UNIVERSIDAD POLITÉCNICA DE MADRID

Escuela Técnica Superior de
Ingenieros Informáticos

Grado en Administración y
Dirección de Empresas

Trabajo Fin de Grado

Finanzas Descentralizadas en Blockchain: Automated Market Makers, Swaps y Arbitraje

Autor: Álvaro Jiménez Mesa
Tutor: Sergio Ríos Aguilar

Madrid, junio 2022

Este Trabajo Fin de Grado se ha depositado en la ETSI Informáticos de la Universidad Politécnica de Madrid para su defensa.

Trabajo Fin de Grado
Grado en Administración y Dirección de Empresas
Título: Finanzas Descentralizadas en Blockchain: Automated Market Makers, Swaps y Arbitraje
Junio 2022

Autor: Álvaro Jiménez Mesa

Tutor: Sergio Ríos
Department of Organization Engineering, Business Administration and Statistics
ETSI Informáticos
Universidad Politécnica de Madrid

Resumen

La madurez del sector financiero está llevando al extremo la centralización institucional. La irrupción de la tecnología Blockchain parece haber sido acogida como una manera de escapar de las barreras y asimetría de un sistema cada vez menos plural. Las Finanzas Descentralizadas han inaugurado una nueva etapa en la que el comercio de capitales ha adquirido un significado totalmente nuevo. No solo han originado nuevos activos *crypto*, sino que también han permitido el desarrollo de nuevos protocolos y mercados que han propiciado unas finanzas mucho más accesibles, justas y transparentes. La revolución con respecto a las finanzas convencionales radica en una desintermediación, automatización y descentralización.

Los *Automated Market Makers* componen el paradigma bajo el que operan los *Decentralized Exchanges*. Concretamente, *Uniswap* fue el protocolo precursor de este modelo, que satisface la oferta y demanda de proveedores de liquidez y operadores a través de plataformas automáticas de reservas o Liquidity Pools. Estos elementos se conjugan con la configuración *Constant Function*, implementada por el AMM de Uniswap. Con él, se logra optimizar el comercio en los mercados descentralizados, maximizando la eficiencia de capital.

De manera paralela a Uniswap, en el entorno se asientan otros medios en los que se facilita el comercio de criptoactivos. Esto termina incubando un ecosistema que promueve la simbiosis e interoperabilidad y, con ello, una fluctuación de los valores que está sujeta a un considerable riesgo. No obstante, este contexto es propicio para un Comercio de Alta Frecuencia que se vale de estrategias como el arbitraje. Este trabajo culminará con la propuesta de una herramienta que pueda ofrecer utilidad para ejecutar este tipo de operaciones.

Términos clave: Blockchain, Finanzas Descentralizadas (DeFi), Decentralized Exchange (DEX), Automated Market Makers (AMM), Constant Function Market Maker (CFMM), Uniswap, Liquidity Pool, Liquidity Provider (LP), swap, arbitraje, oráculo.

Abstract

The maturity of the financial sector is pushing institutional centralization to the extreme. The irruption of Blockchain technology seems to be celebrated as a way to evade the barriers and asymmetry of a system increasingly biased. Decentralized Finance has inaugurated a new stage where capital trading has a whole new meaning. Not only has it originated new crypto assets, but it has also bred the development of new protocols and markets that establish an accessible, fair and transparent financial system. The detachment from conventional finance lies in disintermediation, automation and decentralization.

Automated Market Makers make up the paradigm in which Decentralized Exchanges operate. Specifically, Uniswap served as the precursor protocol of this model satisfying the supply and demand of liquidity providers and traders through automatic platforms of reserves or Liquidity Pools. By combining these elements with the Constant Function Market Maker configuration, Uniswap AMM achieves an optimal trading solution in decentralized markets while maximizing capital efficiency.

In parallel to Uniswap, numerous facilities are settled in the environment for cryptoasset trading. This ends up incubating an ecosystem that promotes symbiosis and interoperability resulting in fluctuation of values, being subjected to considerable risk. Nevertheless, this context is the right place for High Frequency Trading, that makes use of strategies such as arbitrage. This project will culminate in the proposal of a tool that can offer utility in executing these operations.

Key Words: Blockchain, Decentralized Finance (DeFi), Decentralized Exchange (DEX), Automated Market Makers (AMM), Constant Function Market Maker (CFMM), Uniswap, Liquidity Pool, Liquidity Provider (LP), swap, arbitrage, oracle.

Índice de contenidos

1 Introducción 1

1.1 Contexto y Motivación 1

1.2 Objetivo y Alcance 3

1.3 Estructura del documento 4

2 ¿Qué son las Finanzas Descentralizadas? 5

2.1 La crisis de las Instituciones Centralizadas 5

2.2 ¿Qué es Blockchain y qué puede ofrecer a las Finanzas? 9

2.3 Atributos de las Finanzas Descentralizadas 14

I. Nuevos activos digitales: monedas descentralizadas y tokens 14

II. Inflación monetaria automatizada 15

III. Stablecoins, una opción menos arriesgada 15

IV. Pago de extremo a extremo 16

V. Captación de fondos descentralizada 16

VI. ¿Y el blanqueamiento de capitales? 17

VII. ¿Más seguro? Imposible 17

VIII. Derivados y sintéticos financieros 18

IX. Préstamos millonarios a todo riesgo: Flash Loans 18

X. Arbitraje 19

3 Plataformas de Intercambio de Activos y Automated Market Makers 20

3.1 Hola a los Exchanges 20

3.2 Decentralized Order Book Exchanges vs Automated Market Makers 22

El inicio del *Yield Farming* 24

3.3 Constant Function Market Maker (CFMM) 27

3.4 Uniswap 33

Ecosistema Uniswap 35

Aportaciones de Uniswap V3 38

3.5 Otros protocolos de Swaps 43

I. SushiSwap 43

II. Curve 43

III. 1inch 44

3.6 Red de Oráculos: Chainlink 46

4 Caso de Estudio: Oráculo de Precios sobre Swaps en Automated Market Makers 48

4.1 ¿Qué sucede con los precios en los AMM? 48

4.2 Propuesta de un Oráculo de Precios 52

4.3 Con miras al futuro 56

5 Consideraciones y Conclusión 59

6 Referencias 64

Índice de figuras

Figura 1: Optimismo en la proyección de futuro en países desarrollados [11]. 5
Figura 2: ONGs y negocios son consideradas como fuerzas estabilizadoras ante la decadencia de confianza en los gobiernos o medios de comunicación [11]. 6
Figura 3: Comparación superficial entre Finanzas Centralizadas y Descentralizadas [12]..... 13
Figura 4: Curva de CFMM [30]. 27
Figura 5: Swap A ⇌ B [26]. 28
Figura 6: Inyección y retirada de Liquidez en A ⇌ B [26]. 30
Figura 7: Impermanent Loss frente a la fluctuación de precio de mercado [34]..... 32
Figura 8: Funcionamiento de Uniswap V2 [31]. 34
Figura 9: Depósito de Líquido por parte del LP en Uniswap [31]. 34
Figura 10: Swap por parte del corredor en Uniswap [31]. 35
Figura 11: Ecosistema Uniswap [31]. 36
Figura 12: Construyendo un Oráculo de Precios fiable en Uniswap V2 [31]. 38
Figura 13: Virtualización de k en Uniswap V3 [23]..... 40
Figura 14: *Plan de 4 años de liberación de UNI* [42]. 41
Figura 15: Agregación en Sistema Chainlink [57]. 47
Figura 16: Variación del tipo de cambio DAI/USD de Uniswap V3 [63]. 50
Figura 17: Variación del tipo de cambio WBTC/ETH de Uniswap V3 [65]. 51
Figura 18: Variación del tipo de cambio de ETH/USDT en Uniswap V3 [67]. 51
Figura 19: Visión general del Oráculo de Precios 52
Figura 20: Arbitraje con Flash Loans y Swaps en DeFi. 57

1 Introducción

Se comienza el trayecto comprendiendo cuál es el contexto en el que se enmarca el trabajo, así como la motivación detrás del proyecto. Además, se entenderán cuáles son los objetivos que se pretenden alcanzar y se presentará la estructura a la que se regirá el contenido.

1.1 Contexto y Motivación

La explosión de los criptoactivos ha logrado un eco y difusión más que evidente. Es raro no haber escuchado la palabra "Bitcoin"; en el último año se han puesto especialmente de moda los "NFTs". No obstante, la divulgación lograda ha derivado en un desmesurado boom que, mayoritariamente, pretende interpretar estos activos de manera muy superficial. Incluso, este revuelo sobredimensionado con el que ha impactado las a masas, se ha fundido con la cultura popular en un tono casi cómico, originando expresiones como "cryptobro".

No se puede dejar atrás el hecho de que estos instrumentos se asientan en la tecnología Blockchain, y precisamente es esa naturaleza tan innovadora la que otorga a algunos de estos nuevos valores *crypto* tanta repercusión. *Bitcoin* o *Ether* son algunos de estos activos pioneros en esta nueva forma de hacer finanzas.

Mientras la cotización global de los mercados descentralizados ya ronda los 3 billones de dólares (eso son 12 ceros) [1], la revolución que está sucediendo en este entorno se hace patente con la continua irrupción de nuevos instrumentos, mercados y dinámicas. Por el momento, las posibilidades de creación de valor parecen prácticamente infinitas.

Las Finanzas Descentralizadas tienen a su espalda un trayecto relativamente corto y poco sólido; en este momento se encuentran en pleno auge. A pesar de la fuerte capacidad de atracción de capital, este terreno tiene asociados importantes riesgos y, aun así, las *DeFi* son más conocidas por su potencial rentabilidad que por su cuestionable estabilidad y seguridad, tanto a nivel financiero como operativo. Por ello, no se va a partir de la consideración de que las criptomonedas son la inversión definitiva, sino que vamos a observarlas desde la raíz.

Como se argumentaba, Blockchain ha sido la tecnología que ha propiciado el nacimiento de las Fianzas Descentralizadas y, como estudiante del Doble Grado de Ingeniería Informática y Administración y Dirección de empresas, considero esta materia como un marco de investigación idóneo para conjugar mis competencias técnicas y financieras; haciendo un estudio complementario desde ambos Trabajos Fin de Grado. Abordo este proyecto como una oportunidad para profundizar en la materia de las *DeFi*, de la mano de Blockchain, y contribuir a la literatura académica que

pretende hacer más accesible la comprensión de las innovaciones planteadas desde estas áreas.

Los *Decentralized Exchanges (DEXes)* son plataformas del entorno *DeFi* que utilizan protocolos específicos implementados sobre el Blockchain. Los *Automated Market Makers* ya han supuesto una revolución para el modelo de los *DEXes*. Dentro de esta categoría, los *swaps* sirven como operación para que los agentes del contexto intercambien criptoactivos.

Con esta expansión y crecimiento de capital en las Finanzas Descentralizadas, los *swaps* se han posicionado como uno de los servicios más atractivos para los participantes del mercado y es por ello que, progresivamente, han surgido nuevos protocolos que sustentan este modelo de comercio financiero.

Dentro de cada una de las plataformas, existen una amplia variedad de *Liquidity Pools* que ofrecen cambio para un par de criptoactivos. Los tipos de cambio resultan especialmente inestables ya que, no solo están fuertemente influidos por la volatilidad de precios de los valores que involucra cada par, sino que, además, se transforman con las transacciones realizadas por los propios inversores que buscan cambio [2, 3, 4, 5, 6, 7, 8, 9].

Esto plantea uno de los dilemas a los que se enfrentan los agentes corredores en *DeFi*: ¿cuál de las plataformas ofrece el mejor cambio en un momento dado? Más aún, ¿y si fuese posible aprovechar las diferencias entre los pares ofertados desde diferentes AMM?

1.2 Objetivo y Alcance

Desde este trabajo se va a realizar un recorrido por los principales productos de las Finanzas Descentralizadas que servirá como reconocimiento esencial para presentar las innovaciones fundamentales que esta nueva forma de finanzas tiene que ofrecer. Se podrá aportar un estudio más amplio de la naturaleza de los criptoactivos y las dinámicas que rigen los mercados en los que operan.

El recorrido que se realizará desde este Trabajo Fin de Grado comenzará con una perspectiva más general de las *DeFi* y avanzará aproximándose hacia uno de los campos de operación más densos y activos de este entorno. A lo largo de este trayecto se irán exponiendo diferentes atributos, productos, servicios y sistemas particulares a las Finanzas Descentralizadas.

Logrando un nivel más exhaustivo de análisis, se dirigirá el tratamiento hacia los *Decentralized Exchanges* y, más concretamente, hacia los *Swaps* que operan como *Automated Market Makers* en el modelo de *Constant Product Market Maker*. *Uniswap* es uno de los sistemas precursores de este ámbito, y se utilizará como modelo para comprender el funcionamiento generalista de los *swaps*. El tratamiento teórico de los *swaps* resultará muy representativo para reflejar la mecánica que opera detrás de las *DeFi*.

Además, se intentará resolver funcionalmente esa búsqueda del mejor *swap* a través de un Oráculo de Precios que podrá comparar los tipos de cambio de un par en diferentes mercados descentralizados. El diseño de este sistema, permitirá mostrar la interoperabilidad que define las *DeFi*. Más aún, pondrá en valor la funcionalidad incipiente que puede reportar para desarrollar estrategias de comercio en mercados descentralizados como el arbitraje.

Según lo expuesto, definimos el objetivo principal: Aportar una perspectiva muy próxima del funcionamiento de los swaps en los *Automated Market Makers*.

A continuación, se exponen las metas secundarias ordenadas según la prioridad:

1. Recorrer los principales vectores de innovación en las Finanzas Descentralizadas; tanto productos como instrumentos o plataformas.
2. Plantear el diseño de una aplicación *DeFi* que interacciona con otros sistemas del entorno y elaborar consideraciones sobre ello.
3. Obtener una visión sistemática del arbitraje en los mercados descentralizados.

1.3 Estructura del documento

A continuación, se presenta el trayecto propuesto en este trabajo para cubrir las metas y aspectos introducidos anteriormente. Además de esta propia sección, se cuenta con:

- ◊ En el punto 2 tendrá lugar el primer acercamiento a las Finanzas Descentralizadas. Se dará comienzo hablando del deterioro de la confianza general en el modelo de centralización institucional, especialmente vinculado al entorno financiero. Este inicio dará pie a la exposición de los beneficios que puede aportar Blockchain para superar ciertas barreras y debilidades del sistema. Por último, se extenderá un recorrido más detallado por las diferentes posibilidades que ofrecen las *DeFi*, con lo que se podrá demostrar la innovación y el potencial creciente en esta área.
- ◊ A continuación, se centrará el estudio en los *Decentralized Exchanges* o mercados descentralizados para el comercio de criptoactivos. En un principio se hablará del modelo de *Order Book* que interviene en las plataformas convencionales de compraventa de activos y se pondrá en perspectiva con el paradigma propuesto por los *Automated Market Makers*, en los que se basan los mercados descentralizados. Seguidamente, se orientará el análisis en la variación de *Constant Function Market Maker* utilizados por algunos de los AMM más populares. En última instancia, el estudio se encauzará más aun exponiendo el protocolo de *Uniswap*, AMM implementado como CFMM y que se utilizará como caso representativo de los mercados descentralizados.
- ◊ En el cuarto punto, se pondrá el foco en la interoperabilidad del ecosistema *DeFi*. Se hablará de la volatilidad de los tipos de cambio en swaps, lo que nos conducirá al diseño elemental de un Oráculo de Precios, que se alimentará de los datos arrojados por diferentes AMM. Además, se trasladará el uso de esta aplicación al arbitraje en mercados descentralizados. Con esto, se acabará de comprender cómo las Finanzas Descentralizadas se arraigan profundamente en la base técnica del Blockchain y se ofrecerán consideraciones al respecto desde la perspectiva financiera.
- ◊ Para terminar, la sección final concluirá todo el trabajo y será el espacio en el que deliberaré sobre la materia tratada haciendo uso de mi opinión de forma más explícita.

2 ¿Qué son las Finanzas Descentralizadas?

Se plantean los precedentes de la revolución de las Finanzas Descentralizadas así como todo el conjunto de propuestas de innovación que ofrecen para generar un contexto financiero totalmente nuevo.

2.1 La crisis de las Instituciones Centralizadas

La sociedad contemporánea está viviendo una tendencia clara: la confianza institucional está en crisis. Esto pone en juicio múltiples factores que definen los modelos y estructuras que han definido nuestros estados durante siglos, y nos lleva a plantearnos si la civilización occidental ha llegado a un estado de madurez que ya pide una reformulación radical de los sistemas institucionales para retomar un progreso democrático.

Los medios de comunicación y los gobiernos son consideradas las peores fuentes de información, según el informe "Trust Barometer" de Edelman de 2022. De hecho, ambas se ven como fuerzas separadoras de la sociedad y, además, preocupa la aptitud para dar respuesta a problemas sociales o retos existenciales como la pérdida de trabajo, la crisis climática, el uso de los *fake news* como arma o incluso la pérdida de libertades personales [2].

Algo aún más impactante para el sector financiero es que, según el estudio, únicamente un 33% de los encuestados consideraban que las economías reguladas de manera centralizada actuarían mejor que el libre mercado.

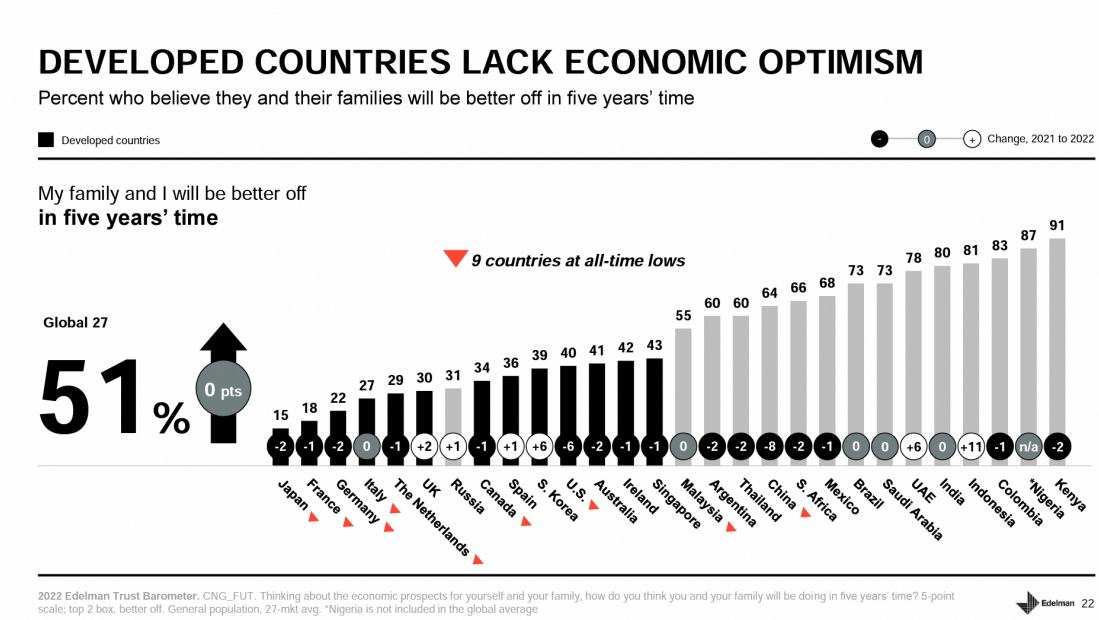


Figura 1: Optimismo en la proyección de futuro en países desarrollados [11].

La fe en la democracia y el sistema capitalista también se ve negativamente afectada. Según el estudio, el capitalismo se considera mayoritariamente más perjudicial que conveniente y la confianza en los líderes políticos de los países cae con respecto a años anteriores. No obstante, la tendencia es bastante diferente entre países en vías de desarrollo y las naciones desarrolladas.

Por otro lado, como se puede ver en la Figura 2, la esperanza puesta en ONGs y empresas, especialmente en los CEOs, definen una tendencia que los acepta como los "aliviadores" de las problemáticas sociales, económicas, humanitarias y medioambientales que envuelven el contexto actual.

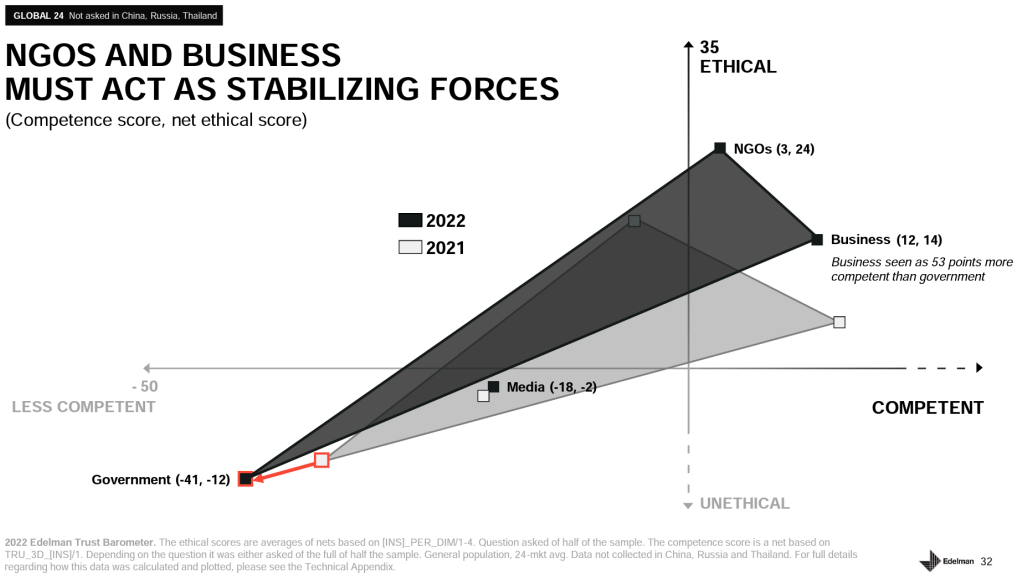


Figura 2: ONGs y negocios son consideradas como fuerzas estabilizadoras ante la decadencia de confianza en los gobiernos o medios de comunicación [11].

