UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Finanzas Descentralizadas

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Raúl Borrega Langa

Tutor: Fernando José Garrigós Simón

2020/2021

Resumen

Las criptomonedas y la tecnología blockchain han tenido un gran auge este último año y con ello la sección de las Finanzas Descentralizadas (DeFi). Sin embargo, la atención a las mismas no ha sido acorde. A pesar de que las DeFi han crecido exponencialmente, los materiales para ayudar a las personas a comprenderlas han quedado a su vez rezagados. Con objeto de acelerar la adopción de esta alternativa a las finanzas tradicionales, este trabajo busca simplificar los diseños complejos de esta idea para que sean entendibles y accesibles para el público, y que éste puedaadentrarse en este fenómeno actual. Esta investigación tratará los conceptos más comunes para entender cómo esta nueva tecnología va a beneficiar de múltiples maneras a la sociedad y cómo puede cambiar las diversas formas de observar el sector financiero. El desarrollo de este proyecto no ha sido aislado, dado que nos ha conducido a la búsqueda de oportunidades para conseguir rentabilidad dentro de las DeFi, y a la creación de una empresa para atender a la gran demanda que generaban estos conocimientos. El objetivo principal es explicar una simple idea, que ha terminado siendo un mercado financiero activo descentralizado funcionando paralelamente con el tradicional.

El trabajo se desarrolla en base a los diferentes proyectos construidos en la red Ethereum, aunque el concepto se puede aplicar a toda la tecnología y a cualquier red. El trabajo explica los proyectos más importantes que hay actualmente en el sector, qué arquitectura interna tienen y cómo han tenido tanto impacto. Por último, se desarrollan los problemas latentes hoy en día y se plantean soluciones a los mismos, finalizando con una reflexión y una conclusión sobre el análisis realizado.

Palabras clave: Criptomonedas, blockchain, DeFi, Ethereum.

Abstract

Cryptocurrencies and blockchain technology have had a huge boom this last year and with it the Decentralized Finance (DeFi) section, although it is not given the attention it requires. DeFi has grown exponentially, but the materials to help people understand this concept have lagged behind. To accelerate the adoption of this great alternative to traditional finance, this work seeks to make the complex designs of this great idea simple for the public to understand and accessible so that they can delve into this great phenomenon of today. This research will deal with the most common concepts to understand how this new technology is going to bring a large number of benefits to society and how the various ways of seeing the financial sector can change. Everything that will be explained in this project has led me to dedicate myself partially to the search for opportunities to achieve profitability within the DeFi, to the point of having to create a company due to the great demand generated by this knowledge. The main objective is to explain a simple idea, which has ended up being a decentralized active financial market working in parallel with the traditional one.

The work is developed based on the different projects built on the Ethereum network, but the concept can be applied to all technology and to any network. The most important projects currently in the sector will be explained, what internal architecture they have and how they have had such an impact. Finally, the problems that are latent today will be developed and in what way they will be solved, ending with a reflection and a conclusion on everything that was previously discussed.

Keywords: Cryptocurrencies, blockchain, DeFi, Ethereum.

