capital, tokens de gobernanza adicionales e intereses anuales. Como se genera este *reporting* es crucial.

Por último, está la investigación: cómo entender y filtrar mejor los crecientes matices y las oportunidades más importantes dentro del ecosistema DeFi. Adaptándose.

Los próximos años son muy importantes en cuanto al futuro que tomará esta industria. El 2021 fue un año de gran adopción institucional, solo el tiempo dirá qué camino sigue.

4. Bibliografía

¿Qué es un token ERC 721? La era del coleccionismo digital. Bit2Me Academy. (2022). Retrieved 30 March 2022, from https://academy.bit2me.com/que-es-token-erc-721/.

¿Qué es un token ERC-1155 en Ethereum?. Bit2Me Academy. (2022). Retrieved 30 March 2022, from https://academy.bit2me.com/que-es-token-erc-1155/.

¿Qué es un token ERC-20?. Bit2Me Academy. (2022). Retrieved 30 March 2022, from https://academy.bit2me.com/que-es-erc-20-token/.

Aave Protocol Whitepaper. (2020), 1.0.

Allison, I. (2015). Nick Szabo: *If banks want benefits of blockchains they must go permisionless.* IBT Times. from https://www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874.

BBVA Research. (2017). *Situación Economía Digital. Diciembre 2017*. Infografía, 17. Bocigas, Pablo Blasco. 2016. Los nuevos players en el sector financiero. Fintech Spain.

Bonilla, María Emilia Vergara. (2017). *Fintech: Innovación bancaria con Responsabilidad Social.*

Breidenbach, L., Cachin, C., Chan, B., & Coventry, A. (2021). *Chainlink 2.0: próximos pasos en la evolución de Redes Oracle descentralizadas.*

Buterin, V. (2014). Ethereum White paper: A next generation smart contract & decentralized application platform. *Ethereum*.

Buterin, V. (2022). *Intro to Ethereum | ethereum.org*. ethereum.org. 2022, from https://ethereum.org/en/developers/docs/intro-to-ethereum/.

Chart, B. (2022). *Bitcoin Block Time Chart.*, from https://bitinfocharts.com/comparison/bitcoin-confirmationtime.html#3y

Crypto Insights#2 Decentralised Exchanges & Automated Market Makers- Innovations, Challenges & Prospects. (2021).

Cryptocurrency prices, charts, and crypto market cap. CoinGecko. (2022) from https://www.coingecko.com/

de Figueiredo, I. (2022). *Property-based testing of ERC-721 Ethereum smart contracts.* U. Porto.

Donaldson, C. (2016). *Craig Donaldson from Metro Bank: Layout of the Store. Fintech Finance.* Retrieved 1 April 2022, from https://ffnews.com/fintech-tv/metro-bank-craig-donaldson-2/.

Dwork, C., & Naor, M. (2022). *Pricing via processing or combatting junk mail. IBM* Almaden Research Center.

Evin Sellin, (2017) *What Exactly Is Turing Completeness?* Blog, Medium, Medium medium.com/@evinsellin/what-exactly-is-turing-completeness-a08cc36b26e2

Gas and fees | ethereum.org. ethereum.org. (2022). Retrieved 30 March 2022, from https://ethereum.org/en/developers/docs/gas/.

Hansen, S. (2021). *BlackRock Files To Add Bitcoin Futures To Funds. Retrieved 1 April* 2022, from https://www.forbes.com/sites/sarahhansen/2021/01/20/blackrock-files-to-add-bitcoin-futures-to-funds/?sh=7c8aa1063086

Harvey, C., Ramachandran, A., & Santoro, J. (2020). *DeFi and the future of finance*. Duke University.

Jakobsson, M. *Proofs of Work and bread pudding protocols (extended abstract*). Information Sciences Research Center By Ari Juels.

Jha-Coin, P. (2022). *Vitalik Buterin clarifies concerns about ETH 2.0 upgrade delays.* Binance. from https://www.binance.com/en/news/top/6693821

John, K., O´Hara, M., & Saleh, F. (2021*). Bitcoin and beyond. Annual Review Of Financial Economics.*

Kim, T. (2018). *Jamie Dimon says he regrets calling bitcoin a fraud and believes in the technology behind it. Retrieved* , from https://www.cnbc.com/2018/01/09/jamie-dimon-says-he-regrets-calling-bitcoin-a-fraud.html

Kirbac, G., & Tektas, B. (2021). *The Role of Blockchain Technology in Ensuring Digital Transformation for Businesses: Advantages, Challenges and Application Steps*, from MDPI.

Li, J., & Mann, W. (2018). *Initial Coin Offering and Platform Building.*

Metamask (2021). *DeFi and Web3 for Organizations*. (2022). from. Consensys

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3977007

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies* (1st ed.). Princeton University Press.

Peyrott, S. (2017). *An Introduction to Ethereum and Smart Contracts* (1st ed.). Auth0 Inc.

Preukschat, A., & Kuchkovsky, C. (2017). *Blockchain. La revolución industrial de internet*. Grupo Planeta.

Proof-of-stake (PoS) | ethereum.org. (2022). Retrieved, from https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Proposals, E. (2022). *EIP-1155: Multi Token Standard. Ethereum Improvement Proposals.*, from https://eips.ethereum.org/EIPS/eip-1155.

R.L., R., A., S., & L., A. (1977). *A method for obtaining digital signatures and public-key cryptosystems.*

Selkis, R. (2022). *Crypto Theses for 2022* (1st ed.). Messari Report.

Capgemini Consulting, *Smart Contracts in Financial Services: Getting from hype to reality*. (2020). Retrieved 1 April 2022

Solidity Documentation. (2022). Ethereum, 0.8.14. Retrieved 1 April 2022

Someone Claims $1.1M from Ape Tokens Airdrop via Flash Loan. The Crypto Times. (2022). Retrieved 30 March 2022, from https://www.cryptotimes.io/someone-claims-1-1m-from-ape-tokens-airdrop-via-flash-loan/.

Szostek, D. (2021). *Blockchain and the law.*). Retrieved 1 April 2022

Tapscott, B. (2021). State of enterprise blockchain. Blockchain Research Institute.

Tetyana, B (20222) *Intro to Fintech* Retrieved 1 April 2022

The 2022 crypto crime report. (2022). Chainalaysis.)

Zetzsche, D., Arner, D., & Buckley, R. (2020). Decentralized Finance (DeFi). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3539194