En el modelo social y financiero actual, los agentes intermediarios permiten a las partes encontrarse, crear confianza y establecer la plataforma o moderar para efectuar la transacción acordada. El principio de la confianza en los organismos, tanto en las instituciones públicas como en las empresas privadas, puede medirse a nivel teórico como el cumplimiento, por parte de la entidad en tela de juicio, de los 4 principios de la integridad: honestidad, consideración, responsabilidad y transparencia [3].

A pesar de los mecanismos de control, calidad, auditoría, legislación vigente o regulación estatal, la seguridad o garantías que se ofrecen no se presentan como suficientes para asegurar la integridad de estos intermediaros y el no perjuicio de las partes interesadas. Por otra parte, la postura de poder y control que abarcan estas entidades intermediarias les otorgan gran capacidad de influencia sobre la política o

economía. Esto genera un conflicto de intereses cuando grandes entidades se ven con la capacidad de perseguir metas propias en detrimento de las demás partes involucradas en el sistema.

Desde los años setenta, la liberalización y una escasa regulación deficiente del sector financiero otorgó a las instituciones de este ámbito nuevas capacidades y, quizás, excesivo poder. Aunque esto promovió la expansión económica, también dio comienzo a un nuevo periodo de inestabilidad económica y financiera que ha permitido la sucesión de numerosas crisis, hasta la más reciente y probablemente de mayor repercusión desde la Gran Depresión, la Crisis Financiera de 2007 [4].

Por otra parte, las recesiones económicas o fenómenos financieros turbulentos han demostrado en numerosas ocasiones disipar las rentas medias [5] [6], más recientemente con la Crisis del Covid-19. Esto está aumentando peligrosamente la brecha social y una indignación generalizada por los segmentos más gruesos de población que demandan redistribuir la renta disponible.

Todo esto nos devuelve al concepto de institución centralizada. Quizás los modelos de organizaciones centralizadas han quedado obsoletos y pasarán a la posteridad como un hito de éxito en el pasado, pero no como estructuras que se adapten a las necesidades, preocupaciones y contexto al que estamos evolucionando.

El monopolio de poder de las grandes instituciones financieras entra en conflicto con la necesidad de transacciones eficientes. A pesar de que la centralización surge para solucionar los costes de transacción uniendo a diferentes agentes del mercado, el contexto actual nos hace cuestionar un sistema que, teóricamente, apoya al pueblo. Dejando de lado los juicios sobre si su actuación es honesta o no, puede que simplemente no tengan más capacidad para operar con la eficiencia que las partes interesadas esperan de ellos.

Remontándonos a Adam Smith y la Ilustración escocesa, surge el concepto de la eficiencia dinámica. La eficiencia dinámica hace referencia a una maximización de la productividad y rentabilidad sustentada por la creación empresarial [15] [16].

El patrón de desarrollo en sistemas complejos y maduros está pasando de centralizado a descentralizado. Prácticamente todas las estructuras de organizaciones o sistemas conocidos comienzan a implementarse de manera centralizada porque resulta la forma más eficiente para establecer reglas, transmitir el conocimiento, crear jerarquía y dividir tareas y responsabilidades. A medida que estos sistemas crecen, van aproximándose a un punto de saturación en el cuál, la estructura centralizada pasa a ser vulnerable y las características que en un principio eran ventajosas se convierten en puntos de control para la explotación deshonesta. En los sistemas financieros centralizados, esto se traduce en inflación desmedida, corrupción y captación de pequeñas rentas.

La adaptación lleva a estos sistemas hacia la descentralización; a medida que los costes de centralización aumentan, los costes de descentralización se reducen. Se debe comprender que esta transición se está dando en la era digital del siglo XXI con avances tecnológicos y una drástica reducción en los costes de recursos de esta categoría [7].

Se ha llegado a un estadio de desarrollo en el que las innovaciones tecnológicas poseen la capacidad suficiente para minimizar o eliminar este tipo de intermediación. Cada vez es más viable que la tecnología cubra las utilidades ofrecidas por las grandes entidades centralizadas, limitando la influencia y control que éstas puedan tener y, por consiguiente, aliviando la desconfianza generalizada que hay hacia estas organizaciones. Aquí es donde entra en juego el papel de la tecnología Blockchain y las consiguientes Finanzas Descentralizadas.

2.2 ¿Qué es Blockchain y qué puede ofrecer a las Finanzas?

A continuación, se recorre la tecnología Blockchain. La intención no es profundizar en la investigación técnica sobre esta tecnología, sino que se pretende establecer un marco muy superficial, manteniendo el foco sobre las Finanzas Descentralizas, que es la materia que se desarrollará de manera más exhaustiva. Por ello, es preciso decir que hay diferentes variaciones y particularidades de Blockchain que no se tratarán aquí.

De manera simplificada, el Blockchain actúa como un gran libro mayor inalterable compartido por todos los integrantes de una red. Dicho en otros términos, es una Base de Datos replicada en múltiples nodos a la cual solo se puede adherir información. El crecimiento de esta "BBDD replicada" se gestiona en una estructura de Cadena de Bloques, que le otorga una seguridad criptográfica sin precedentes [3].

La Web 2.0 es el modelo de Internet que utilizamos actualmente, en el cual los usuarios de la red interaccionan con los contenidos y servicios ofrecidos en ella a través de diferentes capas de software, protocolos y comunicación que se acoplan para gestionarse desde una entidad central, que ofrece el servicio que se está consumiendo. [8].

El valor diferenciador que propone el Blockchain en el modelo Web 3.0 es una alternativa a la centralización: un sistema distribuido en el cual, idealmente, no hay puntos de control ni puntos de fallo. Con acceso a Internet y un alta en una red de Blockchain, puede formalizarse una transacción de extremo a extremo involucrados, sin contar con un medio de intermediación. Para evitar ser imprecisos, podríamos considerar la propia red ofrecida por la tecnología Blockchain como la plataforma o medio facilitador de la transacción, pero la disrupción radica en que el medio del que se vale es intrínsecamente descentralizado desde su origen.

Esta innovación parece estar cambiando el paradigma de las finanzas hacia la descentralización y confianza distribuida prescindiendo la necesidad de intermediación de una tercera parte confiable [9], reflejados de forma convencional en sistemas, entidades o instituciones centralizadas. La confianza distribuida es posible dado a que todas las transacciones que tienen lugar en la red son validadas, registradas en el "gran libro mayor" de manera inmutable, verificable y rastreables unívocamente.

Precisamente, las raíces de la tecnología Blockchain surgen para servir a las finanzas. El considerado padre de esta tecnología es Satoshi Nakamoto, que ideó e implementó el Bitcoin en 2008.

Es importante mencionar que existen teorizaciones previas de modelos de consenso, diferentes diseños de sistemas distribuidos funcionales e incluso soluciones reales de sistemas que sirvieron como precursores de la tecnología Blockchain y se remontan hasta tan pronto como 1981. Todos estos estudios y aplicaciones pretendían resolver la problemática de seguridad, privacidad e inclusión mediante algoritmos criptográficos.

No obstante, tuvieron que pasar décadas hasta que la tecnología, el mercado y la industria estuvieran preparados para las innovaciones que propondría Bitcoin, que fue la primera criptomoneda en funcionamiento que logró aceptación y tracción hasta el amplio reconocimiento que posee actualmente [10].

Sintetizando: todos los datos almacenados en el Blockchain son, teóricamente, permanentes e inalterables. Además, el sistema está implementado bajo protocolos de seguridad criptográficos muy eficaces y su naturaleza distribuida prácticamente imposibilita la actividad fraudulenta o maliciosa al eliminar puntos de control.

En cuanto a lo que concierne a las finanzas, las claves que ofrece esta innovación son los siguientes:

- Descentralización: eliminando la participación de instituciones centralizadas, se pueden evitar los costes de monopolio y, por consiguiente, acabar con el poder de mercado y los beneficios desproporcionados de las entidades dominantes. En esta red *Peer to Peer*, ningún participante tiene la capacidad para monopolizar el sistema.
- Interoperabilidad e inclusión. Frente a las instituciones financieras convencionales que mantienen redes independientes para sus sistemas y una diferenciación a través de fronteras geográficas, Blockchain elimina las barreras de transacción y entrada, permitiendo un flujo de capital global. Esto impulsa una *distribución* del capital y no la *redistribución* del capital que persigue el modelo socioeconómico actual. Por otro lado, presenta un sistema monetario común sin regulación de bancos centrales ni gobiernos. Además, conforma un ecosistema financiero descentralizado que acepta la innovación y promueve la cooperación. Otra ventaja a tener en cuenta es que no existe limitación horaria para la apertura y cierre de los mercados tal y como se da en el entorno financiero actual. [9]
- Laxitud regulatoria en el comercio. Al tratarse de una plataforma descentralizada, no existen importantes exigencias en la cotización de activos por parte de cualquier vendedor ni criterios subjetivos o arbitrarios impuestos por algún organismo que pueda limitar los movimientos del mercado [11].
- Transparencia. En las finanzas centralizadas no existe transparencia total; los intermediarios financieros deben restringir el acceso a sus registros internos para preservar la seguridad y privacidad de las operaciones que realizan. En contraste, la seguridad de Blockchain garantiza la veracidad de las transacciones con la propia estructura distribuida del sistema en el cuál es imprescindible un consenso global. Dado a que no se expone la identidad real de los miembros de la red, las transacciones registradas (y los agentes que las llevan a cabo) son totalmente visibles y verificables por todos los integrantes del Blockchain, permitiendo una transparencia radical. Es más, los mecanismos de auditoría tradicionales quedarán obsoletos y se evitará la concentración de poder en las grandes firmas de auditoría. De nuevo, recuperamos el concepto de confianza distribuida que hace tan atractivo esta tecnología para el sector financiero [9].

- **Valor como incentivo.** Tal y como se expuso en el planteamiento inicial del Bitcoin, la red Blockchain recompensa monetariamente a los participantes que trabajan por el mantenimiento y crecimiento de la red: los mineros. Esto no solo funciona como incentivo, sino que además actúa como un mecanismo automático de emisión de la criptomoneda de manera sostenida e inflación controlada.
- **Conservación de derechos.** Se reconocen los derechos comerciales y libertades individuales de una manera mucho más eficaz que en sistemas centralizados. No es necesaria la negociación, intermediación o moderación por ninguna entidad que pueda derivar en una alteración de los derechos originales. Tú eres dueño de tus datos, tu contenido y tus productos tal y como queda reflejado en los instrumentos producidos en el Blockchain. El posible uso o transacciones que se hagan de estos instrumentos no altera su naturaleza original.
- **Custodia del valor.** La naturaleza criptográfica de los activos en el Blockchain ofrece a los propietarios la posibilidad de controlar sus activos, sin la necesidad de confiar en una tercera parte, las instituciones financieras, como tesoreros de sus valores.
- **Gestión de riesgos.** El riesgo de contrapartida y riesgo operacional hacen referencia al riesgo del impago y el fallo de los sistemas TIC, respectivamente. La atomicidad e irrevocabilidad de los acuerdos y la seguridad en el sistema Blockchain reducen sustancialmente o eliminan estos riesgos. Se desarrollará más adelante para mayor comprensión.
- **Facilidad y accesibilidad para el intercambio de valor.** Las relaciones *Peer to Peer* que permite Blockchain, facilita el comercio de activos, instrumentos de deuda, financiación y otro tipo de acuerdos de extremo a extremo, sin la necesidad de intermediación y, por consiguiente, acortando tiempos y costes. Esta propiedad va en la línea de lo mencionado previamente con respecto a la eliminación de barreras, maximizando la inclusión de los participantes y la eficiencia de las operaciones. [10]

Por otro lado, en esta sección introductoria, se desea presentar el concepto de Contratos Inteligentes. Las criptomonedas nativas a cada red están fuertemente vinculadas a la arquitectura de cada una de ellas, pero la mayor parte de tokens, protocolos, aplicaciones y productos financieros que se superponen en el protocolo Blockchain están implementados a través de Contratos Inteligentes. En definitiva, los Contratos Inteligentes son la herramienta software que hace posible las *DeFi*.

Por esta razón, el término de Contrato Inteligente tendrá bastante presencia a lo largo de todo el trabajo debido a lo esencial de esta herramienta para las *DeFi*. Alejándonos de una perspectiva técnica, definimos Contrato Inteligente como un software o programa que plantea unas condiciones o cláusulas (tal y como se da en un contrato tradicional) y que ejecuta un/unos procesos cuando se cumplan una o varias de las condiciones propuestas.

Este software se caracteriza por su naturaleza determinista e inmutable: el programa se lanza a la red Blockchain y cumple con la función implementada en base a los inputs de los que se nutre, sin posibilidad de alterar su diseño. La interoperabilidad entre contratos inteligentes es de lo más común. De hecho, es probable que un mismo

sistema esté implementado por varios contratos inteligentes, dependiendo de su complejidad y la función que cubre.

La mayor parte de Contratos Inteligentes se programan en el lenguaje *Solidity* para la red *Ethereum*, ya que es la plataforma que más prestaciones y flexibilidad ofrece en este ámbito, permitiendo la implementación de funcionalidades muy diversas. En las próximas secciones se irá comprendiendo el papel que juegan los Contratos Inteligentes en las *DeFi*.

Uno de los aspectos más definitorios de este software es el coste implícito asociado a su ejecución. Esto, en muchos sentidos compone una optimización del entorno, ya que, entre otros beneficios, limita la saturación de aplicaciones en ejecución o una mayor calidad del código de los sistemas construidos en la red Ethereum. Sin embargo, supone un claro obstáculo para la entidad o individuo en términos presupuestarios. Se entiende que los programas convencionales llevan asociado una carga computacional que, de manera última, deriva en un coste energético que se puede medir en términos de gasto económico. Aun así, el consumo computacional asociado a la ejecución de un programa promedio puede considerarse despreciable.

Subrayamos que estamos enmarcados en el sector financiero, donde los procesos electrónicos funcionales en el software y hardware tradicional no requieren de una importante carga computacional. No obstante, en el caso de la red Ethereum, el despliegue y ejecución de los contratos inteligentes lleva implícito un gasto en gas, que no es más que una tasa de *Ether* aplicada sobre el usuario que invoca el programa y que retiene la red. Este factor será de especial consideración para algunos de los próximos apartados.

Para finalizar, recapitulamos algunas de las diferencias más significativas entre las Finanzas Centralizadas y Descentralizadas en la Figura 3:

Table 1. : A relative comparison of characteristics: DeFi vs. Traditional Finance

Characteristic	Traditional Financial Services	DeFi - Decentralized Finance
Degree of automation	Low	High
Network Structure	Centralised	Decentralized
Self-custodial	No	Yes
Trustless	No	Yes
Technology importance	Low	High
Intermediary importance	High	Low
Costs of service	High	Low
Product Focus	High	Low
Single Point of failure	Yes	No
Counterparty risk	High	Low
Anonymous	No	Yes
Inclusive	No	Yes
Transparent	No	Yes
Open Source	No	Yes
Permissionless	No	Yes
Flexibility	Low	High
Security	Low	High
Regulated	Yes	No

Figura 3: Comparación superficial entre Finanzas Centralizadas y Descentralizadas [12].

2.3 Atributos de las Finanzas Descentralizadas

En los próximos apartados se tratarán diferentes aspectos que caracterizan las Finanzas Descentralizadas: activos, instrumentos, mecánicas y otro tipo de prestaciones innovadoras. El recorrido comenzará desde los atributos más definitorios y populares hasta otro tipo de propuestas especialmente atractivas. No se pretende estudiar de manera exhaustiva estos elementos, sino que se introducen para ofrecer una visión inicial de las *DeFi*.

I. Nuevos activos digitales: monedas descentralizadas y tokens

Las monedas nacionales fiduciarias (*fiat*, en inglés) han existido durante siglos. Hasta finales del siglo XX, las monedas estaban respaldas por una equivalente cantidad en oro, que quedaba en reserva como "garantía" de la moneda oficial. Cuando se abandonó el patrón oro en los años 70, la credibilidad de la moneda quedó limitada a la propia confianza colectiva en el sistema económico, estado y organismos que emiten y sostienen dicho metálico.

Paralelamente, las criptomonedas o monedas descentralizadas son activos o medios de cambio muy líquidos dentro de las redes Blockchain y su valor no se fundamenta en la credibilidad de una economía centralizada, un Estado o instituciones oficiales, sino que se trata de confianza distribuida en toda una red descentralizada.

Tal y como se ha mencionado anteriormente, Bitcoin fue la primera criptomoneda o, en otras palabras, la primera moneda emitida por una tecnología descentralizada en lugar de por un gobierno. Actualmente existen muchas más criptomonedas y tokens en diferentes redes Blockchain, que se generan en un ritmo cada vez más acelerado [9].

Los tokens son la representación digital de bienes o servicios en el entorno del Blockchain. La emisión de tokens es, de alguna manera, similar a la emisión de valores en la banca tradicional, ya que los tokens otorgan derechos. Es un medio de cambio que se genera con una utilidad muy específica. Los tokens permiten comercializar con bienes poco líquidos como Propiedad Intelectual u obras de arte. Esta flexibilidad que existe para "tokenizar" abre nuevas posibilidades para los mecanismos y medios de comercio, trayendo consigo a diferentes perfiles de inversores con oportunidades para invertir en activos de naturaleza muy diferente a los que las finanzas convencionales ofrecen.

Clarificando: la criptomoneda es un tipo de token, ya que sigue siendo un activo digital. Sin embargo, las criptomonedas son un medio de pago, no de cambio, y funcionan como una reserva de valor (y ahorro) dado a que generalmente, su liquidez es mucho mayor. Otro criterio para diferenciar criptomonedas y tokens es su naturaleza nativa al Blockchain específico. Es decir, Bitcoin o Ether serían tokens nativos a las redes Bitcoin y Ethereum respectivamente; son criptomonedas que extraen los mineros en sus redes asociadas. Por ello, los tokens pueden utilizar las redes de Bitcoin o Ethereum para operar, aunque no sean las monedas nativas de esos sistemas [13] [14] [12].

II. Inflación monetaria automatizada

La inflación se refiere a un incremento generalizado del precio de los bienes y servicios del mercado e implica que la moneda (del sistema financiero pertinente) se devalúa. En las finanzas tal y como se conocen actualmente, es mayoritariamente aceptado que la inflación se da tras una ampliación de la oferta monetaria, aunque no es estrictamente necesario [9].

En los sistemas económicos centralizados, la emisión de la moneda recae sobre la autoridad o banco central, y por lo tanto son los responsables de regular la inflación. Normalmente, la inflación se ajusta con referencia en el IPC (Índice de Precios al Consumidor). Algunas de las críticas a este sistema es la poca representatividad que tiene el IPC o el diferente impacto de dicho índice sobre los diversos estratos sociales. Por otra parte, la inflación motiva la inversión para evitar incurrir en pérdidas de valor de capital.

Las monedas fiat solían tener una emisión fija hasta la suspensión del patrón oro. Criptomonedas como Bitcoin tiene un calendario fijado de oferta monetaria que busca una evolución anti-inflacionaria. Por el otro lado, hay criptomonedas se emiten de manera variable. La emisión fija de Bitcoin también evita que el valor de la moneda caiga abruptamente.

El establecimiento precursor de Bitcoin lo ha convertido en la reserva principal de valor en el mundo Blockchain y, además, le ha otorgado una posición de barómetro o *Blue Chip* en esta industria: muchos criptoactivos se comercian contra Bitcoin. De alguna forma, Bitcoin hace el papel que cubre el oro en las finanzas tradicionales.

Con el escaso recorrido de esta forma de finanzas, es difícil esclarecer si un algoritmo fijo de emisión de criptomoneda es más conveniente que uno variable. Igualmente, numerosos agentes de las Finanzas Descentralizadas consideran las criptomonedas como medio para desvincularse de la influencia de bancos centrales [11].

III. Stablecoins, una opción menos arriesgada

Los stablecoins son un tipo de activo digital que pretende ser una alternativa para aquellos inversores que prefieren comerciar con valores menos volátiles que las criptomonedas. Para minimizar la fluctuación de precios de los stablecoins se hacen uso de distintos mecanismos:

El sistema más común para fijar el valor de la stablecoin es el de Reservas de Divisas Fiat Vinculadas, que consiste en respaldar su precio en una moneda fiat almacenada en una reserva. Cuando el precio del stablecoin cae por debajo del valor fijado, se compran stablecoins para reducir la oferta monetaria, mientras que cuando el precio se incrementa, se generan más stablecoins. En definitiva, se pretende mantener un tipo de cambio constante entre la stablecoin y la reserva de fiat. La adversidad que presenta este sistema es que es necesaria la incorporación de una tercera parte confiable para la

administración de la reserva de monedas fiat y, por lo tanto, este mecanismo falta al principio de descentralización.

Dos procedimientos alternativos que respetan la pauta de descentralización son los Préstamos Apalancados (Leveraged Loans) y la Oferta de Ajuste Algorítmico (Alorithmic Supply Adjustments). Los Préstamos Apalancados funcionan de la similar manera que las Reservas de Divisas Vinculadas, pero en este caso, el stablecoin está respaldado por una criptomoneda que queda custodiada mediante un contrato inteligente. Por el otro lado, la Oferta de Ajuste Algorítmico logra regular la generación de stablecoin de manera automática (normalmente mediante contratos inteligentes) en función a la fluctuación de precio [11]. Recordamos que los contratos inteligentes operan de manera descentralizada.

IV. Pago de extremo a extremo

Las soluciones de pago telemáticas actuales se categorizan como sistemas de pago centralizados: Visa, SWIFT o PayPal. Existen otros medios de pago telemáticos implementados en las redes de las entidades financieras, pero generalmente, tal y como se ha mencionado con anterioridad, no promueven la interoperabilidad. Por otra parte, estos servicios de pago cobran unas tasas que pueden llegar a ser significativamente elevadas, especialmente cuando se tratan de transacciones internacionales. A pesar de que Internet ha reducido los costes en diversos servicios financieros, las comisiones de los pagos telemáticos continúan siendo significativas.