Tabla de contenidos

Índice de ilustraciones

1. Introducción

El mundo de la informática va evolucionando muy rápidamente y si no se le dedica tiempo suficiente a estar informado no se puede estar al tanto de lo que va sucediendo en el panorama actual. En la época actual todo se desarrolla con velocidad y la sociedad tecnológica se encuentra en constante cambio, creando de esta forma una carrera tecnológica entre los usuarios activos de este sector de forma inconsciente.
Con la llegada de la Web 3.0, la web de la descentralización, era de esperar que surgieran otras formas de ver las aplicaciones que tiene internet en el actual mundo globalizado. Con esta necesidad imperiosa nacieron diferentes proyectos basados en la tecnología blockchain, con muchos intentos fallidos, hasta que una persona con seudónimo de Satoshi Nakamoto presentó el documento en el que detalla la nueva forma que había inventado para pagos por internet y que resolvía el gran problema del "double spending" que mantenía en jaque a la comunidad de la época. De esta forma nació el rey de las criptomonedas y la que dirige actualmente el panorama, Bitcoin.
Esta nueva forma de pagos *peer to peer* mediante una red blockchain, fue un camino hacia la innovación, privacidad y descentralización que trajo consigo una gran cantidad de personas interesadas por el proyecto, entre ellos Vitalik Buterin.
Vitalik fue uno de los cofundadores de Ethereum, la red en la que principalmente se basará este Trabajo Fin de Grado y en la que están construidos la gran parte de proyectos que mencionaremos más adelante. Esta red, considerada como la reina, ha conseguido llevar la adopción de las criptomonedas a otro nivel junto a Bitcoin, pero esta última se creó con propósitos diferentes a Bitcoin, entre ellos, estos últimos años se ha estado formando un movimiento financiero descentralizado que creó las llamadas Finanzas Descentralizadas (DeFi). Este sector dentro de las criptomonedas captó la atención de millones de personas, debido a la velocidad con la que estaba creciendo y a las diferentes aplicaciones que tienen. Las DeFi son proyectos que aún están en fase de desarrollo y son proyectos experimentales, igual que Ethereum y todas las criptomonedas, aunque tengan grandes cantidades de capital dentro de ellas, son experimentos, tecnologías que buscan diferentes enfoques para que prosperen en la sociedad y que vayan de la mano con el avance del tiempo y que desemboque en un futuro mejor.
Una de las ideas que más asombró al panorama fue la de intentar crecer junto a un sistema financiero que mueve la economía global y que arrasa con todo aquello que se interpone en su camino. Hoy en día, las personas dependen y confían en los grandes intermediarios, como los bancos, gobiernos… para establecer una confianza en nuestra economía y esos intermediarios son los que llevan a cabo las transacciones de las empresas. El problema, es que está centralizado, excluye a billones de personas de la economía global, por ejemplo, aquellas que no tienen dinero suficiente. Las DeFi, pretenden cambiar esta situación. En este Trabajo Fin de Grado, explicaremos los fundamentos de las finanzas descentralizadas, sus riesgos, beneficios, visión, proyectos… y la pretensión de las mismas de crear consigo un mejor sistema financiero y más justo. La busqueda de los conocimientos aportados en este trabajo, nos ha conducido, paralelamente, a la creación de una empresa, con el fin de maximizar los retornos mediante el uso las herramientas que ofrecen estos activos digitales.

1.1 Motivación

La elección de este tema se debe a que, durante cierto tiempo, impulsados por la curiosidad, hemos estado dedicando una cierta cantidad de tiempo a aprender sobre este tema en mi tiempo libre. En los inicios, todo empezó como una forma alternativa de ganar dinero y, poco a poco, se convirtió en la pasión que tanto tiempo llevabamos buscando. Era la fórmula perfecta: inversiones, riesgo, tecnología, grandes retornos y grandes pérdidas. Cualquiera que escuchara lo que conllevaba invertir en este nuevo paradigma se interesaba por aprender más al respecto. Posteriormente, se creó una nueva forma de finanzas, que pretendían ser la alternativa a las finanzas tradicionales que conocemos hoy en día. Esto y las nuevas herramientas que ofrecía esta tecnología, sumado a la falta de desarrollos prácticos, fue lo que captó totalmente nuestra atención.

1.2 Objetivos

El objetivo de este trabajo es el poder profundizar en el conocimiento de un tema de actualidad y que ha tenido y continúa teniendo un crecimiento exponencial en los últimos años: las Finanzas Descentralizadas. Las DeFi han llegado para quedarse y explicar e introducir los beneficios que estas traen a la sociedad y cómo pueden cambiar sus formas de ver este sector. Con el auge de las criptomonedas, sobre todo en los años que parece que el dinero llueve del cielo, no todo el mundo habla de esta sección, cuando en verdad es una de las que más potencial tiene. Con este trabajo pretendemos que, cuando todo el mundo deje de hablar de las criptomonedas por el fin de los momentos de ganancias, que el publico en general conoceza este maravilloso mundo que la informática ha construido y expandido por todos los rincones de nuestro planeta.
DeFi ha crecido muy rápidamente en el último año, pero los materiales para ayudar a las personas a comprenderlo no han crecido en la misma medida. Para acelerar la adopción de DeFi, queremos hacer que los diseños complejos de DeFi sean simples de entender para el público, y accesibles para que puedan comenzar su travesía. Esperamos que al compartir nuestros aprendizajes, ellos puedan ayudar al lector a ponerle al día con DeFi, con objeto de que pueda unirse para participar en este movimiento.