Las redes de pago descentralizadas ofrecen una alternativa que es, no solo más económica, sino que ofrece ventajas de instantaneidad, mayor alcance e irreversibilidad. Esto reduce sustancialmente los costes de transacción para las empresas, motivando la viabilidad de negocios emergentes pequeños y abriendo nuevas puertas para nuevos servicios de pagos. *Libra* o *Bitcoin Lightning Network* son algunas de las empresas que ofrecen estos servicios. [9]

V. Captación de fondos descentralizada

En el sistema financiero convencional, la captación de fondos suele requerir la promoción de una entidad confiable, lo cual puede dificultar el acceso a la financiación para *start-ups* y otros nuevos proyectos que cuentan con escaso respaldo.

Blockchain está cambiando el entorno con diferentes formas de financiación como ICO (Initial Coin Offering). Un ICO es un mecanismo de crowdfunding por el cual un nuevo proyecto emite un token específico vinculado a su proyecto en una red pública de Blockchain y venderlo a potenciales inversores para obtener financiación en las primeras fases de desarrollo del proyecto.

Los ICO pueden minimizar la fricción en la financiación, facilitando el acceso al capital e impulsando el emprendimiento. Más aún, los ICO promueven la creación de ecosistemas, cuando el propio token actúa como una garantía de servicios u otras

facilidades entre los grupos de interés y el proyecto financiado [9]. Se volverá a este concepto en futuras secciones.

VI. ¿Y el blanqueamiento de capitales?

Bajo el principio de transparencia del Blockchain, la tarea de blanquear el dinero se vuelve más compleja. No obstante, existen servicios "mixer", gestionados de manera centralizada o por contratos inteligentes, que mezclan los activos de unos usuarios con los de otros, de forma similar al blanqueamiento de dinero en las finanzas convencionales.

Técnicamente, en caso de que se lleven a cabo este tipo de operaciones con objetivos ilícitos, la cantidad o naturaleza de los activos y la *pseudoidentidad* los usuarios involucrados pueden ser señalados, ya que todos los parámetros de la operación quedarán reflejados en el Blockchain [11].

VII. ¿Más seguro? Imposible

En las finanzas centralizadas, el negocio de los seguros es una industria multimillonaria. Estas entidades suelen involucrar múltiples agentes en diferentes niveles de intermediación y las relaciones contractuales que mantienen con sus clientes son objeto de deliberación desde la perspectiva legal por la ambivalencia que puede llegar a orecer en muchas ocasiones.

La transparencia y naturaleza distribuida del Blockchain puede ayudar a democratizar este negocio, favoreciendo siempre los intereses comunitarios por encima de la rentabilidad de una entidad. En este hilo, puede servir como plataforma para centrar su funcionalidad como red de seguridad orientada a lo social.

Aunque las finanzas descentralizadas, idealmente, no sostienen riesgo operativo, la realidad es que existen múltiples amenazas que pueden poner en peligro los fondos de los inversores, y debido a la irreversibilidad que caracteriza al Blockchain, la recuperación de estos flujos es más bien improbable. Por ello, los seguros en DeFi juegan un papel fundamental.

Los seguros descentralizados actúan como un colchón amortiguador en el ecosistema de las DeFi: durante los últimos años, los inversores han perdido miles de millones de dólares en activos digitales por la mala custodia de las claves privadas, operaciones gestionadas erróneamente y diversos tipos de ataques. Solo en 2021, se estiman pérdidas de hasta 10.000 millones [15].

La finalidad de los seguros en el entorno de las DeFi es distribuir el riesgo entre todos los participantes. De la misma forma que sucede en las aseguradoras convencionales, se pueden cubrir tanto factores y causas externos a las finanzas como seguros para minimizar el riesgo de operaciones financieras.

Por ejemplo, *NexusMutual* permite asegurar los fondos gestionados a través de contratos inteligentes de la red Ethereum. La participación en el fondo de riesgo compartido se representa a través del token NXM. Por otra parte, *Etherisc* ha implementado una infraestructura común que ofrece productos "plantilla" personalizables que dan gran flexibilidad al cliente a la hora de crear el tipo de seguro que necesita: desde cobertura para el retraso de un vuelo hasta la protección de un aval. *CDx* responde a una de las necesidades más crecientes en las finanzas descentralizadas: protección en los activos involucrados en "Exchanges" [16].

VIII. Derivados y sintéticos financieros

Los derivados financieros son contratos ampliamente conocidos en las finanzas centralizadas. El valor obtenido de los derivados financieros se fundamenta en el desempeño que tenga el activo subyacente al acuerdo. Principalmente se opera con los derivados financieros bajo dos escenarios:

- Protección de la fluctuación de valor de un activo. Esto se formaliza a través de un acuerdo en el que se fija de antemano el precio al que se comprará/venderá el subyacente en un momento dado.
- Buscar beneficio especulando sobre la evolución del precio del subyacente en el futuro o a través del arbitraje [12].

Los principales derivados financieros son: futuros, forwards, opciones y swaps.

- Los futuros otorgan derecho y obligación a realizar la compra/venta en momento y a precio determinados de antemano.
- Los forwards son muy similares a los futuros, pero más flexibles a ambas partes del contrato.
- Las opciones otorgan el derecho, pero no la obligación, a realizar la transacción.
- Por último, los swaps acuerdan el intercambio de dos tipos diferentes de flujos de efectivo.

Existen otros sintéticos financieros que flexibilizan el comportamiento de ciertos activos para adaptarse a las necesidades e intereses de los agentes [15] [16]. Dado a que estos instrumentos instalan su funcionamiento en una relación contractual, las herramientas que ofrecen las *DeFi* pueden ser significativamente convenientes para potenciar este comercio a través de contratos inteligentes que se ejecutan de manera autónoma y automática [16].

IX. Préstamos millonarios a todo riesgo: Flash Loans

Los *Flash Loans* o Préstamos Flash son una nueva forma de préstamo que solo es posible en las Finanzas Descentralizadas debido a el principio de atomicidad bajo el que funcionan las tecnologías Blockchain y los contratos inteligentes. Con este innovador instrumento financiero producido mediante contratos inteligentes, tienen lugar las siguientes transacciones en una sola operación:

1. El usuario solicita el préstamo en un fondo de flash loans.
2. El solicitante hace uso del monto del préstamo de manera arbitraria
3. Se devuelve el préstamo (más intereses) al fondo.

La atomicidad con la que sucede esta operación evita que el solicitante tenga que ofrecer aval o cualquier tipo de garantías ya que, en caso de que el préstamo no pueda ser devuelto, la operación se revocará y no se dará por completa, como si el préstamo nunca hubiese tenido lugar. Por esta razón, los prestamistas siempre tienen la seguridad de que se amortizarán sus pagos y recibirán interese [11].

X. Arbitraje

El Comercio de Alta Frecuencia *o High Frequency Trading* (HFT) hace referencia a estrategias automatizadas de comercio que se aprovechan de las fluctuaciones del mercado a corto plazo. Esto ya es posible dentro de los mercados centralizados gracias a la digitalización del comercio.

El arbitraje es la práctica más común de HFT. Se vale de la diferencia de precios en mercados distintos. Los beneficios se generan con la compra de un activo en un mercado A, a un precio a, vendiéndolo inmediatamente después en un mercado B, a un precio superior b.

En el arbitraje en las finanzas centralizadas, se pretende ganar una ventaja competitiva al minimizar la latencia intentando atomizar la compra y venta del activo en cuestión para eludir el riesgo por fluctuación de precios, sin llegar a lograr una operación 100% atómica.

En las finanzas descentralizadas, la latencia se disminuye con mayor poder computacional y ejecución en múltiples nodos, mientas que la atomicidad es perfectamente alcanzable gracias a los contratos inteligentes [11].

3 Plataformas de Intercambio de Activos y Automated Market Makers

Una vez se han dado a conocer los productos, instrumentos y nuevas posibilidades de comercio en las *DeFi*, es imprescindible lograr comprensión sobre los mercados o entornos donde se comercia con dichos activos. Es aquí donde subyace gran parte de la innovación tecnológica propuesta por las Finanzas Descentralizadas.

3.1 Hola a los Exchanges

En febrero de 2022, se superó la barrera de los 10.000 criptoactivos [17] en mercados descentralizados. A pesar de que la mayoría de ellos no son especialmente relevantes, otros han logrado posicionarse como importantes depósitos de valor dentro de la industria. Tanto para los primeros criptoactivos como todos los generados en este momento de expansión, es fundamental la existencia de plataformas que permita el comercio de esta categoría de producto en proceso de explotación.

Un "Exchange" (por su terminología en inglés), es un mercado donde se comercian instrumentos financieros. Es decir, son entornos primordiales para soportar la actividad esencial del comercio financiero. Pese a su origen como espacio físico, estas plataformas han evolucionado hacia un soporte electrónico en la era digital. Los 3 componentes más característicos de los *exchanges* electrónicos son [11]:

- Mecanismo de descubrimiento de precio mediante el cual las partes de oferta y demanda se encuentran para satisfacer sus intereses [18].
- Motor algorítmico de comercio que permite ejecutar transacciones de diferente índole en diferentes mercados, de manera flexible y contando con la disponibilidad de información de diferente naturaleza o históricos de datos. Además de la obvia eficiencia y capacidad que estos sistemas otorgan a los agentes individuales, la reducción de la latencia es lo que resulta más conveniente de la implementación algorítmica [19].
- Sistema de liquidación y compensación de activos, que materializa el traspaso de activos hacia ambas partes involucradas en la transacción [20].

Frente a la eficaz funcionalidad que ofrecen, estas plataformas de comercio han sido adoptadas por las *DeFi*. La modalidad original de Exchange que se implementaron en los mercados descentralizados fueron los CEX o *Centralized Exchange*. Tal y como indica este término, son sistemas centralizados y se adhieren a la estructura paradigmática de las finanzas convencionales.

Con la expansión de las *DeFi*, esta implementación se trasladó a la tecnología Blockchain en sus inicios para establecerse como el formato de mercado más común para los activos digitales. A pesar de que son sistemas caracterizados por su eficiencia

en comparación a otros modelos de mercado, los CEX plantean varias debilidades que van cogidas de la mano:

a) Los usuarios de estas plataformas deben transferir o depositar los valores que desean cambiar para iniciar la transacción, lo que implica confianza en la plataforma y agentes intermediarios involucrados en la operación.
b) Los CEX contradicen el principio de distribución y descentralización que persigue la tecnología Blockchain y las DeFi. La centralización del mercado supone potenciales vulnerabilidades del sistema ante ataques.
c) La desregulación de los CEX (y DeFi en general) genera aún más riesgo.

Los DEX o *Decentralized Exchanges* pretenden resolver estas deficiencias de los CEX. Esto se consigue al eliminar la necesidad de custodia por una tercera parte confiable centralizada; es decir, el usuario estará en posesión de sus valores hasta el momento exacto de la ejecución de la transacción. Por otra parte, la ejecución de esta transacción mitiga totalmente el riesgo a impago dado a que se procesa de manera atómica a través de contratos inteligentes: la transacción se completa únicamente si las partes implicadas han cedido los fondos a intercambiar. De esta forma, se puede generar un mercado descentralizado, seguro y que coloca la custodia de los valores en sus propietarios [21].

Actualmente, existen diferentes paradigmas para *Exchanges*, principalmente diferenciados por el mecanismo de descubrimiento de precios. La mayoría de ellos están implementados en la red Ethereum dado a las prestaciones y flexibilidad que ofrecen los Contratos Inteligentes de esta red con respecto a otras como Bitcoin.

3.2 Decentralized Order Book Exchanges vs Automated Market Makers

En las finanzas centralizadas es ampliamente conocido el modelo de *Order Book* o Libro de Pedidos como núcleo de los mercados financieros. Con esta herramienta se mantiene registro de las órdenes abiertas de oferta y demanda fijadas por compradores y vendedores. Cuando dos partes satisfacen sus intereses recíprocamente, el acuerdo se cierra.

Los *Order Book* DEX hacen uso del modelo preexistente de *Order Book* adaptándolo a la tecnología Blockchain para su operatividad descentralizada. Este protocolo utiliza contratos inteligentes para el procesamiento de las transacciones, pero existen diferentes formas de abordar su implementación en función de cómo se almacena el registro del Order Book: "on-chain" u "off-chain", o bien "en la cadena" o "fuera de la cadena" [12]:

- *On-chain Order Book DEX*. Cuentan con un mecanismo completamente descentralizado: todos los registros se almacenan en un contrato inteligente en el Blockchain Así, se evita la intermediación de una tercera parte o el soporte de una infraestructura adicional. Además, se facilita la verificación pública. No obstante, esta implementación es lenta y costosa, ya que cada operación que tiene lugar en este mercado, requiere de interacción con el Blockchain, lo que implica tasas y tiempo de procesamiento.
- *Off-chain Order Book DEX*. Surgen como mejora del modelo anterior. Estos sistemas utilizan el Blockchain como capa de cimentación, pero implementan otras capas de abstracción para la gestión del sistema. De esta forma, el mecanismo se hace más eficiente, rápido y barato. En el sistema se alberga una mayor capacidad operativa limitando las interacciones con la red Blockchain a lo esencial. Aunque es necesario contar con una plataforma centralizada como tercera parte confiable, el poder de ésta sobre los fondos es bastante reducido: su influencia se reduce al mecanismo de descubrimiento de precio.

El mecanismo de *Order Book* era el óptimo para el contexto de las *CeFi*, sin embargo, con la irrupción de las *DeFi* y todas las innovaciones consecuentes, este sistema queda algo obsoleto ante las posibilidades de automatización de los mercados.

Los *Automated Market Makers (AMM)* o Creadores de Mercados Automáticos son, una evolución de los *Exchanges* originales. El valor diferencial de estas plataformas de intercambio radica en la gestión automatizada del líquido del fondo gracias a los Contratos Inteligentes. De esta forma, la plataforma no actúa como entorno de comercio donde los compradores y vendedores acuerdan directamente para satisfacer su oferta y demanda, sino que la base programática en *smart contracts* de los AMM permite que estas operaciones de intercambio se efectúen sin previo acuerdo de las partes interesadas, maximizando la eficiencia a la vez que reduciendo tiempos y costes [11].

Los *Market Makers* son agentes que ya se conocen de las Finanzas Centralizadas. Estos intermediarios financieros actúan como compradores y/o vendedores inmediatos de activos que obtienen beneficio de la diferencia entre el precio de compra y venta a la vez que facilitan el mecanismo de descubrimiento de precio ya que eliminan la presencia simultánea de compradores y vendedores [22]. Los *Automated Market Makers* se quedan con lo mejor de los *Exchanges* y *Market Makers* ya conocidos en CeFi para potenciarlo más aún con la tecnología Blockchain.

Los AMM establecen un precio al que los agentes del mercado pueden comprar y vender sus activos. Esto difiere de manera muy notable con los sistemas basados en el paradigma *Order Book,* en los que la oferta y la demanda debe coincidir para que se ejecute el intercambio. Por ello, los AMM resultan especialmente beneficiosos en mercados en los que la brecha entre precios de compra y de venta es más amplia.

Cuando los AMM actúan como contrapartida de la operación de compra o venta, se convierten en un "embudo" canalizador del comercio incluso en los mercados menos cotizados con criptoactivos específicos o poco comunes. Por otra parte, de la misma forma que los *Market Makers* convencionales, promueven la estabilidad de precios a través del arbitraje y la flexibilidad de operaciones [23].

Este mecanismo huye de la burocracia y control, mientras que mantiene la seguridad gracias a su cimentación criptográfica. Por otro lado, prescindir de los procesos "Know Your Customer" permite una reducción muy importante de los costes de transacciones con respecto a, no solo las Finanzas Centralizadas, sino también las soluciones mayoritariamente implementadas en los *Exchanges*. Esto facilita y motiva aún más los flujos de efectivo entre proveedores de líquido y agentes deficitarios de crédito, impulsado la financiación e innovación.

En los AMM es primordial la funcionalidad ofrecida por los *Liquidity Pools*. Estas "piscinas de liquidez" son una reserva de criptoactivos que actúa como fuente de líquido de los AMM, para las operaciones que se llevan a cabo con los compradores o vendedores. Esta reserva está administrada de manera segura mediante contratos inteligentes.

Hay diferentes maneras de abordar la implementación de los Liquidity Pools según la funcionalidad que se quiera cubrir en el AMM. Por ejemplo, el AMM puede servir como fuente de financiación, crédito de un criptoactivo específico a corto plazo o como plataforma de cambio de valores. En consecuencia, los *Liquidity Pools* funcionarán como *Lending Pools, Swap Pools etc.*

Los proveedores de liquidez que nutren los *Liquidity Pools* no son más que agentes con superávit de fondos, participantes del mercado, que está incentivados a depositar su exceso de líquido (o ahorro) en estas reservas. A cambio del uso de su capital, reciben, de manera proporcional a la inversión inyectada, parte de los intereses aplicados a los comerciantes que hacen uso de los servicios de los AMM.

La participación de los *Liquidity Providers* (LP) o Proveedores de Liquidez en el valor del fondo será representada a través de unos *Liquidity Tokens* o Tokens de Liquidez. Estos tokens serán percibidos por los LP una vez realicen el ingreso de fondos y, más adelante, en el momento de retirar los fondos del *Liquidity Pool*, deberán acreditar la posesión de dichos tokens. El Fondo de Liquidez emitirá más Tokens de Liquidez a medida que crece su valor mientras que "quemará" estos "derechos" cuando se retiren participaciones (y liquidez) del fondo.

Recapitulando, en los sistemas de los AMM, hay involucrados dos tipos de agentes: los proveedores de liquidez y los operadores que desean intercambiar valores u obtener algún tipo de financiación o crédito. Los primeros actúan como fuente de liquidez para que los AMM puedan funcionar como contrapartida para los segundos [24].

En los AMM el precio se fija de manera algorítmica. Aun así, en este último caso, ¿cómo se garantiza que el AMM refleje las condiciones reales de oferta y demanda del mercado? [23]

- El mecanismo más común es el **arbitraje**. Recordamos que el arbitraje (en *DeFi*) busca beneficio a través del margen de diferencia de la compra y venta de criptoactivos en diferentes mercados. Los agentes que se valen de esta táctica también realizan una tarea "accidental" de alineamiento de precios. Es decir, las diferencias que puedan existir entre diferentes mercados se mitigan u homogeneizan a través del arbitraje.
- Otro de las herramientas fundamentales son los **Oráculos**. Un Oráculo es esencialmente una fuente de información que se nutre de datos externos a la plataforma e incluso externos al ecosistema Blockchain y que actúa como referencia para la actividad que suceda en el sistema específico que lo implementa.

Para concluir, se podrá sintetizar que los *Automated Market Makers* ofrecen un protocolo *Peer-to-Contract* frente a los modelos convencionales de Order Book que funcionan como Peer-to-Peer [25].

El inicio del *Yield Farming*

A mitad de 2020, los AMM vivieron un momento de expansión extraordinario que logró inyectar miles de millones de dólares en estos fondos de liquidez, convirtiéndose en uno de los segmentos fundamentales de las Finanzas Descentralizadas. En el momento que se escribe el presente documento, en torno a 75 mil millones de dólares están almacenados en DEX implementados con *Automated Market Makers*, aunque esta cantidad ha llegado a superar los 100 mil millones [26].

Una de las pioneras de esta industria es AMM es *MakerDAO*, creada en 2015. Este sistema permite a los usuarios obtener su stablecoin *Dai* a través de un préstamo. Debido al pseudoanonimato del Blockchain, el préstamo no se financia a través de una

línea de crédito convencional, sino que se "sobrecolateraliza" con un depósito de otro valor, normalmente Ethereum.

"Sobrecolateralizar" significa que la inversión requerida de Ether para obtener el préstamo es superior al valor ofrecido en Dai (entre un 70 y 90%). Así se logra margen suficiente para amortiguar la alta volatilidad de la criptomoneda y, por lo tanto, que el valor del aval pueda quedar siempre vinculado al valor del préstamo concedido. En el momento en el que el valor del colateral cae por debajo del valor del préstamo, el aval se liquida automáticamente en un Exchange [16].

Por otra parte, el token *Maker* (MKR) ofrecido por *MakerDAO* otorga competencias de gobernanza a los usuarios que lo posean sobre el DAO que administra este sistema [27]. En este nivel, introducimos el término "Decentralized Autonomous Organization" o DAO, que son organizaciones que carecen de dirección y gestión humana, sino que están codificadas a través de contratos inteligentes. Son entidades totalmente democratizadas, cuya estrategia estará definida por el consenso de los miembros integrantes [28].

Otra solución muy popular es *AAVE*, que atiende tanto a prestamistas como prestatarios que se benefician del intercambio de Ether o tokens circulantes en la red de Ethereum. Normalmente, los proveedores de líquido esperan recibir intereses de los fondos ofrecidos, mientras que los prestatarios utilizan los activos digitales del fondo como una línea de crédito a corto plazo o incluso como aval para otro tipo de inversión [29].

En este entorno multimillonario, se acuña el término *Yield Farming* o "Cosecha de Rendimientos", que ha tenido mucha resonancia en los últimos años. Se refiere al conjunto de estrategias de inversión mediante las que un poseedor de criptomonedas u otros activos digitales intenta multiplicar la rentabilidad de su capital.

El término alcanza su máxima expresión con *Compound*. Es un protocolo similar al de AAVE, con un valor diferencial en el mecanismo de recompensa: los prestamistas y prestatarios que se benefician del sistema reciben un token de gobernanza por su participación. Por ello, el término de cosecha de rendimientos ya no solo se refiere a los intereses que puede percibir el agente que canaliza su ahorro hacia estas plataformas, sino que además se obtiene rentabilidad de otro tipo de incentivos obtenidos de la inversión como COMP.

Haciendo un símil; un hipotético *yield farming* en finanzas centralizadas podría consistir en movilizar los fondos particulares para maximizar la consumición o inversión en empresas que ofrezcan a cambio bonificaciones, descuentos o incluso propias acciones de la empresa. Debido al ecosistema *High Frequency Trading* en DeFi, esta lógica se vuelve perfectamente viable y rentable.

Condensando: diferentes plataformas de los mercados descentralizados están incentivando a los agentes a involucrarse en sus sistemas (ofreciendo liquidez o

realizando transacciones de diverso tipo) otorgando a cambio un token de gobernanza, intereses muy atractivos u otro tipo de ventajas que crean valor a los agentes.

Desde que comenzó a ofrecerse el token de gobernanza COMP a prestamistas y prestatarios en junio de 2020, muchos usuarios de finanzas descentralizadas han apostado por abarcar toda la cantidad posible de COMP, maximizando sus operaciones de préstamo y deuda. Este negocio ha sido tan popular que han surgido múltiples aplicaciones e iniciativas que facilitan y hacen más eficiente el proceso de *Yield Farming* a los usuarios a cambio de unas comisiones.

Generalmente, estas estrategias implican un apalancamiento importante: un mismo usuario se endeuda para obtener activos digitales que después utilizará para convertirse proveedor de líquido en otro fondo. Este proceso se repite sucesivamente incrementando las bonificaciones percibidas, además del apalancamiento y, por lo tanto, el riesgo asociado a ello [16].

3.3 Constant Function Market Maker (CFMM)

Es el mecanismo más común bajo el que operan los AMM. Se aplica sobre un *Liquidity Pool* que dispone de, al menos, dos criptoactivos diferentes; aunque su implementación más popular es en forma de par. El CFMM se basa en el modelo del producto constante que garantiza que el producto de la cantidad de los criptoactivos almacenados en el repositorio es siempre constante [23].

El algoritmo sobre el que funcionan los CFMM normalmente está adaptado y modificado para controlar el tipo de cambio. Igualmente, el mecanismo más simplificado bajo el que operan estos sistemas busca satisfacer la siguiente ecuación:

$$a \cdot b = k$$

Donde *a* y b corresponden a la cantidad de tokens A y B contenidos en el Liquidity Pool y *k* es una constante que se define en cada *Liquidity Pool* según la cantidad de líquido del que dispone la reserva en ese instante concreto [21]. Cuando se alteran las cantidades de *a* o *b*, se observa que:

$$(a + \Delta a) . (b + \Delta b) = k \qquad \Delta b = (k/(a + \Delta a)) - b$$

Esto demuestra que la variación de *a* y b es inversamente proporcional: el valor de *a* se verá negativamente afectado con un incremento de b, y viceversa.

Los AMM pueden funcionar con otro tipo de curvas, pero el modelo del producto constante suele ser el más adecuado dado a que su convexidad asegura el crecimiento o decrecimiento monótono del valor en base a su disponibilidad en el Liquidity Pool. La función implementada por estos AMM no es más que la curva que genera el producto de a y b.

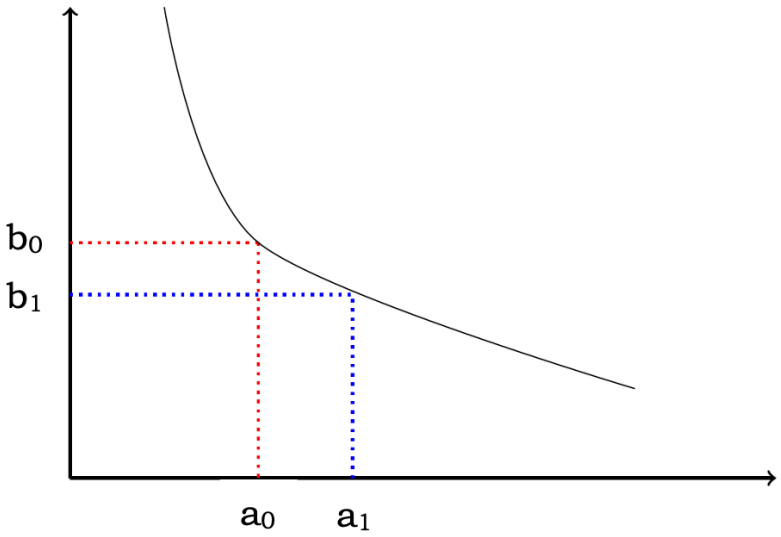


Figura 4: *Curva de CFMM [30].*

Si consideramos a_0 y b_0 como las reservas iniciales comprendidas en el Liquidity Pool, para un depósito de $a_1 - a_0$, el proveedor de liquidez obtendrá un monto de $b_0 - b_1$ a cambio. En esta representación no se ha contemplado la cuota que reciben los proveedores de liquidez a efectos de facilitar la explicación. Ejemplificando con números. Las condiciones base para una piscina de liquidez del par A ⇌ B son:

- Hay una cantidad inicial de $a_0 = 10$ y $b_0 = 100$.
- Bajo los parámetros anteriores, $k = 1000$.

Un agente se involucra para cambiar 90 unidades del criptoactivo A por B:

1. La nueva cantidad de $a_1 = 10 + 90 = 100$.
2. Dado que se debe cumplir la condición $a_1 \cdot b_1 = k$, $b_1 = k/a_1$ o $b_1 = 1000/100 = 10$
3. La cantidad percibida del criptoactivo B será $|b_1 - b_0| = |10 - 100| = 90$.
4. Por ello, en estas condiciones del AMM, 90 uds de A equivalen a 90 uds de B.

Se puede observar que, si llevamos a cabo la operación inversa en el contexto derivado de la operación anterior, se obtiene el mismo cambio. Es decir, el *swap pool* de A ⇌ B se presenta como: hay una cantidad inicial de $a_0 = 100$ y $b_0 = 10$ y $k = 1000$.

Si realizamos el cambio de 90 unidades de B para obtener A:

1. La nueva cantidad de $b_1 = 10 + 90 = 100$.
2. Dado que se debe cumplir la condición $a_1 \cdot b_1 = k$, $a_1 = k/b_1$ o $b_1 = 1000/100 = 10$
3. La cantidad percibida del criptoactivo A será $|a_1 - a_0| = |10 - 100| = 90$.
4. Se mantiene el cambio: 90 uds de B equivalen a 90 uds de A.

A continuación, se representa de manera esquemática este proceso de swap [31]:

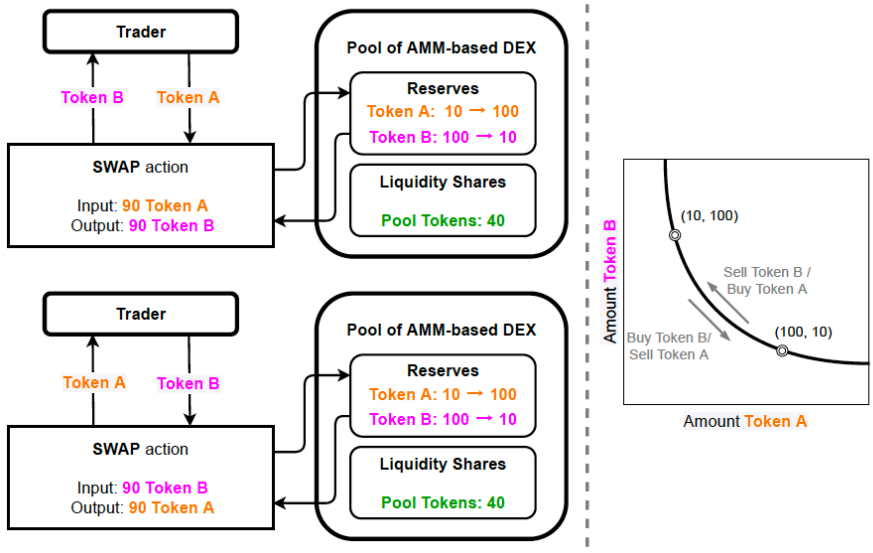


Figura 5: Swap A ⇌ B [26].

En el ejemplo anterior, se ve cómo el ratio de cambio permanece igual debido a que se han realizado movimientos inversos en curvas simétricas. Es decir, la primera operación nos ha movido de (100, 10) a (10, 100) mientras que la segunda ha vuelto a desplazar el punto (10, 100) al lugar original (100, 10).

Si tratamos movimientos inversos en la misma curva de la que partíamos al principio, observamos cómo el cambio es totalmente diferente. En este caso, deseamos vender 3 uds del criptoactivo A para percibir B, con $a_0 = 10$, $b_0 = 100$ y $k = 1000$:

1. La nueva cantidad de $a_1 = 10 + 3 = 13$.
2. Se satisface la ecuación $a_1 \cdot b_1 = k$, $b_1 = 1000/13 = 76.923$
3. $|b_1 - b_0| = |76.923 - 100| = 23.007$
4. Para la operación de venta de A y compra de B, 3 uds de A equivalen a 23.007 uds de B.

En oposición, partiendo nuevamente de $a_0 = 10$, $b_0 = 100$ y $k = 1000$, deseamos recibir 3 uds de A a cambio de un ingreso del criptoactivo B:

1. $a_1 = 10 - 3 = 7$.
2. $a_1 \cdot b_1 = k$ lleva a $b_1 = 1000/7 = 142.858$
3. $|b_1 - b_0| = |142.858 - 100| = 42.858$
4. Para la operación de venta de B y compra de A, 3 uds de A equivalen a 42.858 uds de B o 42.858 uds ofrecidas de B equivalen a 3 uds de A.

Con este ejemplo, se ve que ambas operaciones presentan unos ratios de compra y venta de A (o venta y compra de B) no simplemente desiguales, sino que difieren en magnitudes muy grades. Siguiendo el mismo procedimiento con cambios mucho más reducidos:

a) Si se cambia 0.1 uds de A obtendríamos 0.9901 uds de B.
b) Si se desea obtener 0.1 uds de A, deberíamos vender 1.0101 uds de B.

Ahora, la diferencia entre el ratio de compra y venta es significativamente inferior. Esto se debe a que operar con magnitudes grandes (en relación a la cantidad de liquidez total) provoca grandes fluctuaciones entre los cambios de compra y venta, mientras que, a medida que disminuye la cantidad del criptoactivo a comprar o vender, el ratio de compra y venta se aproxima. En concreto, en este último ejemplo, el ratio de compra y venta converge en 1.

Por otro lado, tal y cómo se ha mencionado anteriormente, la constante *k* dependerá de la cantidad de líquido contenida en Fondo de Liquidez, por lo que *k* se ajustará en caso de que haya una inyección o retirada de líquido. No obstante, la entrada o salida de liquidez no se puede dar de manera arbitraria, ya que se desea mantener la función de conservación que permite la propiedad de invarianza [32].

En otras palabras, la modificación de las magnitudes de los tokens A y B puede alterar la forma de la curva y, por lo tanto, los ratios de compra y venta del par A ⇌ B. Por ello, pueden darse dos situaciones diferentes [24]:

a) Aún no existen tokens en la reserva del *Liquidity Pool,* porque está vacía o porque se acaba de crear. En este caso, el LP podrá inyectar la cantidad que desee de tokens A y B. A cambio recibirá $\lambda = \sqrt{x \cdot y}$ tokens de liquidez.
b) Ya existen unas reservas de los tokens A y B en magnitudes a y b y por lo tanto ya existe tipo de cambio a/b. Para mantener dicha proporción, el LP solo podrá hacer ingresos δ que cumplan $\frac{\delta_a}{\delta_b} = \frac{a}{b}$. El LP recibirá a cambio a $\lambda \cdot \delta_a/a$ (o lo que es lo mismo $\lambda \cdot \delta_b/b$) Tokens de Liquidez recién emitidos y que se añadirán a los ya emitidos.

La retirada de liquidez sigue el mismo procedimiento a la inversa. Se desea puntualizar que, en la mayoría de protocolos, a la hora de reclamar los fondos, no es estrictamente necesario extraer toda la participación, sino que es posible solicitar cualquier cantidad (menor que el depósito inicial) que conserve la invarianza del ratio a/b. En la siguiente figura se representa este proceso:

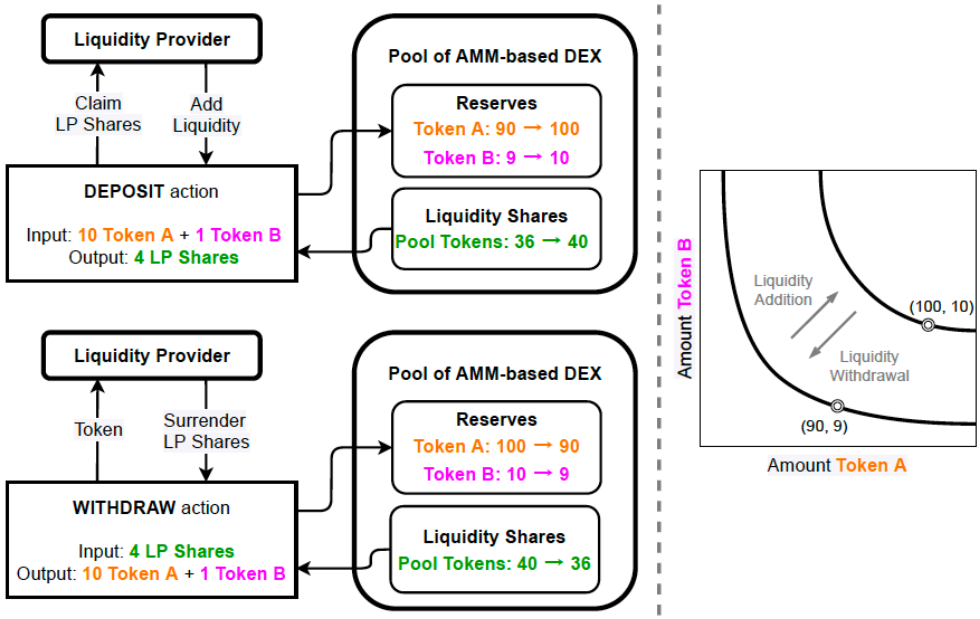


Figura 6: Inyección y retirada de Liquidez en A ⇌ B [26].

Con lo que se ha recorrido, se pueden establecer dos reglas generales a modo de síntesis [31]:

1. Movimientos en la curva. La constante *k* mantendrá su propiedad de invarianza mientras sólo se produzcan operaciones de *swapping* (o cambios de tokens) de mano de los corredores.
2. Movimientos de la curva. Agregando o sustrayendo liquidez del fondo, a través de los *Liquidity Providers*, el precio de los tokens contenidos en el *Swap Pool* permanece constante y, por tanto, el tipo de cambio también.

Antes de finalizar esta sección, se desean exponer dos costes implícitos o riesgos a los que se exponen los agentes que operan en AMM [31]:

a) Deslizamiento o *slippage*. Este término alude a la diferencia entre el precio spot y el precio realizado, es decir, el precio al que se espera realizar la transacción vs el precio al que finalmente se ejecuta. El deslizamiento se realiza en el intervalo que transcurre entre el lanzamiento de la orden y la finalización de la ejecución. Por ello, está condicionado directamente por la latencia. Ya se sabe que las tecnologías *DeFi* minimizan la latencia, pero aun así, hay otros factores que pueden motivar el slippage [33]:
   i. La volatilidad de los valores involucrados en la operación. Cuanto mayor sea la fluctuación de precios, más probabilidades hay de deslizamiento.
   ii. La relación del monto a cambiar y el tamaño de la reserva. Para intercambios infinitesimales, el deslizamiento tiende a ser despreciable. No obstante, a medida que crezca la magnitud de la operación, el desplazamiento se amplificará, especialmente si la proporción con la liquidez que mantiene el fondo se eleva. Por ello, para *Swap Pools* más pequeñas, el *slippage* suele ser muy elevado.

a) Impermanent Loss. Este riesgo va asociado a dos oscilaciones: la fluctuación del precio cotizado para el token en el mercado vs la variación del precio del token en el *Swap Pool*. Se recuerda que cada *swap* que se ejecuta dentro de la *Liquidity Pool* altera el tipo de cambio sujeto a la curva de conservación. Es en el margen de estas dos variables donde sucede el arbitraje entre diferentes mercados o plataformas.

   Entonces, la "Pérdida Impermanente" se refiere al potencial perjuicio que pueden sufrir los LP cuando los valores que han depositado en el Fondo de Liquidez de un AMM se deprecian con respecto al precio de mercado. Dicho de otra manera: el LP hubiese obtenido mayor rentabilidad de sus valores si hubiese sostenido sus activos fuera del AMM [24].

   La pérdida es "Impermanente" ya que la continua variación del valor de los tokens depositados en el Swap Pool puede darse a la baja en ciertos momentos para a continuación crecer (y viceversa). Por ello, la pérdida (o beneficio) no se efectuará como tal hasta que los LP no hayan retirado los criptoactivos de la plataforma.

En la siguiente figura, bajo la condición de precios constantes en la reserva, observamos cómo se produce *Impermanent Loss* en cualquier dirección: tanto si el valor de mercado cae como si el valor crecer.

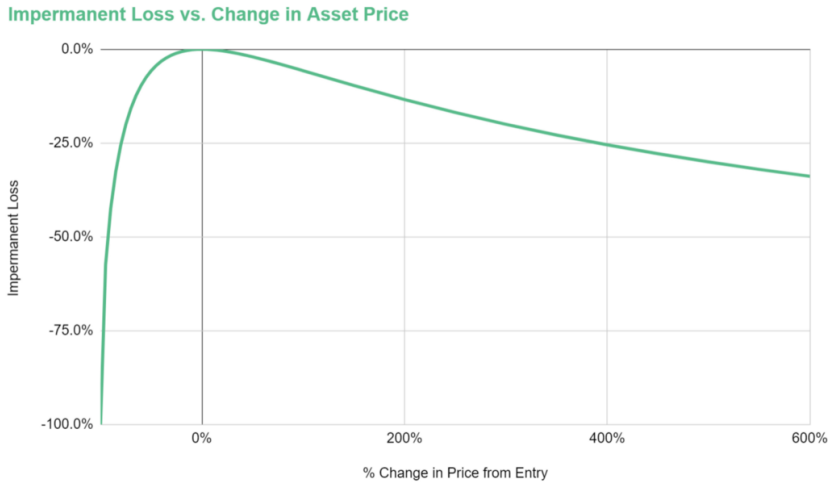


Figura 7: Impermanent Loss frente a la fluctuación de precio de mercado [34].

A pesar de que el paradigma de CFMM es el más común para los AMM, existen otras implementaciones de DEX con AMM como: *Constant Mean Market Makers* (CMMM), *Constant Sum Market Makers* (CSMM), *Hybrid Function Market Makers* (HFMM) o *Dynamic Automated Market Makers* (DAMM). Planteando un ejemplo: Curve Finance es otra de los AMM más populares y está diseñado con el modelo HFMM.

3.4 Uniswap

Uno de los *Decentralized Exchanges* más populares es *Uniswap*. Permite el intercambio de tokens ERC20 (red Ethereum) a través de diferentes *Swap Pools* y está implementado como *Automated Market Maker* con el modelo de *Constant Function Market Maker*.

La primera versión del protocolo surge en noviembre de 2018 y permite el intercambio de cualquier ERC20 token por ETH. El protocolo no margina absolutament eningún token (ERC20) dado a que, en caso de que no exista el *Swap Pool* concreto para ese par, puede invocarse a través del contrato Factory, que genera un nuevo *Swap Pool* (implementado a través de un Contrato Inteligente) para el par A ⇌ B solicitado. Esto facilitará también las subsecuentes transacciones que se quieran dar en Uniswap para el mismo par.

Uniswap V2 aparece dos años después, en mayo de 2020. En esta implementación, es posible intercambiar cualquier par de tokens ERC20. Aun así, los pares más cotizados incluyen WETH (*Wrapped Ether*, equivalente al ETH). Además, esta versión también añade un oráculo que pueda servir a otros *Smart Contracts*. La versión 3 de Uniswap se inauguró en mayo de 2021 y actualmente es el protocolo más utilizado para este servicio [35]. Más adelante, se explica con mayor extensión las mejoras que presenta.

A continuación, vamos a hablar de algunas particularidades de *Uniswap*. Elegimos la versión 2 para comenzar el estudio dado a que es especialmente representativo para la materia. Aunque es menos reciente que la V3, este protocolo cuenta con mayor recorrido en los mercados financieros y estableció el paradigma pionero que abriría paso a los siguientes AMM.

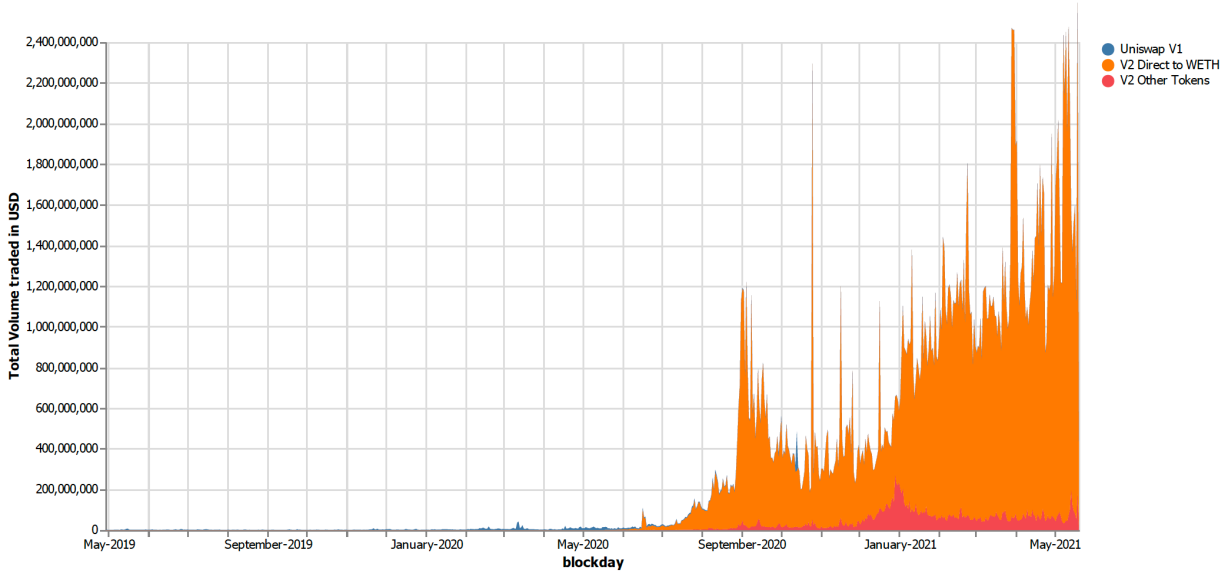


Figura 6: Volumen de operaciones en Uniswap hasta la aparición de V3 (mayo de 2021) [30].