1.3 Impacto esperado

El impacto esperado al finalizar el Trabajo Fin de Grado es que cualquier persona, después de leer y entender este trabajo, obtenga una información sencilla y práctica sobre las DeFi y sus conceptos, de forma que puedan interactuar con las diferentes aplicaciones que se están ejecutando en la red Ethereum. También, se pretende que después de este trabajo, las personas interesadas puedan llevar a cabo investigaciones mucho más técnicas y que cuando escuchen noticias sobre este ámbito puedan tener firmes opiniones y conocimientos al respecto.

Conocer el intrincado mundo de las nuevas tecnologías conlleva a estar al tanto de lo que sucede en la sociedad y que intereses la está moviendo y hacia dónde está yendo.

1.4 Metodología

El proyecto ha sido desarrollado mediante el uso de muy diversas herramientas e información, provenientes de los creadores de los proyectos, y ofrecidas en sus respectivas páginas web. Se han invertido numerosas horas de investigación para que toda la información encontrada en internet se plasme de la forma más sencilla posible, para que cualquier lector pueda entender el concepto de DeFi.
A todo esto, se le ha sumado la experiencia que adquirida durante 3 años de trabajan a tiempo parcial, en un puesto de inversor en proyectos de criptomonedas con baja capitalización de mercado e ICOs relacionadas con DeFi. Hemos probado numerosas estrategias y alcanzar el máximo rendimiento ha requerido un gran esfuerzo de análisis y estudio del mercado al igual que conocer a fondo las funcionalidades de este sector.

1.5 Estructura

Esta memoria se divide en 8 apartados, más las referencias. El segundo apartado se utiliza como antecedente sobre el tema a tratar, explicando el motivo del surgimiento de este tipo de finanzas, y comparándolas con las tradicionales A su vez, cada uno de los restantes capítulos,con una estructura similar y homogenea, realiza una introducción sobre lo que se va a explicar,habla de sus componentes principales, características y por último propone un caso práctico muy común entre los usuarios de estas plataformas, para que el lector se acerque un poco más al entorno de trabajo. A continuación, enumeramos de forma breve lo mencionado anteriormente:

1. **Introducción:** se determina el tema a abordar de forma general, además de realizarse una breve explicación del contexto actual.
2. **DeFi y las finanzas tradicionales:** se enumeran y explican las diferencias entre los dos tipos de finanzas, con sus ventajas y desventajas.
3. **Blockchain Ethereum:** provee información general de la red Ethereum, para abordar en qué tecnología se basa esta nueva forma de finanzas.
4. **Stablecoins descentralizadas**: estudia un tipo de moneda estable basada en la red Ethereum y cómo se gobierna de forma autónoma.
5. **Exchanges descentralizados**: indaga sobre las plataformas de intercambio de criptomonedas, sobre que fundamentos se basan y cómo están implementadas.
6. **Préstamos descentralizados:** se muestra cómo es gestionada a través de los contratos inteligentes una plataforma descentralizada de préstamos denominada Compound.
7. **Ethereum 2.0:** recoge información acerca de cómo se va a implementar la siguiente versión de la red Ethereum y cómo va a afrontar los diferentes

problemas actuales que llevan a Ethereum a ser una red con diversos contratiempos cuando la red es altamente demandada.

8. **Conclusión:** finaliza el trabajo con un análisis sobre el sector actual de las criptomonedas desde el punto de vista del usuario y con una conclusión que observa limitaciones, y nuevas perspectivas o trabajos juturos, tratando a su vez sobre cómo se prevé que este sector afronte un presente y futuro de incertidumbre.
9. **Bibliografía:** donde se encuentra un listado de toda la documentación y páginas webs consultadas para la elaboración del estudio y posibles consultas a realizar si el lector decide indagar más en el tema.

2. DeFi y las finanzas tradicionales

En este apartado, se van a explicar las diferencias entre las finanzas centralizadas y descentralizadas y las características de cada unade ellas. Además, se van a exponer las ventajas y desventajas que ofrecen y cómo conviven cada una con la otra hoy en día.

2.1 Bancos

Para simplificar, este subapartado se va a centrar en las instituciones más importantes del sistema financiero tradicional, los bancos, además de discutir sus principales áreas para observar los potenciales riesgos que puede representar el estar altamente apalancado.

2.1.1 Sistema financiero actual

Los bancos son los gigantes de la industria financiera que facilitan los pagos, aceptan depósitos y ofrecen líneas de crédito a personas, empresas, otras instituciones financieras e incluso gobiernos. Son tan grandes que los 5 bancos más importantes representan una capitalización de mercado de 19,5 Trillones de USD [1]. En contraste, para que observemos el poder de crecimiento de las criptomonedas, la capitalización de mercado de las criptomonedas alcanzó los 2,5 Trillones de USD en mayo de 2021, cuando hace 5 años la capitalización era de sólo 6 Billones de USD [2].