Uniswap se define como un protocolo de liquidez automática. Opera en la red Ethereum y es un software *open source*, por lo que la implementación del sistema en está a nuestro total alcance. Animamos al lector a investigar la documentación de Uniswap V2 [36]. El esquema general del mecanismo se puede observar en la siguiente figura:

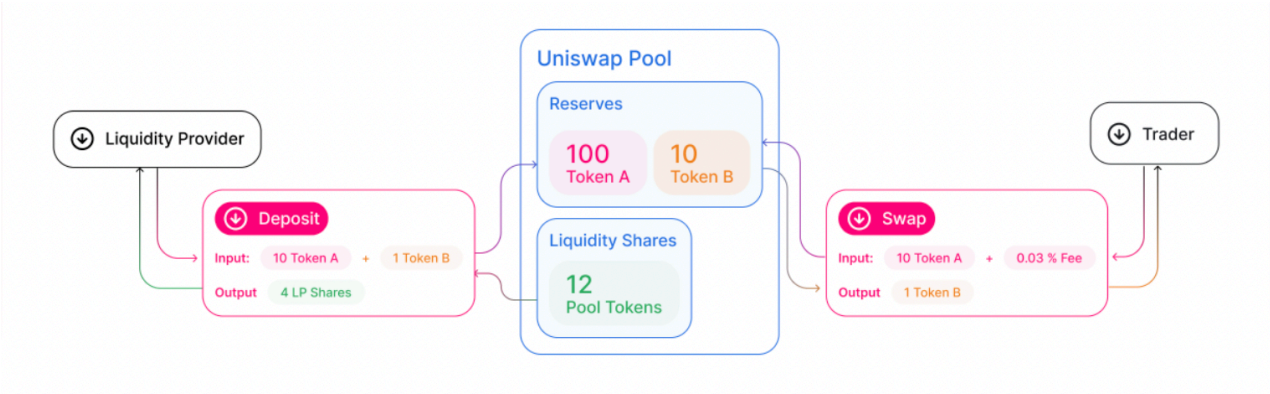


***Figura 8**: Funcionamiento de Uniswap V2 [31].*

Tal y como se expuso desde la presentación de los AMM, Uniswap cuenta con Proveedores de Liquidez (LP) a la par que con corredores u operadores que desean cambiar sus criptoactivos en el *Swap Pool* ofrecido por el sistema. La documentación de Uniswap V2 simplifica las transacciones realizadas por ambos agentes de la siguiente forma:

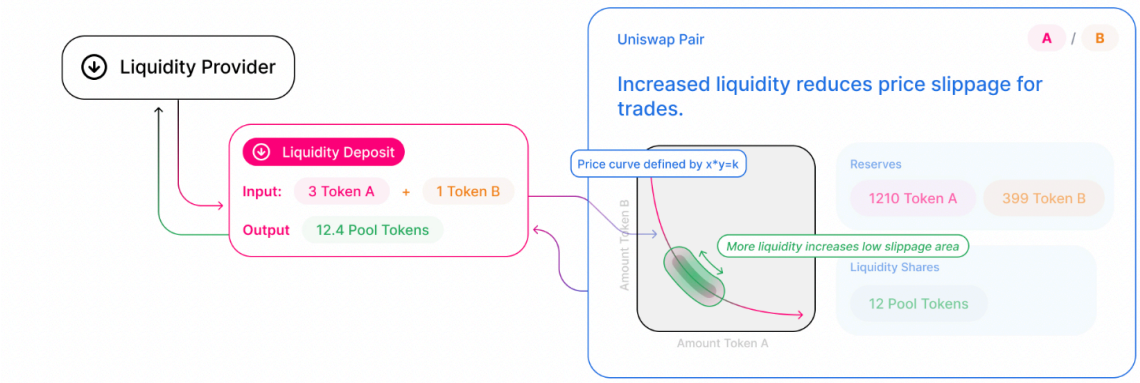


***Figura 9:** Depósito de Líquido por parte del LP en Uniswap [31].*

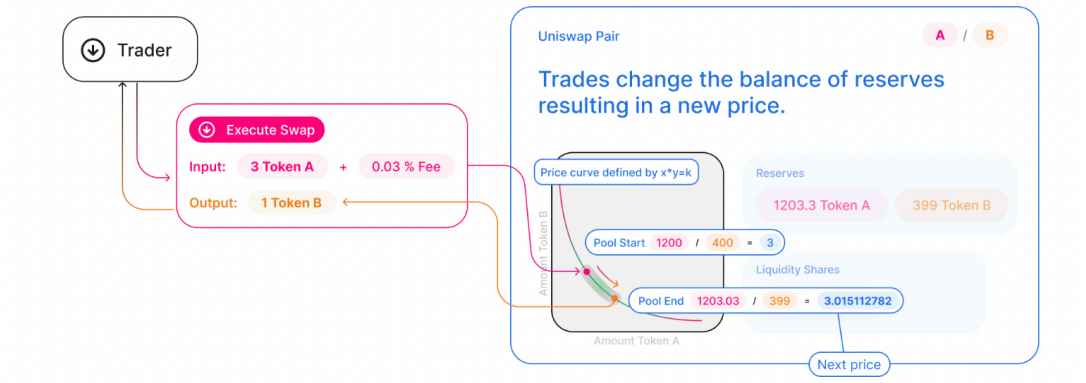


Figura 10: Swap por parte del corredor en Uniswap [31].

Ambas figuras muestran un comportamiento que ya se conoce desde el apartado anterior. Sin embargo, en este punto es oportuno abordar la implicación de las tasas aplicadas sobre los corredores y que en apartados anteriores se ha obviado.

En *Uniswap V2*, la tasa aplicada a los operadores que desean cambiar valores es del 0.3%. Esta tasa es repartida de manera proporcional al líquido aportado por cada LP a modo de intereses.

Recordamos que la inversión ingresada va destinado a un fondo compartido por todos los proveedores de liquidez (que será uno de los *Pools* sostenidos por la plataforma). Pero ¿dónde queda almacenadas las comisiones aplicadas sobre los operadores que ejecutan *swaps* hasta que se transfiera a los LP? Precisamente el Swap Pool actúa también como repositorio para estos pagos, por lo que, a medida que se ingresen estas cantidades, *k* se verá incrementada.

Ecosistema Uniswap

El recorrido que estamos haciendo sigue la mecánica de los AMM implementados como CFMM. Sin embargo, en este punto es interesante mencionar que el protocolo de Uniswap V2 cuenta con funcionalidades más extensas que el cambio de criptoactivos. Observemos el siguiente esquema:

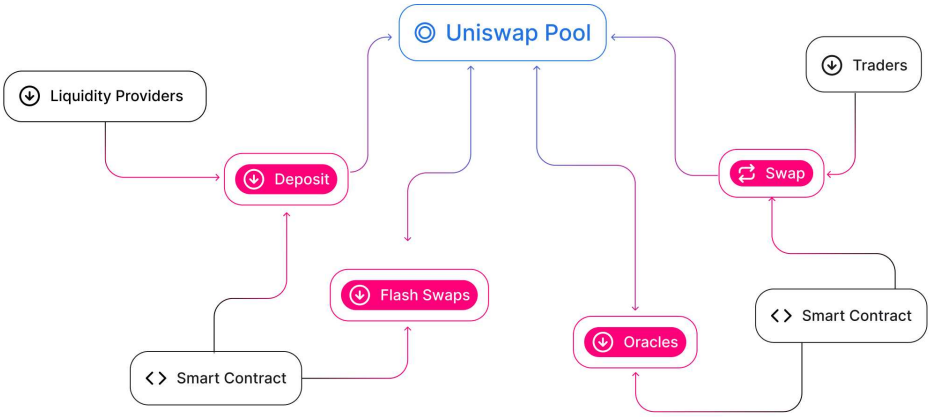


Figura 11: *Ecosistema Uniswap [31].*

Ya se conocen las operaciones de depósito y *swapping* que pueden ejecutar los Proveedores de Liquidez y los corredores respectivamente. Introducimos dos nuevas utilidades de Uniswap V2 [31]: *Flash Swaps* y *Oráculos*.

Las dos prestaciones ya expuestas son servicios perfectamente accesibles y funcionales para el usuario final. Sin embargo, solo se puede sacar partido de estas dos nuevas funcionalidades a través de Contratos Inteligentes. Es decir, los *Flash Swaps* y *Oráculos* se proponen como facilidades para los agentes que desean integrar estas soluciones en sus propias aplicaciones software construidas a través de Contratos Inteligentes. Las desarrollamos a continuación:

Por si los Swaps no eran suficientes: Flash Swaps

El término "Flash" probablemente nos suene de algo; en el apartado *Préstamos millonarios a todo riesgo: Flash Loans* se la sección 1.3, se ha hablado de los "Flash Loans" como un atractivo instrumento financiero viable únicamente en las DeFi que, a través de su ejecución atómica, permite percibir un préstamo sin ningún aval.

Los *Flash Swaps* se valen de la misma metodología: se sirve cambio de un token B a partir de una aportación de tokens A que el agente no llega a depositar explícitamente o con anterioridad (porque ni siquiera tiene en su posesión), sino que se aporta un "enlace" a la fuente de la que parte dicho líquido. El contrato que gestiona el Flash Swap liberará los fondos de B solo en caso de que encuentre líquido de A como contrapartida del cambio.

Para una mayor comprensión, mencionamos que dicho "enlace" se pasa como argumento a la misma función que ejecuta los *swaps*. Este enlace es una referencia o puntero a un *callback function*. Evitando entrar en tecnicismos, aclaramos que esta función lanza un proceso que se encarga de depositar el líquido requerido para el *swap* y que se acopla en el mismo proceso del flash swap de manera atómica [37] [38].

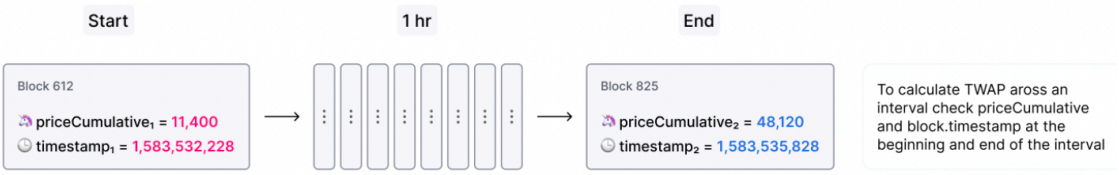
Haciendo de Uniswap un Oráculo de Precios

Uniswap vio el mercado que había establecido como una oportunidad para crear un Oráculo de Precios. Ya mencionábamos antes cómo los oráculos son fuentes de información de las que se valen los sistemas del entorno Blockchain para operar conforme a referencias del contexto externo a la plataforma. Como cabe esperarse, un oráculo de precio ofrece información acerca de la cotización de ciertos valores.

Hablemos del "Oracle Attack" [30] [31]. En esencia, este ataque consiste en distorsionar los precios o tipos de cambio del mercado de un *DEX* concreto a través de una operación de intercambio de gran magnitud. Ya se conoce cómo en los CFMM se altera el tipo de cambio con nuevas transacciones de los corredores. Esta distorsión momentánea del valor de un criptoactivo permitirá al atacante aprovecharse de un margen de beneficio con el que puede, por ejemplo, *sobrecolateralizar* un préstamo alterando al alza el valor del token que sirve de aval.

Este ataque se lleva a cabo mediante el desarrollo de un contrato inteligente que permita ejecutar todo el procedimiento de manera atómica. Además, es importante tener en cuenta que el ataque solo será efectivo si la plataforma en la que se desea manipular el precio se nutre de un oráculo que sólo contempla el precio de un mercado (como Uniswap).

Ante esto, la versión 2 de Uniswap presenta un mecanismo que ofrece resistencia a la manipulación de precio. El procedimiento consiste en incluir al final de cada bloque y al principio del siguiente una variable de precio acumulativa ponderada sobre el tiempo que ha existido dicho precio, llamada TWAP (*Time-Weighted Average Price*). En las siguientes figuras se esquematiza este mecanismo:



$$\text{TWAP} = \frac{priceCumulative_2 - priceCumulative_1}{timestamp_2 - timestamp_1} = \frac{48{,}120 - 11{,}400}{1{,}583{,}535{,}828 - 1{,}583{,}532{,}228} = 10.2$$

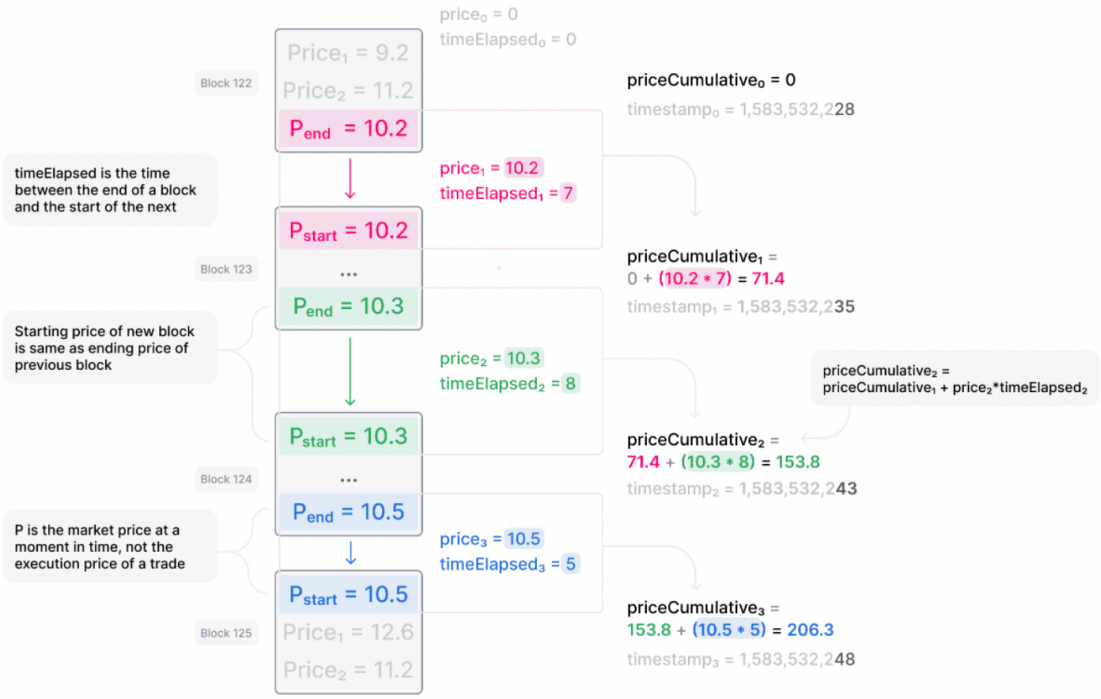


Figura 12: *Construyendo un Oráculo de Precios fiable en Uniswap V2 [31].*

Aportaciones de Uniswap V3

Después del éxito de *Uniswap* V2, se despliega el nuevo protocolo *Uniswap* V3 en mayo de 2021, el cuál presenta importantes cambios que buscan seguir posicionando a la plataforma como uno de los *Exchanges* predilectos.

Liquidez concentrada

El cambio más sustancial de esta nueva versión es la denominada "Liquidez Concentrada" (o *Concentrated Liquidity*). En este caso, la provisión de capital no se distribuye uniformemente en toda la curva [0, ∞) del Swap Pool, sino que el Proveedor de Liquidez toma una posición con un rango específico [P0, P1], concentrando su liquidez. El rango al que se adhiere su posición se formaliza en función de *ticks*, que representan una variación del 0.01% puntos básicos.

Con esta implementación, la aportación de liquidez en UniswapV3 no exige un ingreso equitativo de tokens A y B que componen el par A ⇌ B como se hacía en los protocolos de las versiones previas. Recordamos que este mecanismo servía para mantener los tipos de cambio constantes. Ahora, la provisión de liquidez de A y B dependerá de la posición [P_0, P_1] tomada, que requerirá un ratio específico A/B.

Con esta mejora se busca maximizar la eficiencia del capital de dos maneras:

- Optimización de la distribución de liquidez que soporta la estabilización del tipo de cambio. La concentración de las inyecciones de liquidez en el fondo aporta mayor solidez a la curva, ya que la fluctuación de la relación que existe entre las magnitudes cambiadas y la reserva del fondo es despreciable. A pesar de que la volatilidad de precios de los valores puede seguir afectando al desplazamiento, esta mejora reduce sustancialmente el *slippage* al que se exponen los corredores que intercambian criptoactivos en la plataforma [39].
- Maximización de la rentabilidad para los proveedores de liquidez. En las versiones anteriores de Uniswap, las cuotas que recibían los proveedores de liquidez se reparten equitativamente en función del uso que se hacía de su capital. Es decir, los LP que ofrecieran mayor liquidez para todo [0, ∞), obtendrían potencialmente mayores beneficios. Dado a que la liquidez deja de estar distribuida equitativamente en la curva, suceden dos cambios primordiales [31] [40].
    a) Las potenciales cuotas que puede ganar un proveedor de liquidez dependen del nicho al que aporte liquidez. Los LP siguen recibiendo cuotas en función del uso que se haga de su inversión, pero bajo este nuevo contexto, solo se explotará el capital inyectado por un LP en caso de que el tipo de cambio se encuentre dentro de la posición de dicho LP. El capital explotado en un momento puede pertenecer a diferentes LP, por lo que las cuotas se repartirán respectivamente entre ellos (en proporción al capital ingresado). En otras palabras:
    i. Un LP puede no recibir ningunas cuotas si el precio actual no se ubica dentro del rango definido por su posición.
    ii. La cuota que recibe un LP puede verse multiplicada ya que, en medida que su aportación deja de estar extendida en toda la curva para concentrarse en un rango específico, se puede sacar mucha mayor utilidad del capital provisto y, por lo tanto, puede también recibir muchos más intereses.
    b) La "pérdida impermanente" se reduce sustancialmente dado a que se acota el rango de precios (o tipo de cambio) al que el LP está dispuesto a operar. En otras palabras: el LP establece un precio mínimo y máximo entre el cual se podrá explotar la liquidez que ha ofrecido, por lo que, aunque se sigue exponiendo al *impermanent loss*, el riesgo se ve amortiguado por los límites del intervalo [41].

Para terminar, es interesante mencionar la mayor complejidad a la que se atiene la geometría de la nueva curva que propone Uniswap V3 (en cada *Pool*). Aunque la función $x \cdot y = k$ que define a los CFMM sigue siendo la misma, se da una ampliación de la curva a través de una *virtualización* de la invariante *k*. Esto se debe a que, como ya se ha mencionado en apartados previos, k refleja la liquidez con la que cuenta el fondo y, en Uniswap V3, esta liquidez concentrada varía a lo largo de la curva. En la siguiente figura, se muestra una virtualización de k, desarrollado matemáticamente en el trabajo de Vijay Mohan [23]:

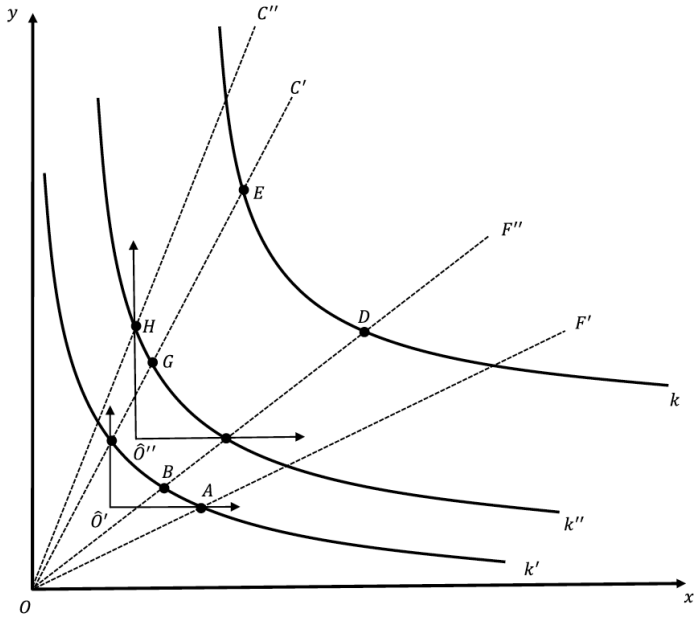


Figura 13: Virtualización de k en Uniswap V3 [23].

Introducción del token UNI

La versión 3 del protocolo de Uniswap propone el lanzamiento del token UNI. Motivado por el buen posicionamiento que ha logrado la plataforma en los últimos años, Uniswap considera que es el momento de introducir el token propio UNI, de tipo ERC20 (red Ethereum).

Este criptoactivo contribuye a un crecimiento sostenido del protocolo apoyado en su comunidad, a la que cede una propiedad compartida del sistema y en la que delega una nueva forma de gobierno. Fomentado desde los propios principios de las redes Blockchain, el token UNI facilita el acceso a la propiedad del sistema a la vez que promueve la distribución, descentralización y una infraestructura autosuficiente.

Originariamente se han emitido mil millones de tokens UNI en la génesis del protocolo y se distribuirán de la siguiente forma:

- 60% a los miembros de Uniswap, es decir, los agentes involucrados en las operaciones de la plataforma.
- 21.266% al equipo de desarrollo y futuros empleados de Uniswap.
- 18.044% a inversores particulares.
- 0.69% a asesores del sistema.

En los tres últimos casos, la adquisición del token se realizará de manera progresiva en un periodo de 4 años. Al inicio de su lanzamiento, se liberó un 15% de la emisión total, con 150.000.000 UNI tokens destinados a la comunidad. En la siguiente gráfica se puede observar el plan propuesto por Uniswap [42]:

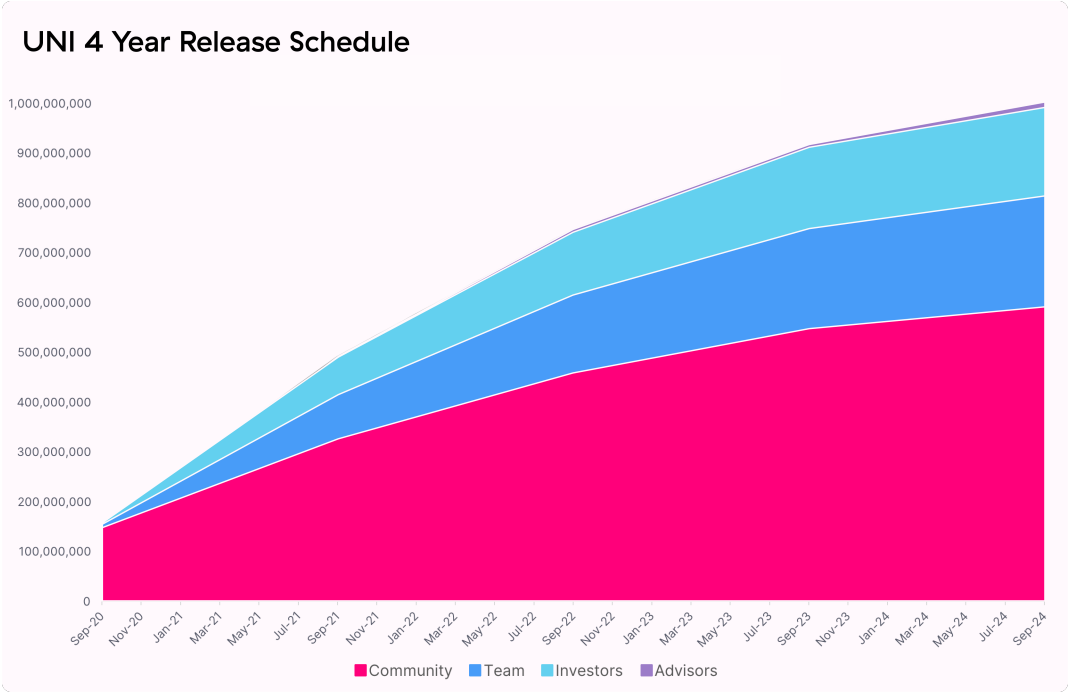


Figura 14: *Plan de 4 años de liberación de UNI* [42].

En los primeros minutos de la apertura de la Oferta Inicial Pública, que se presentó en *Coinbase* en marzo de 2021, el valor del token UNI se disparó en un 8%. De hecho, este token ya se considera dentro del entorno *DeFi* como un *BlueChip* de la industria [43].

Otras mejoras

Se hace un breve recorrido por otras de las mejoras implementadas en Uniswap V3 [44] [45]:

- **Comisiones flexibles**. Frente a las comisiones fijas de 0.3% en todos los pools, V3 introduce un rango mayor de comisiones con la que los LP podrán inicializar los Swap Pools; 0.05%, 0.3% y 1%. El criterio de elección irá motivado por la volatilidad del tipo de precios de ese par específico y servirá como política de incentivo tanto a LP como a *swappers*. Es decir, los pares más seguros tenderán a tener las menores comisiones para los operadores que deseen cambiar, por lo que reportarán menores beneficios a los LP. Por el contrario, los pares que sostienen más riesgo se sujetarán a mayores tipos de interés, para apremiar a los LP que ponen a disposición su capital.
- **Eficiencia del código**. La actualización del protocolo ha implicado también una reimplementación de los contratos inteligentes en los que se sostiene el sistema. Para ello se han tenido en cuenta las ineficiencias del código de la versión anterior y, como resultado, los costes de gas en la red Ethereum al operar con Uniswap V3 son más reducidos.

- **Mejora del Oráculo de Precios.** El cálculo del TWAP, introducido en la versión v2 de Uniswap y presentado en apartados anteriores, ya servía como Oráculo de Precios fiable para otros sistemas que se quisieran valer de esta referencia. No obstante, Uniswap V3 enriquece el TWAP con datos históricos de hasta nueve días anteriores. Esto, además de resultar más informativo, ofrece mayor flexibilidad, adaptándose a las necesidades del agente que consulta el Oráculo. A pesar de esta mejora, se ha optimizado la implementación de código para reducir los costes de gas del oráculo en hasta un 50%.
- **Licencia sobre el protocolo**. El éxito de las versiones anteriores derivó el lanzamiento de una amplia variedad de aplicaciones paralelas, que se basaron el código fuente de Uniswap V2. Sushiswap, por ejemplo, hijo directo de Uniswap V2, acabó transvasando más de mil millones de dólares en activos bloqueados en el protocolo primogénito. Por ello, la implementación del protocolo de la versión 3 se ha protegido a través de "Business Source License 1.1" [46] para evitar su explotación comercial por parte de otras entidades *DeFi* por un periodo de dos años.

3.5 Otros protocolos de Swaps

Se ha querido presentar a Uniswap como el AMM paradigmático para Swaps dado a que fue realmente precursora en su ámbito. No obstante, se quiere dedicar una breve sección a otras plataformas del mismo entorno.

Aunque, en un principio, ofrecen el mismo servicio, estos AMM se diferencian de Uniswap en algunos aspectos que los convierten en protocolos atractivos a operadores que tienen necesidades más específicas. Es por ello que, a pesar de que plataformas como *SushiSwap, Curve o 1inch* quedan atrás en términos de capitalización, resultan competidoras directas de Uniswap y potenciales *DEX* estrella.

I. Sushiswap

SushiSwap es un *fork* del protocolo Uniswap V2. Para reducir el alcance de esta explicación: en esencia, *SushiSwap* es un protocolo que ha clonado a UniswapV2. La motivación detrás de su nacimiento no es precisamente tomar la misma dirección, sino que se propone como "bifurcación" a la estrategia planteada por Uniswap.

La diferencia primordial que el protocolo de SushiSwap ofrecía en un principio, fue la emisión del token de gobernanza SUSHI, que era emitido para su distribución a los participantes del sistema. Ante el rápido éxito de esta estrategia, Uniswap lanzaría el token UNI en su versión V3 del protocolo (comentado previamente).

Este token reportaría unos beneficios del 0.05% de las tasas aplicadas a los corredores que comercian en el mercado creado por *SushiSwap*. Este 0.05% se desglosa del total de 0.3% de comisión aplicado sobre los operadores. Entonces, el 0.25% restante iría destinado a los proveedores de liquidez [47].

Por otro lado, *SushiSwap* da juego al *yield farming* ya que continúa con su política de incentivos sobre los agentes que operan en ciertos Liquidity Pools, en los que se ofrecen recompensas de hasta un 80%. Por otro lado, la interfaz de usuario de *SushiSwap* ofrece prestaciones muy diferentes en forma de "menús" con respecto al clásico servicio de cambio de tokens presentado en *Uniswap*.

Por último, se habla de que *Uniswap* ha tomado un camino de innovación más reservado e independiente que le ha llevado a prescindir de su transparencia original y la implicación de la comunidad. Esto lo ha alejado de los valores fundamentales de descentralización, mientras que *SushiSwap* sigue apostando por una participación más activa de la comunidad y potenciar la interoperabilidad de la plataforma con otros protocolos [48].

II. Curve

Curve es otro protocolo muy similar a *Uniswap*. El aporte diferencial que presenta frente a este otro es su orientación de mercado hacia stablecoins. Aunque estos

criptoactivos están presentes para el comercio en las plataformas previas, Curve destina su sistema exclusivamente para el intercambio de stablecoins.

En este sentido, se puede visualizar a *Curve* como un mercado *Forex* dentro de los mercados descentralizados, ya que, como se ha explicado en secciones anteriores, los *stablecoins* funcionan como valores mucho más estables y seguros que las criptomonedas debido a su vinculación a una moneda fiat (en los casos más populares).

Curve se posicionó como una de los AMM populares dado a que prácticamente no contaba con competidores en el momento de sus inicios, y con su notable expansión ha abierto un nicho de mercado para otras plataformas que dirigen sus servicios al intercambio de *stablecoins*.

La estabilidad de los valores que se operan en Curve hace que la compraventa en esta plataforma se vuelva especialmente atractiva:

- Se minimiza el deslizamiento al trabajar en pools que mantienen una proporción de valor 1:1 muy constante.
- De la misma manera, el *impermanent loss* es prácticamente despreciable.

Para terminar con el repaso de Curve, cabe mencionar que Curve también emite un token propio CRV y ofrece tasas sobre las operaciones de cambio de stablecoins mucho mejores que las de Uniswap V2: 0.04% en Curve frente a un 0.3% en Uniswap [49] [50].

III. 1inch

1inch es un DEX agregador. El protocolo implementado por esta entidad no se enfoca en construir infraestructura propia para soportar las operaciones de cambio o provisión de liquidez, sino que pone el énfasis en la comparación de las diferentes alternativas de swaps disponibles en el entorno, ofrecidas por otras plataformas.

De esta manera, la plataforma *1inch* sirve como medio para navegar por los *pools* del mercado DeFi y encontrar las ofertas más rentables. Esto es posible a través de lo que *1inch* llama "pathfinder" o explorador. Para maximizar el beneficio, la operación puede llegar a partirse para comerciar cada monto en diferentes protocolos [51].

A primera vista, el servicio ofrecido por *1inch* parece ser la forma definitiva de rentabilizar los cambios de divisas. Sin embargo, el trabajo realizado por el sistema para realizar esa búsqueda algorítmica a través de las redes Blockchain requiere de una importante inversión de gas. Por esta razón, las comisiones aplicadas por *1inch* suelen ser sustancialmente mayores que las de otras plataformas [52].

1inch puede resultar especialmente atractivo para operaciones con grandes magnitudes. Dividir la operación para su comercio en diferentes protocolos disminuye el deslizamiento, resultando en tipos de cambios más rentables, a pesar de la comisión pagada a *1inch*. Para pequeñas operaciones de cambio, este servicio no resulta tan

atractivo, aunque la última versión lanzada por *1inch* se propone como sustancialmente más optimizada que la anterior a efectos de coste de gas [53] [54].

Añadimos una última información de interés: 1inch también mantiene Liquidity Pools en los que los agentes se pueden involucrar como LP. Además, 1inch también tiene su propio token de gobernanza y "utilidad" [55].

3.6 Red de Oráculos: Chainlink

Chainlink se define a sí misma como una *Decentralized Oracle Network* (DON) o Red de Oráculos Descentralizada. Este sistema pretende mejorar y potenciar las capacidades de los smart contracts para servir como Oráculo o fuente de información normalmente inaccesible de manera nativa a las redes Blockchain.

Este *middleware* es "agnóstico al Blockchain" o, utilizando otras palabras, solo se vale de información externa al Blockchain por lo que, a su vez, se integra como complemento flexible en todas las redes Blockchain. A través de los denominados adaptadores, *Chainlink* puede facilitar un flujo de datos entre las fuentes de datos externos al ecosistema y las redes Blockchain. Es un vehículo de transvase de información desde los paradigmáticos servidores de la Web 2.0 hacia las cadenas de bloques.

En definitiva, esta aplicación aporta un enorme valor al entorno Blockchain. Permite la creación de múltiples aplicaciones descentralizadas que se alimentan de los datos *off-chain* sin la necesidad de que estas aplicaciones generen redes Blockchain propias para integrar estas fuentes de información.

Uno de los mayores retos existentes en los mercados descentralizados (y mundo Blockchain en general) es utilizar fuentes de información fiables. De hecho, las ya existentes implementaciones de Oráculos ofrecían el potencial riesgo de reportar información corrupta, especialmente si sus fuentes de datos provienen de fuentes centralizadas [56].

Chainlink funciona como un Oráculo de datos *off-chain* fiable, seguro y descentralizado:

- El diseño de su arquitectura se fundamenta en una red de nodos que imita el comportamiento descentralizado de Blockchain.
- Las fuentes de información originales en las que se basa Chainlink son APIs premium y autenticadas. A su vez, Chainlink trabaja con proveedores de datos que funcionan como agregadores que contrastan la información.
- Importante implementación de seguridad asentada en protocolos e infraestructura.
- Datos transparentes en el Blockchain, lo que permite la auditoría pública.

La siguiente figura sintetiza el funcionamiento del sistema implementado por *Chainlink*:

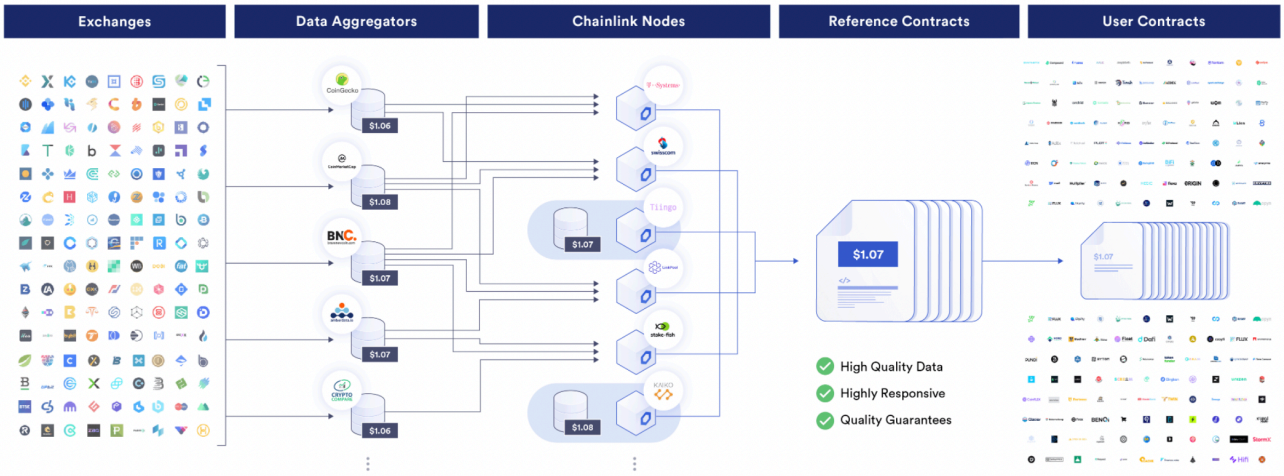


Figura 15: *Agregación en Sistema Chainlink [57].*

Por último, cabe mencionar que Chainlink también mantiene su propio token, LINK. Sin embargo, a diferencia de los tokens de gobernanzas que suelen emitir la mayoría de protocolos de AMM, LINK funciona como medio de pago de las tasas impuestas sobre los servicios de *Chainlink*. Por ello, este token va más orientado a usuarios del servicio más que a inversores de criptoactivos generalistas [58] [59].

4 Caso de Estudio: Oráculo de Precios sobre Swaps en Automated Market Makers

Como ya se ha adelantado desde el principio del proyecto, este Trabajo Fin de Grado en Administración y Dirección de empresas se ha desarrollado concurrentemente al Trabajo Fin de Grado de Ingeniería Informática. Desde ambos se ha realizado un proceso de investigación con un foco diferente dentro del área de Blockchain, pero finalmente se deseaba confluir en un punto común en el que poder relacionar ambas ramas.

Ya se sabe cómo las Finanzas Descentralizadas componen uno de los sectores de mayor expansión que nacen de la tecnología Blockchain y, se ha visto cómo los *Automated Market Makers* facilitan una el flujo de Comercio de Alta Frecuencia con operaciones tan elementales como los *swaps*. También se conoce lo que es un Oráculo, llegando a tocar el concepto de Red de Oráculos, implementado por *Chainlink*.

Una vez se ha direccionando el avance y profundidad del análisis hacia los componentes más importantes del ecosistema, se puede dar un paso más. El epítome del proyecto la conformará la aplicación financiera presentada desde esta sección.

Así, se descubrirán algunos de los conflictos a los que se puede enfrentar un operador de *swaps* en los mercados descentralizados, se planteará la mecánica y capacidades de una solución financiera basada en contratos inteligentes y, terminantemente, se logrará converger todo el análisis realizado en esta aplicación. Un añadido más que se desea presentar en este proyecto es, tratar el atractivo potencial que puede tener un sistema como el propuesto para ejecutar estrategias de arbitraje en los mercados descentralizados.

4.1 ¿Qué sucede con los precios en los AMM?

Ya se conocen los factores que más influyen, no solo en los AMM, sino en el tipo de cambio obtenido en los swaps que ofertan: la volatilidad de los valores que se negocian, la liquidez provista por los LP o las operaciones que realizan los otros agentes sobre el mismo *pool* son algunos de los condicionantes que se han expuesto. Como es natural, la variabilidad de todos estos elementos acaban por generar, en suma, una oscilación del tipo de cambio más que importante.

Nos parece interesante comenzar presentando el caso de volatilidad de dos *stablecoins*: DAI y USDC. Ambas equivalen a un dólar estadounidense, pero son implementados por protocolos diferentes, el primero ya nos puede resultar familiar de MakerDAO [27] (se ha hablado de él en el apartado "El inicio del Yield Farming" en el

punto 0), mientras que el segundo fue creado por CoinBase [60]. A pesar de que, en teoría van vinculadas al precio del dólar, se puede observar en las siguientes figuras el comportamiento del tipo DAI/USD y USDC/USD:

Figura 12: *Variación del tipo de cambio DAI/USD en Uniswap V3* [61].

Figura 13: *Variación del tipo de cambio USDC/USD en Uniswap V3* [62].

Observamos cómo, aunque sea en términos centesimales, existe una notable oscilación de los tipos de cambios de DAI y USDC con respecto al USD. Pese a lo que se podía esperar, el swap entre dos stablecoins como DAI y USDC es más estable que el propio cambio DAI/USD o DAI/USDC. Esto sucede simplemente porque ambos *stablecoins* van vinculados a la fluctuación de la misma referencia: el dólar estadounidense. Por ello, la mecánica algorítmica implementada para aproximarse a la

oscilación del dólar desde cada uno de los criptoactivos parte de la misma base. En definitiva, la misma referencia de ambos valores amortigua la oscilación entre ellos, como se puede observar en la siguiente figura:

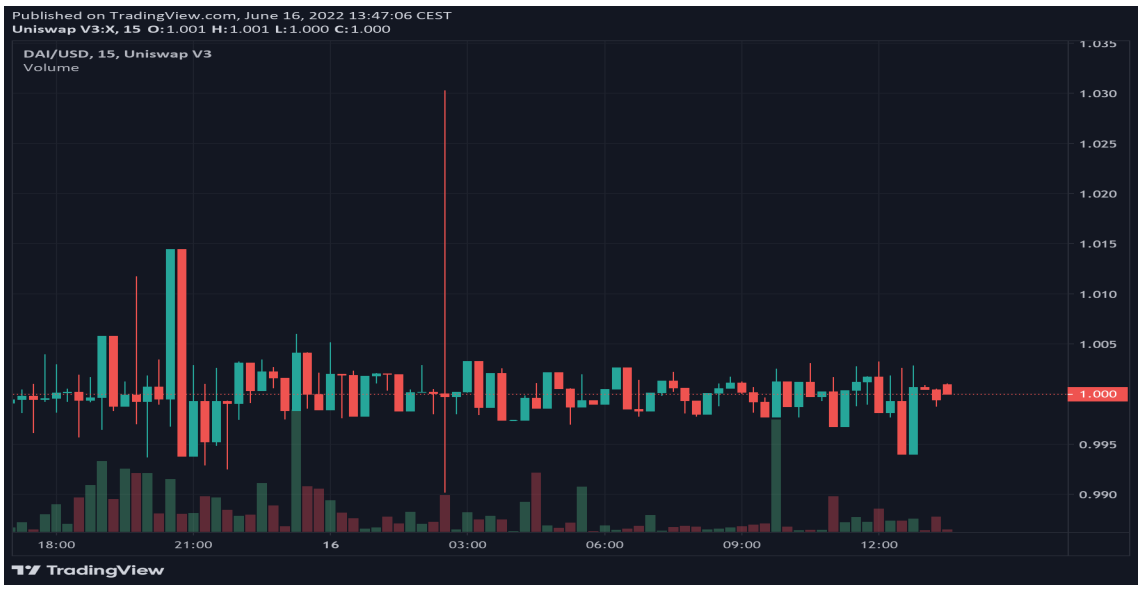


Figura 16: Variación del tipo de cambio DAI/USD de Uniswap V3 [63].

El par anterior corresponde al pool DAI/USDC de Uniswap V3, con una tasa del 0.01%. Recordamos que en el protocolo V3 de Uniswap existe la posibilidad de crear *pools* con una tasa flexible. Este *swap* concreto es el más comerciado en toda la plataforma de *Ethereum* en el momento de la redacción de este proyecto [63].

Para este mismo par existe otro pool con tasas del 0.05%, que cuenta con un volumen de comercio mucho menor. Además, la liquidez provista para este fondo también es bastante inferior. Se puede comparar las magnitudes de estos parámetros en la propia plataforma *GeckoTerminal* [63] o la propia plataforma de Uniswap [64].

Con esto , se demuestra que, incluso unos tokens tan seguros como los *stablecoins* presentan una volatilidad apreciable y, aunque en cambios de pequeñas magnitudes puede considerarse casi despreciable, un cambio de 100.000 DAI a USDC con un tipo de 0.999, ya implica una diferencia de 100 de USDC (sin considerar las comisiones de la operación de *swap*) para unos valores que, en principio, están vinculados.

Si estudiamos la evolución del tipo de cambio de criptoactivos más volátiles, encontramos un comportamiento totalmente diferente. En la siguiente figura se observa la progresión de otro de los pares más cotizados en swap en Uniswap V3, WBTC/ETH:

Figura 17: Variación del tipo de cambio WBTC/ETH de Uniswap V3 [65].

El día en el cual se muestra esa evolución del histórico de precios para los swaps WBTC/ETH, el valor de ETH ronda los 1800$. Entonces, en menos de 24 horas, el tipo de cambio ha oscilado en un rango de hasta 0.2 ETH, o lo que es lo mismo, 360$ (en los precios del momento de redacción).

Veamos otro caso: ETH/USDT; una criptomoneda contra un *stablecoin*. ¿Qué podríamos esperar de la evolución del tipo de cambio de este *swap*? Sabiendo que USDT es un stablecoin vinculado al USD, la evolución de este índice no hace más que replicar el propio valor de ETH reflejado en términos del USD, moneda fiat.

Figura 18: Variación del tipo de cambio de ETH/USDT en Uniswap V3 [67].

4.2 Propuesta de un Oráculo de Precios

El sistema que planteamos es, fundamentalmente, un Oráculo de Precios que, tal y como su propio nombre indica, ofrecerá datos sobre los precios que confieren los protocolos de Uniswap V2, Uniswap V3, Sushiswap, Curve, 1inch y Chainlink. El servicio de consulta de precios irá orientado en primera instancia a los tipos de cambio de las operaciones *swap* de pares A ⇌ B, que se refleja como A/B o la cantidad de critpoactivo A que se obtiene en función a una unidad de criptoactivo B. También es aplicable la operación inversa.

Además, en segunda instancia, también se ofrecerá información de precios de tokens individuales desde estas mismas fuentes. Esto dotará al sistema de mayor alcance, dado a que no es estrictamente necesaria la consulta del cambio de un par, sino que además es posible conocer información sobre precios de criptoactivos de manera más abierta o flexible, reflejados en términos de ETH. Es precisamente por ello que se incorporará *Chainlink* como fuente del sistema, porque, aunque no es un protocolo de AMM, puede aportar información muy actualizada, fiable y exacta sobre precios.

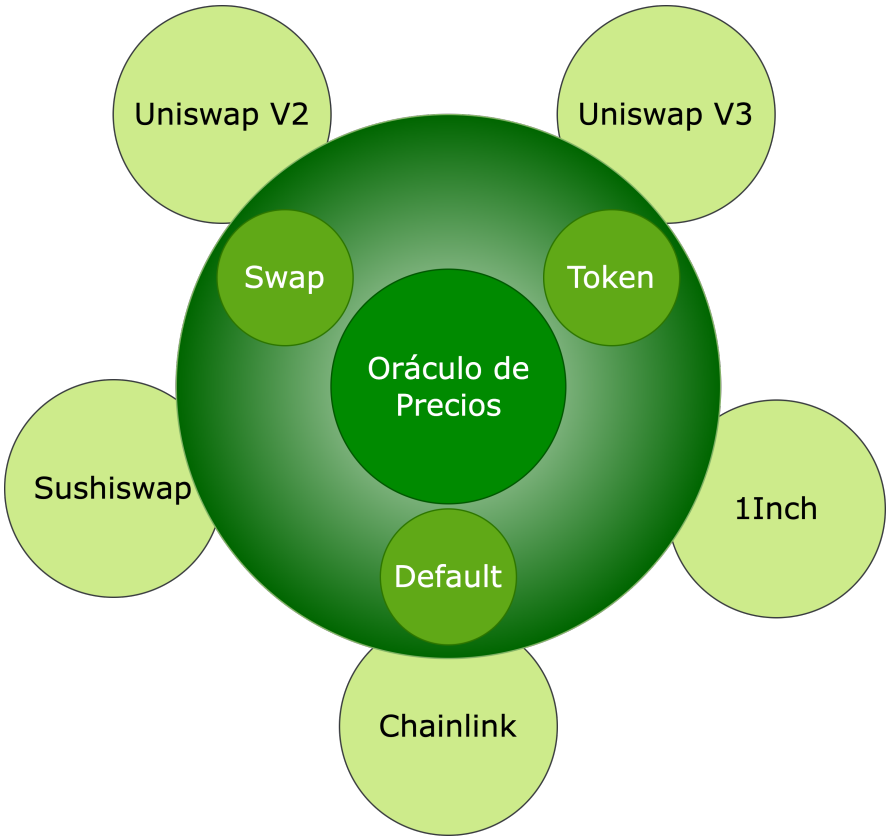


Figura 19: *Visión general del Oráculo de Precios*

La interacción con los estos protocolos solo es posible de la siguiente forma: haciendo uso de los mecanismos que dichos sistemas ponen al alcance de manera pública en su *open source.* Aunque las implementaciones de código abierto son bien conocidas en el sector tecnológico, esta puesta en común de la arquitectura de las plataformas nativas al Blockchain es un factor muy relevante a la hora de promover el desarrollo simbiótico del entorno, la interoperabilidad de los diferentes mercados o servicios así como establecer un marco más inclusivo para nuevos agentes creadores de mercado. Así, *Sushiswap* o *Chainlink* no solo se benefician de facilitar sus protocolos, sino que necesitan hacerlo para que herramientas como este Oráculo de Precios puedan sacar partido del servicio que ofrecen.

La aplicación se diseñará de tal manera que podamos predefinir los AMM o plataformas de preferencia para obtener el precio de cada par o token. Aun así, se tendrá en cuenta una consulta por defecto o *default* en el oráculo, de manera que, en caso de no plantear una solicitud específica al sistema, este siempre devuelva una información sobre precios que pueda resultar de interés.

Aunque se establecen esas 6 fuentes específicas con las que nutrir al Oráculo, la arquitectura del sistema es fácilmente escalable para agregar nuevos DEXes o plataformas. No obstante, esto requerirá una programación explícita de contratos inteligentes. En esta misma línea cabe mencionar que desde este sistema no se pretende prestar un servicio accesible a un perfil poco cualificado, sino que se orienta a usuarios más técnicos que:

a) Pueden sacar partido a la herramienta en base a conocimientos financieros en mercados descentralizados.
b) Son capaces de, no solo interaccionar, sino también escalar el Oráculo de Precios enriqueciéndolo con fuentes de nuevos protocolos.

De una forma y otra, el usuario debe estar habituado al despliegue de operaciones en *DeFi* mediante contratos inteligentes. Por ello, con esto expuesto, se clarifica que esta propuesta no consiste en un servicio comercial que monetizar, sino que se trata de una herramienta de la cuál beneficiarse como participante de los mercados descentralizados.

El sistema implementado se desplegará a través de un *Provider* o punto de acceso a la red. Proveedores como *Alchemy* o *Infura* permitirán ejecutar la aplicación de la misma forma que si se ejecutase en la red, pero de manera totalmente gratuita. Esto es posible ya que, sistemas como estos lanzan los contratos en nodos de su propia infraestructura, en los cuales replican la Blockchain. Esto supone que, a efectos prácticos, la ejecución funciona de la misma manera que si estuviese desplegado en la red, pero realmente, no está sucediendo de manera descentralizada, sino que se ejecuta en una red gestionada por una entidad centralizada. De esta forma, se delega el funcionamiento del contrato en una tercera parte centralizada.

A pesar de esta desventaja de reducir el aspecto descentralizado, desplegar la plataforma con esta intermediación aporta un valor muy significativo: la consulta de precios es totalmente gratuita. Es decir, desplegar un sistema como este en la red *Ethereum* y ejecutarlo para obtener información sobre precios puede generar un coste en *gas* desproporcionado. Así, un operador en mercados descentralizados que desea definir la siguiente estrategia que abordará debería incurrir en gastos simplemente por obtener información sobre precios. Mientras tanto, usar un Oráculo de Precios a través de un *Provider* termina por conferir exactamente la misma funcionalidad de consulta de datos en la red descentralizada de manera totalmente gratuita.

¿Por qué integrar estas funcionalidades en una herramienta que además no ofrece una interfaz gráfica de navegación? ¿No puedo consultar ya los precios de los tokens online de manera clara? Aquí es donde nuestra aplicación resulta aún más conveniente y, es que, aunque la información sobre los precios es totalmente accesible desde la Web 2.0, el servicio de internet convencional, se deben entender la naturaleza de estas fuentes:

1. Son plataformas centralizadas. Fuentes como *Binance* que son *Exchanges* o sistemas puramente centralizados (*CEXes)* en todos sus niveles. Por otro lado, hay interfaces webs donde se presentan informaciones de precios provistas por protocolos descentralizados como *Uniswap*, sin embargo, el soporte software y hardware de dichos medios son centralizados. Esta naturaleza centralizada de los datos puede inferir en detrimento de la fiabilidad o integridad.
2. No ofrecen datos totalmente actualizados. Las fuentes off-chain tienden a facilitar la información del Blockchain con cierta latencia. Esto se debe esencialmente a la arquitectura típica estos productos software, que deben obtener los datos de las redes Blockchain para conducirlos hacia capas superiores de abstracción de la estructura del protocolo. Las innumerables decisiones involucradas en el diseño de estas plataformas, como la frecuencia de consulta o la velocidad de comunicación entre los diferentes módulos del sistema, condicionan en gran medida la frescura de los datos que disponen.
3. No disponen de total exactitud. Por otra parte, las fuentes online más accesibles reproducen datos de precios orientativos. No se pretende sugerir que los datos que administran no son reales, sino más bien que la información que proporcionan se dirige a un público más amplio que no desea conocer la exactitud de los precios en un orden infinitesimal. Por ello, se realizan redondeos, aproximaciones, ponderaciones o promedios que pueden afectar la exactitud de la consulta de precios en el momento en el que nos interesa.

Resumiendo, operar en mercados descentralizados de manera eficiente implica ser partícipe de esa descentralización en todos sus sentidos, valiéndose de recursos e información originada directamente en la red Ethereum. A medida que abstraigamos un servicio con una infraestructura de software más gruesa, muchas de las fuentes de información sustentadas en Blockchain se degradan, mientras que, alimentando un

Oráculo de precios desde la raíz, a un bajo nivel, se pueden obtener datos fiables, exactos y frescos de primera mano,.

Por otro lado, ya se han expuesto implementaciones de Oráculos de Precios en las secciones 3.4 y 3.6 por parte de *Uniswap* y *Chainlink* respectivamente. Como ya se ha visto, los mecanismos del TWAP y red de Oráculos buscan una máxima aproximación a los precios; en el primero sobre los datos de los valores comerciados en *Uniswap*, mientras que el segundo conjuga diferentes fuentes de AMM. Además, sus diseños evitan que los datos que ofrecen sean susceptibles a ataques que corrompan la integridad de esta información con fines maliciosos. El Oráculo de Precios propuesto se podría beneficiar de dichos servicios, ofreciendo la ventaja adicional de constar de diferentes fuentes a modo de comparación o mayor acercamiento al precio real con el que se opera en el mercado.

Con la puesta en valor del Oráculo de Precios se conforma una fuente de datos *on-chain* para comerciar en mercados descentralizados de manera óptima. En la siguiente sección se entenderá mejor la utilidad de una información de esta naturaleza.

4.3 Con miras al futuro

Esta plataforma no se plantea tanto como un sistema cerrado que orienta en torno a los mejores tipos de cambio, sino que se propone con expectativas de integración para ofrecer un servicio más extenso que pueda sacar partido de estas fuentes de datos. Una de las opciones con mayor potencial es enfocar la implementación hacia el arbitraje.

En la sección X del punto 1 ya introducíamos el concepto de arbitraje como parte de las estrategias de *High Frequency Trading*. En el punto 3 también hicimos varias alusiones a esta mecánica dentro de los *Exchages*: cómo el arbitraje aprovecha el margen entre la fluctuación de diferentes mercados y, además, acaba por beneficiar la estabilidad de precios entre los mercados que ofrecen las diferentes plataformas.

Conociendo ya el papel que juega el arbitraje dentro de los mercados descentralizados, se puede intuir dónde entra en juego el papel del Oráculo de Precios: nuestro sistema permitirá encontrar las mejores ofertas de swaps disponibles en un momento muy preciso para, en base al resultado, poder ejecutar un swap que aproveche dicha ventaja.

Como es natural, cuanto mayor sea el capital invertido en el swap, mayor será el margen de beneficio. Por ello, se pueden incorporar otra de las potentes herramientas de las Finanzas Descentralizadas: *flash loans*. Junto a ellas, se maximiza el capital que destinado al arbitraje. Ya se conoce que la utilización de *flash loans* no necesita un colateral o aval del préstamo, por lo que contar con más o menos capital propio no supone un problema para poder llevar a cabo esta estrategia.

Por otro lado, se debe ser consciente que los servicios financieros ofrecidos por cada uno de los protocolos retienen tasas, y aunque ya se sabe que estas tasas son mínimas en comparación con las ofrecidas por las *CeFi*, sigue siendo necesaria contemplarlas en la estrategia para obtener algún tipo de rentabilidad. Es decir, operar con grandes magnitudes implica multiplicar la tasa impositiva que afrontamos, por lo que, como resultado, las comisiones de los servicios podrían minimizar, anular el beneficio o incluso reportar pérdidas para el agente si la operación no se diseña exhaustivamente.

El Oráculo de Precios se podría conjugar con otra aplicación que ejecute todo el proceso expuesto. Más bien, la funcionalidad del oráculo se debería acoplar en otro sistema que llevar a cabo toda la tarea de manera atómica:

1. Petición del *flash loan* de criptoactivo A.
2. Primer swap $A \rightarrow B$ en pool $A \rightleftharpoons B$ con el mejor cambio ofrecido por el oráculo. Deducción de comisiones del cambio ofrecido.
3. Segundo swap $B \rightarrow A$ en otro pool $A \rightleftharpoons B$ con el mejor cambio ofrecido por el oráculo. Deducción de comisiones del cambio ofrecido.
4. Devolución del principal del *flash loan* más las comisiones.

En la siguiente figura se puede observar el proceso de manera esquemática:

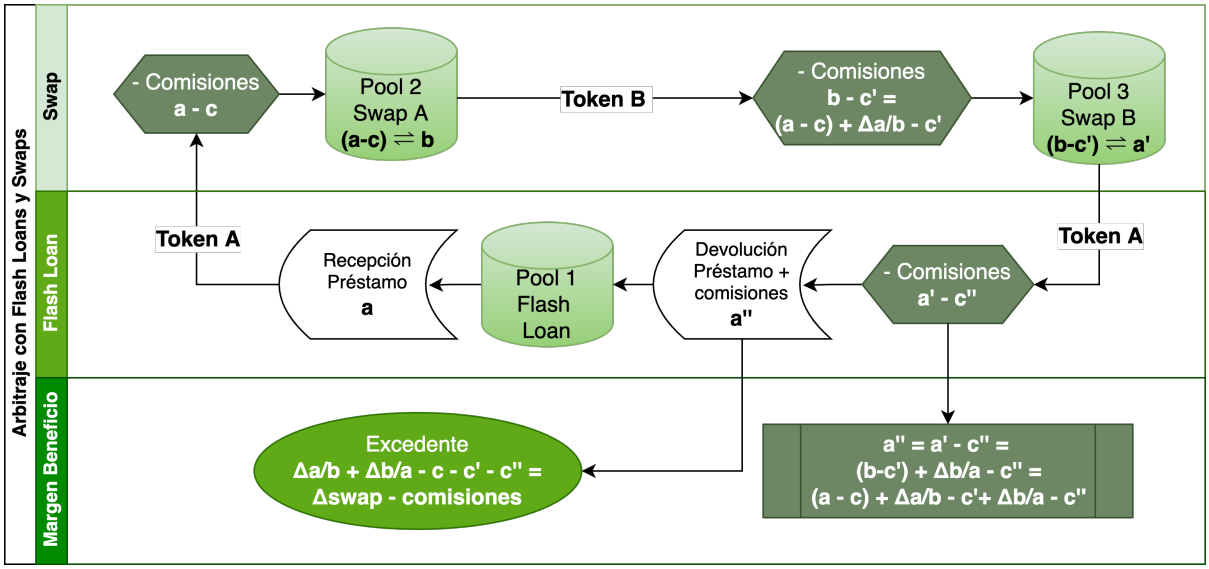


***Figura 20**: Arbitraje con Flash Loans y Swaps en DeFi.*

Vamos a ejemplificar esa estrategia con nombres y valores hipotéticos para lograr entender el proceso:

- AA*VE* ofrece un *flash loan* con un principal de ETH valorado en 1.000.000 $ y pide unos intereses del 0.08%.
- *Uniswap* V3 ofrece cambio DAI/USDT a 1.002, es decir, con un margen de beneficio de 0.2% DAI sobre USDT. Impone tasa del 0.08% sobre la operación.
- *Sushiswap* ofrece cambio USDT/DAI a 0.998, o lo que es lo mismo, un excedente de 0.2% DAI sobre USDT o, en otras palabras, USDT es 0.2% más barato que DAI. Comisiones de del 0.05%.

Con esta premisa, y asumiendo que la vinculación USD-USDT-DAI es constante, el proceso se desarrollaría de la siguiente manera:

1. Se cuenta con un capital de 1.000.000$ en DAI ofrecido por el flash loan de AAVE.
2. Se cambia en el pool DAI ⇌ USDT de *Uniswap* V3 los 1.000.000 $ en DAI por 1.000.000 · 1.002 = 1.002.000 USDT. Se deducen tasas de 0.08% sobre el ingreso de la operación, es decir, 1.002.000 – 1.000.000 · 0.08%= 1.001.200 DAI.
3. Se cambia en el pool DAI ⇌ USDT de *Sushiswap* 1.001.200 $ en USDT por 1.001.200/0.998 = 1.003.206,4 USDT. Se restan las comisiones 1.003.206,4 – 1.001.200 · 0.05% = 1.002.705,8
4. Se devuelve a AAVE el principal de 1.000.000 USDT más los intereses de 1.000.000· 0.08% = 800 $.

Se retienen 1.002.705,8 – 1.000.800 = 1.905,8 $ del proceso.

Con esta casuística de arbitraje expuesta se logra demostrar dos aspectos:

a) Una estrategia de arbitraje en los mercados descentralizados que se vale de las herramientas de las DeFi para maximizar la eficiencia del capital. Se multiplican los beneficios de una operación partiendo de una inversión inicial nula.
b) La utilidad que pueden ofrecer unos datos sobre precios fiables, exactos y actualizados como los dispuestos desde el Oráculo de Precios.

Se ha obtenido un beneficio de casi 2000 $ operando con un capital de un millón. No obstante, este caso ha utilizado datos agnósticos o hipotéticos. Así, la diferencia de precios entre dos mercados puede verse minimizada, reduciendo el potencial beneficio. De la misma manera, la brecha de precios entre diferentes plataformas de las que se aprovecha el arbitraje puede ampliarse, especialmente en momentos de inestabilidad y fluctuación en el entorno financiero.

Es claro que, con semejantes magnitudes, una diferencia en un orden de milésimas puede impactar significativamente el efecto de cada una de las operaciones compuestas en la estrategia y la resolución final de ésta. Por ello, el potencial beneficio que ofrece el arbitraje sólo será viable si el procedimiento se sustenta en una información fuente de calidad.

5 Consideraciones y Conclusión

Con el acercamiento al final de este trabajo, se va a sintetizar el recorrido realizando, reflexionando sobre lo que se ha aprendido y estimando su aportación en materia financiera.

Se insiste nuevamente que este trabajo no pretende constituir una apología de las Finanzas Descentralizadas, sino que se sitúa como un acercamiento a esta materia. Esto implica que se debe ofrecer una visión conjunta de los factores involucrados y, habiéndola asimilado, es oportuno juzgar el campo de las *DeFi* de manera equilibrada.

Para empezar, uno de los factores más relevantes y característicos de las Finanzas Descentralizadas son su fuerte componente tecnológico que genera una gran brecha con respecto a los paradigmas más tradicionales de hacer finanzas. Sí es cierto que, a lo largo del proyecto, ha sido bastante perceptible el reciclaje de múltiples aspectos de las finanzas más convencionales por parte de las Finanzas Descentralizadas. Al fin y al cabo, estas entidades, sistemas o dinámicas de las CeFi que se reutilizan en los mercados descentralizados no buscan otra cosa que la mayor eficiencia del capital. En este sentido, sí que se puede considerar que las *DeFi* mantienen muchas similitudes teóricas con las *CeFi*. Sin embargo, las finanzas no se hacen efectivas de manera teórica y es por ello que, a un nivel más pragmático o funcional, tratar las *DeFi* y las *CeFi* en el mundo real como áreas afines no sería proporcionado, ni siquiera con una mira más superficial.

Las bases de las finanzas bien conocidas se han asentado después de un trayecto de siglos de duración. El factor tecnológico en las finanzas centralizadas ha surgido de manera mucho más tardía. Precisamente, la automatización y digitalización de los mercados financieros con la aportación tecnológica, ha resultado en un importante empuje en el sector financiero. Consecuentemente, ha dado de sí numerosos sistemas o instrumentos que han desarrollado nuevas estrategias o mecanismos financieros inviables hasta el momento. Incluso, podríamos comparar esta primera ola de innovación tecnológico-financiera que ha estado sucediendo en las últimas décadas con la nueva revolución actual que constituyen las finanzas descentralizadas. Aunque satisfechos de maneras muy distintas, beneficios como un mayor acceso al comercio financiero, la globalización del mercado o la reducción de costes o tiempos de transacción también nos recuerda a las aportaciones prometidas por las *DeFi*. La gran y rotunda diferencia entre las *CeFi* y las *DeFi* es que las primeras pueden existir sin la tecnología, mientras que las segundas solo son posibles gracias a Blockchain.

Definitivamente, las finanzas convencionales han sufrido una transformación que las ha actualizado conforme al desarrollo tecnológico actual, pero en esencia, sigue una estructura muy firme arraigada en la centralización. Por el contrario, las Finanzas Descentralizadas nacen de la mano de Blockchain, valiéndose de esta infraestructura tecnológica para plantear un modelo totalmente novedoso opuesto al paradigma institucional y centralizado convencional. En este sentido, las *DeFi* son una revolución

mientras que las *CeFi* actuales quedan como una mejora, producto del progreso tecnológico.

Justamente esta consolidación de los mercados descentralizados en la tecnología Blockchain hace muy difícil separar el elemento técnico del financiero. La naturaleza de una criptomoneda, la ejecución de un *flash loan*, la emisión algorítmica de un token, la liquidez concentrada de Uniswap V3 o la mecánica subyacente a una red de oráculos son algunos de los puntos que se han explorado y, ¿cómo se podrían abordar esto campos si no es con una mínima aproximación a la tecnología? En definitiva, no es viable ahondar en el concepto de *flash loan* sin saber lo que es un contrato inteligente.

De vuelta a las *CeFi*, matizamos que efectivamente existen operaciones financieras como el análisis técnico o el comercio intensivo (HFT) a corto plazo que solo es viable con la digitalización de mercados como la Bolsa. Aun así, insistimos que la metodología con la que opera radica en un modelo bien conocido; sin ir más lejos, la primera bolsa de valores data en el siglo XV [60].

Aunque ya se han expuesto muchos de los aportes que tiene en Blockchain a las finanzas en términos de seguridad, este mismo arraigo de las *DeFi* en la tecnología puede ser un arma de doble filo. Es decir, la confianza en el sistema se desplaza a un hardware y software que no está exento de limitaciones y trabas. Más aún cuando la inclusividad que promueve este sistema hace accesible la participación de muchos más usuarios. Y estos usuarios no son solo operadores, sino que también pueden involucrarse como agentes creadores de mercado desplegando protocolos al alcance de los demás miembros del entorno. Es decir, un sistema asentado en la red e implementado por un o unos usuarios de manera deficiente o malintencionada puede constituir un importante riesgo para el mercado. El alcance de este riesgo irá condicionado por multitud de factores, pero vale decir que la irreversibilidad que caracterizan las *DeFi* puede convertirse en un importante inconveniente en estos casos.

Recapitulando, los perjuicios e ineficiencias que pudieran producir la intervención humana en las finanzas han sido mitigados exitosamente dotándolas de una descentralización, automatización y autonomía que ha derivado en una marginalización del juicio humano [61]. Existen numerosos testimonios de esta flaqueza, siendo uno de los más populares el "Ataque al DAO" lanzado en 2016 y que sustrajo 60 millones de dólares en fondos de *Ether* y que, paradójicamente, solo se pudo corregir con la intervención explícita humana, generando una bifurcación o *fork* de la red Ethereum para "deshacer" la malversación de los fondos lograda mediante el ataque [62] [63].

Haciendo este balance, podríamos concluir que las finanzas descentralizadas amortiguan muchos de los riesgos más pesados del sector financiero tradicional a costa de incrementar los riesgos operacionales sujetos a la tecnología. Es justo repasar por última vez todas las ventajas que introducen.

Se ha visto cómo las *DeFi* limitan el poder de las grandes entidades financieras, no solo para maximizar la eficiencia que estas estructuras ya no eran capaces de ofrecer

sino también para alcanzar un mercado más accesible, honesto, proporcionado y común. Cuando se prescinde del control institucional, también se eliminan barreras de entrada y se fomenta una competencia justa. Por otro lado, es primordial mencionar una vez más la capacidad de auditoría pública de la que están dotados estos mercados gracias a la transparencia que define la tecnología en que subyace.

Se ha enfatizado la implicación de una comunidad a la cual se le retribuye el valor del sistema, es decir, se pretende construir un ecosistema que estimule la movilidad de los agentes y el capital a través de las diferentes plataformas para operar con los instrumentos en los que confíen. En última instancia se devuelve el valor a estos participantes, no cómo un dividendo o beneficio colateral, sino como compensación fundamental por su aporte al sistema. Al fin y al cabo, las mínimas comisiones o recompensas que retienen las redes Blockchain y los protocolos implementados sobre ellos van destinados fundamentalmente al mantenimiento de la infraestructura, el sistema y, en última instancia, en caso de que existan, a los tokens que representan el valor del protocolo o sistema del que se hace uso. Con esto se quiere llegar a que, los gastos en los que incurre un usuario al consumir los servicios o productos financieros no van asignados directamente a la remuneración de ningún tipo de directivos o personal humano. Esto ya supone una clara ventaja para una orientación honesta de la estrategia de los protocolos que operan en las redes Blockchain, que no buscan el beneficio de un individuo o grupo de interés secular, sino que persiguen la satisfacción de todos los miembros en los que se apoya el sistema.

Una cuestión que puede salir a flote es: ¿y qué incentivos existen para innovar en el contexto de las *DeFi* si no es percibiendo directamente un beneficio económico? Pues bien, es importante comenzar aclarando que los participantes de los mercados descentralizados se involucran desde un principio en este entorno accediendo a los valores que promulga la tecnología Blockchain, las *DeFi* y las entidades que participan en esta plataforma. Ya se conocen estos valores. Rápidamente señalamos que operar en Blockchain no te hace seguidor de una doctrina ni tampoco se va a defender la utopía de que los pioneros de las redes y protocolos que hoy en día sostienen miles de millones de dólares dieron a luz esta infraestructura con objetivos puramente altruistas y solidarios. Sin embargo, el origen de todas estas innovaciones sí que se inspira en el afán de dar una vuelta al paradigma financiero vigente con el foco puesto en un beneficio colectivo. Esto no implica la distribución estrictamente simétrica de bonificaciones entre todos los componentes del sistema, sino poner al alcance de cada individuo la posibilidad de involucrarse en operaciones que, potencialmente, le pueden otorgar el mismo valor que a cualquier otro agente del mercado sin marginación en función de la identidad personal, posición o capital del que se dispone.

Habiendo hecho hincapié en esta concepción comunitaria de las *DeFi*, se puede responder a la pregunta anterior: el incentivo para innovar consiste en crear valor no solo para sí mismo como individuo, sino para todos los participantes. Un perfecto ejemplo de esto se ha prestado cuando hablábamos del token UNI introducido por Uniswap V3 y tratado en la sección 3.4; el protocolo Uniswap reparte un 21% del total

de tokens UNI emitidos a su equipo de desarrolladores y futuros empleados. De esta manera, los propios responsables de producir, mantener y perfeccionar el protocolo perciben valor de su trabajo y ¿no es este estímulo suficiente para un mejor desempeño como profesional en las *DeFi*? Esta forma de incentivo no es ajena a las *CeFi*, donde es normal que algunas empresas e instituciones cedan acciones a empleados de la compañía [64].

Haciendo uso de estos argumentos se llega a la conclusión de que estudiar los *Decentralized Exchanges*, *Automated Market Makers* y determinados protocolos que lo implementan, ha otorgado gran proximidad a los principios y mecánicas de los mercados descentralizados. Se ha puesto en perspectiva algunos de los modelos más extendidos de las *CeFi* para trasladarlos a las *DeFi* con una vuelta de 180º. Tal y como ya se ha expresado en varias ocasiones en este trabajo, las Finanzas Descentralizadas vienen para quedarse con lo mejor de las finanzas convencionales y solventar muchas de sus lagunas.

Los *Decentralized Exchanges* sirven como plataformas de intercambio de criptoactivos que disponen de todos los atributos ventajosos de la descentralización del sistema. El sistema más paradigmático bajo el que se implementan los DEXes son los *Automated Market Makers*, que conjugan de manera óptima a agentes que ceden su capital (*Liquidity Providers*) y operadores que desean intercambiar sus criptoactivos. Ambas partes quedan satisfechas cuando los primeros reciben intereses por su capital mientras que los segundos obtienen el cambio deseado de manera instantánea, segura y con mínimo coste. El mecanismo de estos protocolos funciona íntegramente gracias a su implementación en contratos inteligentes, es decir, de manera totalmente descentralizada.

Uniswap fue la plataforma precursora de este ámbito y estableció como precedente la configuración de *Constant Product* que satisface la ecuación $a \cdot b = k$. En base al éxito que tuvo este servicio, surgen nuevos protocolos que se aproximan en mayor o menor medida a la mecánica de Uniswap, pero en general, buscan encontrar su nicho dirigiendo su propuesta hacia una cartera de tokens más acotada, una optimización de la eficiencia del protocolo o una reducción de las comisiones (entre otras diferencias). El *Yield Farming* (mencionado en el punto 3.2) introduce nuevos incentivos desde cada plataforma para involucrar a nuevos agentes. Simultáneamente, esto impulsa más aún el desarrollo de los mercados descentralizados y el lanzamiento de nuevos tokens en los que apoyar los protocolos propuestos desde cada servicio.

En base al estudio del Oráculo de Precios se ha logrado profundizar más aún en diferentes puntos de las *DeFi*. Por una parte, se ha comprendido la naturaleza flexible y diversa de los *swaps*. Por otro lado, se ha descubierto que una utilidad como la ofrecida desde este sistema puede resultar muy conveniente para operar en un entorno tan inestable como el de los mercados descentralizados, donde la naturaleza de los datos de los precios es de extrema importancia para lanzar una estrategia acertada.

Por último, con la casuística del Oráculo de Precios se ha podido mostrar uno de los aspectos más atractivos de las Finanzas Descentralizadas: la interoperabilidad. De alguna manera, este atributo compendia muchos de los otros rasgos definitorios. Es decir, la interoperabilidad abre los distintos mercados o plataformas del ecosistema *DeFi* para fomentar la participación de diferentes agentes y su movilidad a través de todo este universo. A su vez, se potencia el alcance de cada uno de los instrumentos que se producen, que no pretenden quedar limitados a su sector de origen, sino que son capaces de generar valor en muchas de las otras áreas (si no a todas). En definitiva, se motiva un flujo de información y activos sin barreras entre todos los mercados descentralizados.

Se concluye este trabajo expresando la esperanza de que el lector haya podido disfrutar su recorrido por este proyecto para lograr una mayor comprensión sobre las Finanzas Descentralizadas, los *Automated Market Makers* y los *Swaps*. Me llena de gratitud el que el recipiente de esta lectura haya podido encontrar cualquier tipo de valor en mi trabajo, aunque sean pequeñas nociones de conocimiento.

Hago notar que, yo mismo, a lo largo de este estudio, he experimentado un prolífico proceso de aprendizaje. Incluso he de reconocer que, a pesar de todas mis ambiciones al inicio del proyecto, definitivamente he alcanzado un nivel de entendimiento sore la materia mucho mayor de lo que esperaba. No obstante, soy totalmente consciente de que me queda mucho más que descubrir y aprender de este mundo y soy positivo al afirmar que las *DeFi* o los AMM tienen mucho más que ofrecer y que aún se encuentra en periodo de incubación.

Para conocer más sobre la tecnología en la que se soportan las *DeFi* o la programación de contratos inteligentes que hay detrás del Oráculo de Precios, mencionamos por última vez el Trabajo Fin de Grado de Ingeniería Informática "Blockchain y Contratos Inteligentes. Oráculo de Precios para Automated Market Makers", dónde podrá encontrar un extenso análisis al respecto.

6 Referencias

[1] CoinMarketCap, «CoinMarketCap,» [En línea]. Available: https://coinmarketcap.com/charts/. [Último acceso: mayo 2022].

[2] Edelman, «https://www.edelman.com/,» 2022. [En línea]. Available: https://www.edelman.com/trust/2022-trust-barometer. [Último acceso: Marzo 2022].

[3] D. &. A. Tapscott, Blockchain Revolution, Portfolio, 2016.

[4] X. Vives, «La Crisis Financiera y La Regulación,» *IESE Business School, Universidad de Navarra,* pp. 4-6, 2010.

[5] J. G. Jorrín, «elconfidencial.com,» febrero 2021. [En línea]. Available: https://www.elconfidencial.com/economia/2021-02-10/crisis-clases-medias-rentas-bajas-desigualdad_2943527/. [Último acceso: abril 2022].

[6] F. J. G. Gisbert, «Distribución de la Renta, Crisis Económicas y Políticas Redistributivas,» *Fundación BBVA,* 2016.

[7] S. Davidson, P. D. Filippi y J. Potts, «Economics of Blockchain,» 2016.

[8] Messari, «Crypto Theses for 2022,» 2022.

[9] Y. Chen y C. Bellavitis, «Blockchain disruption and decentralized finance: The rise of decentralized business models,» p. 2, 2020.

[10] D. Yaga, P. Mell, N. Roby y K. Scarfone, «Blockchain Technology Overview,» 2018.

[11] K. Quin, L. Zhou, Y. Afonin, L. Lazzaretti y A. Gervais, «CeFi vs. DeFi — Comparing Centralized to Decentralized Finance,» 2021.

[12] P. Schueffel, «DeFi: Decentralized Finance - An Introduction and Overview,» Vols. %1 de %29,3, 2021.

[13] V. P. Nartallo, «bbva.com,» Noviembre 2021. [En línea]. Available: https://www.bbva.com/es/que-diferencias-hay-entre-un-token-y-una-criptomoneda/. [Último acceso: Marzo 2022].

[14] T. B. o. N. Y. M. Corporation, «https://www.bnymellon.com/,» Junio 2019. [En línea]. Available: https://www.bnymellon.com/us/en/insights/all-insights/tokenization-opening-illiquid-assets-to-investors.html. [Último acceso: Marzo 2022].

[15] T. Farren, «es.cointelegraph.com,» enero 2022. [En línea]. Available: https://es.cointelegraph.com/news/immunefi-report-10b-in-defi-hacks-and-losses-across-2021. [Último acceso: marzo 2022].

[16] A.-D. Popescu, «Transitions and Concepts Within Decentralized Finance Space,» 2020.

[17] R. d. Best, «statista.com,» febrero 2022. [En línea]. Available: https://www.statista.com/statistics/863917/number-crypto-coins-tokens/#:~:text=How%20many%20cryptocurrencies%20are%20there,of%20digital%20coins%20in%202013. [Último acceso: 2022 marzo].

[18] J. Chen, «Investopedia,» Investopedia, 4 mayo 2022. [En línea]. Available: https://www.investopedia.com/terms/p/pricediscovery.asp. [Último acceso: 15 mayo 2022].

[19] S. Seth, «Investopedia,» Investopedia, marzo 2022. [En línea]. Available: https://www.investopedia.com/articles/active-trading/090815/picking-right-algorithmic-trading-software.asp. [Último acceso: mayo 2022].

[20] V. Lazen y J. R. M. Resano, «El proceso de compensación y liquidación de valores,» *Estudio sobre los sistemas de registro, compensación y liquidación de valores en Iberoamérica,* vol. Capítulo II.

[21] F. Schär, «Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,» pp. 160-163, 2021.

[22] J. R. Jensen, V. v. Wachter y O. Ross, «An Introduction to Decentralized Finance,» 2021.

[23] V. Mohan, «Automated market makers and decentralized exchanges: a DeFi primer,» *Financial Innovation,* 2022.

[24] L. Heimbach, Y. Wang y R. Wattenhofer, «Behavior of Liquidity Providers in Decentralized Exchanges,» 2021.

[25] «Binance Academy,» 2022. [En línea]. Available: https://academy.binance.com/es/articles/what-is-an-automated-market-maker-amm. [Último acceso: mayo 2022].

[26] «DeFi Pulse,» abril 2022. [En línea]. Available: https://www.defipulse.com/. [Último acceso: abril 2022].

[27] «MakerDAO,» [En línea]. Available: https://makerdao.com/. [Último acceso: abril 2022].

[28] M. Risius y K. Spohrer, «A Blockchain Research Framework,» *Springer,* 2017.

[29] «AAVE,» [En línea]. Available: https://aave.com/. [Último acceso: abril 2022].

[30] A. Lehar y C. A. Parlour, «Decentralized Exchanges,» p. 46, 2022.

[31] J. Xu, K. Paruch, S. Cousaert y Y. Feng, «SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols,» 2022.

[32] C. A. P. Alfred Lehar, «Decentralized Exchanges,» p. 46, 2022.

[33] A. Hayes, «Investopedia,» 10 mayo 2021. [En línea]. Available: https://www.investopedia.com/terms/s/slippage.asp#:~:text=Slippage%20refers%20to%20all%20situations,market%2Dmaker%20executes%20the%20order.. [Último acceso: 1 mayo 2022].

[34] «Alpaca Finance,» noviembre 2021. [En línea]. Available: https://docs.alpacafinance.org/alpaca-academy/lesson-5-the-truth-about-impermanent-loss-and-common-misunderstandings. [Último acceso: mayo 2022].

[35] «CoinMarketCap,» mayo 2022. [En línea]. Available: https://coinmarketcap.com/es/rankings/exchanges/dex/. [Último acceso: mayo 2022].

[36] «Uniswap Docs,» marzo 2022. [En línea]. Available: https://docs.uniswap.org/protocol/V2/introduction. [Último acceso: mayo 2022].

[37] Uniswap Labs, «Uniswap Docs,» [En línea]. Available: https://docs.uniswap.org/protocol/V2/concepts/core-concepts/flash-swaps. [Último acceso: mayo 2022].

[38] Uniswap Labs, «Uniswap Docs,» [En línea]. Available: https://docs.uniswap.org/protocol/V2/guides/smart-contract-integration/using-flash-swaps. [Último acceso: mayo 2022].

[39] J. Yin y M. Ren, «On Liquidity Mining for Uniswap v3,» 2021.

[40] M. Neuder, R. Rao, D. J. Moroz y D. C. Parkes, «Strategic Liquidity Provision in Uniswap v3,» 2021.

[41] Z. Fan, F. Marmolejo-Coss, B. Altschuler, H. Sun, X. Wang y D. C. Parkes, «Di erential Liquidity Provision in Uniswap v3 and Implications for Contract Design,» *Harvard University, IOHK,* 2022.

[42] Uniswap, «Introducing UNI,» septiembre 2020. [En línea]. Available: https://uniswap.org/blog/uni. [Último acceso: mayo 2022].

[43] J. Young, «Se lanzó Uniswap V3 - el precio del token UNI se dispara un 8% en minutos,» *cointelegraph.com,* 23 marzo 2021.

[44] Uniswap Labs, «uniswap.org,» 23 marzo 2021. [En línea]. Available: https://uniswap.org/blog/uniswap-v3. [Último acceso: mayo 2022].

[45] «Uniswap Docs,» [En línea]. Available: https://docs.uniswap.org/protocol/concepts/V3-overview/fees. [Último acceso: mayo 2022].

[46] M. C. Ab, «GitHub,» MariaDB Corporation Ab, 2021. [En línea]. Available: https://github.com/Uniswap/v3-core/blob/main/LICENSE. [Último acceso: mayo 2022].

[47] The Shrimpy Team, «shrimpy academy,» octubre 2021. [En línea]. Available: https://academy.shrimpy.io/post/uniswap-vs-sushiswap-which-defi-exchange-is-better. [Último acceso: mayo 2022].

[48] J. Finneseth, «Cointelegraph,» febrero 2021. [En línea]. Available: https://es.cointelegraph.com/news/dex-goals-diverge-as-sushiswap-sushi-and-uniswap-uni-rally-to-new-highs. [Último acceso: mayo 2022].

[49] The Shrimpy Team, «shrimpy academy,» octubre 2021. [En línea]. Available: https://academy.shrimpy.io/post/what-is-curve-finance. [Último acceso: mayo 2022].

[50] G. Ovadia, «MoneyMade,» 12 mayo 2022. [En línea]. Available: https://moneymade.io/learn/article/curve-vs-uniswap-balancer. [Último acceso: 19 mayo 2022].

[51] 1inch, «1inch,» [En línea]. Available: https://1inch.io/aggregation-protocol/. [Último acceso: mayo 2022].

[52] Dappgrid, «dappgrid,» febrero 2021. [En línea]. Available: https://dappgrid.com/1inch-vs-uniswap/. [Último acceso: mayo 2022].

[53] A. Shevchenko, «Cointelegraph,» marzo 2021. [En línea]. Available: https://es.cointelegraph.com/news/new-version-of-1inch-s-dex-aggregator-makes-it-cheaper-than-uniswap. [Último acceso: mayo 2022].

[54] S. Dickens, «yahoo! finance,» noviembre 2021. [En línea]. Available: https://finance.yahoo.com/news/1inch-dex-rolls-v4-version-104409356.html. [Último acceso: mayo 2022].

[55] 1inch, «1inch,» [En línea]. Available: https://1inch.io/token/. [Último acceso: mayo 2022].

[56] L. Breidenbach, A. Coventry, C. Cachin, S. Ellis, A. Miller, A. Juels, B. Magauran, S. Nazarov, A. Topliceanu y F. Zhang, «Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks,» 2021.

[57] «Chainlink,» [En línea]. Available: https://chain.link/data-feeds#price-and-market-feeds. [Último acceso: mayo 2022].

[58] «Chainlink Docs,» [En línea]. Available: https://docs.chain.link/docs/link-token-contracts/. [Último acceso: mayo 2022].

[59] «Financially Independent Pharmacist,» octubre 2021. [En línea]. Available: https://thefipharmacist.com/uni-vs-link/. [Último acceso: mayo 2022].

[60] «Expansión,» Economía para andar por casa, [En línea]. Available: https://www.expansion.com/economia-para-todos/inversion/que-es-la-bolsa-cual-fue-su-origen-y-funcion.html#:~:text=La%20primera%20bolsa%2C%20en%20sentido,de%20Madrid%2C%20creada%20en%201831.. [Último acceso: mayo 2022].

[61] Y. Chen y C. Bellavitis, «Decentralized Finance: Blockchain Technology and the Quest for an Open Financial System,» 2019.

[62] C. Staff, «gemini.com,» 17 marzo 2022. [En línea]. Available: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao. [Último acceso: 2022 abril 2022].

[63] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim y M. Laskowski, «Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack,» *Journal of Cases on Information Technology*, vol. 21, nº 1, 2019.

[64] M. d. Pozo, «blogs Expansión,» marzo 2022. [En línea]. Available: https://www.expansion.com/blogs/peon-de-dama/2022/03/13/motivar-al-empleado-con-acciones.html. [Último acceso: mayo 2022].

[65] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz1 y W. J. Knottenbelt, «SoK: Decentralized Finance (DeFi),» 2021.