Bancos más importantes en 2021 [3]:

1. JPMorgan Chase: 488.600 MUSD
2. Bank of America: 358.790 MUSD
3. ICBC: 274.650 MUSD
4. China Construction Bank: 202.760 MUSD
5. Wells Fargo: 192.410 MUSD

Aunque la economía pueda parecer compleja, funciona de una forma simple y mecánica. Consta de unas transacciones simples que se repiten infinidad de veces, impulsadas por la naturaleza humana. Las personas, empresas, bancos y gobiernos todos participan en transacciones, canjean dinero y crédito por mercancías, servicios y activos financieros. El crédito es la parte más importante de la economía y seguramente la más incomprendida, cuando es la más importante porque es la más grande y la más volátil. Aquí entran en juego los prestamistas y los prestatarios, los prestamistas quieren convertir su dinero en más dinero, y los prestatarios quieren pedir prestado dinero porque no pueden pagar algo que quieren. Los prestatarios deben devolver el dinero prestado más una cantidad de dinero, al cual se le denomina interés. Cuando el prestatario promete devolver el préstamo y los prestamistas les creen, se crea el crédito. Pero no todo es tan sencillo, el crédito tiene una doble cara, ya que por cada crédito dado hay una deuda. ¿Y por qué el crédito es tan importante?,

porque cuando un prestatario obtiene un crédito significa que por algo lo ha pedido, es decir, que puede aumentar los gastos y el gasto impulsa la economía.
Los bancos tienen una importancia muy clara en el sistema financiero y su función ha sido aceptada desde hace tiempo por todos los países. Resultan fundamentales para que la economía evolucione, siendo su misión realizar una buena gestión de los recursos económicos, alcanzar una estabilidad monetaria y bancaria y proporcionar seguridad en los sistemas de flujo de capital. Los bancos [4] son entidades centralizadas, que desempeñan un papel central en el sistema financiero, de esto deriva su alta participación e influencia en la actividad económica de los países.
Actúan como intermediarios financieros de la mano de la ley de la oferta y la demanda, además de tener la capacidad de estimular, recibir el ahorro de una sociedad, y, por otro lado, distribuirlo entre los diferentes factores que componen la base del capitalismo para que completen sus acciones de consumo e inversión.
Los bancos son una parte fundamental de la *Economic Machine* [5], ellos permiten que el dinero se mueva por todo el mundo, ofreciendo servicios de transferencias de valor como son los depósitos, retiradas y transferencias, créditos y mucho más. No obstante, los bancos están manejados, dirigidos y gobernados por políticas humanas, esto quiere decir que los humanos son propensos a cometer muchos errores en la gestión y, sobre todo, de corrupción.
Un ejemplo básico es la crisis de 2008 [6], esto es la representación exacta de la codicia humana, de la cantidad de riesgos que toman los bancos y todo lo que son capaces de hacer, para que unos pocos ganen dinero mientras millones de personas pierden sus trabajos, sus casas etc. La crisis expuso las deficiencias del sistema financiero tradicional y destacó la necesidad de mejorarlo.
DeFi busca construir un mejor marco financiero gracias a la ayuda de internet y de la tecnología blockchain.

2.1.2 Sistema de pago y transferencia

Las personas que han intentado enviar dinero a alguien o a alguna empresa en otro país, conocen muy bien este proceso: las remesas que involucran a bancos de todo el mundo suelen tardar varios días laborables en completarse [7] e implican todo tipo de tarifas. Para empeorar las cosas, también puede haber problemas con la documentación, el cumplimiento de las leyes contra el lavado de dinero, problemas de privacidad y más. Por ejemplo, si se vive en España, y se desea enviar 1.000 € desde su cuenta bancaria en España a la cuenta bancaria de un amigo en China, generalmente hay tres tarifas involucradas: el tipo de cambio de su banco, la transferencia internacional saliente tarifa y la tarifa de entrada de transferencia internacional. Además, el destinatario tardará unos días hábiles en recibir el dinero, según la ubicación del banco destinatario.
La verdad, es que esto que se ha explicado no incita a realizar transferencias de un país a otro, de hecho, cada vez más se están buscando alternativas legales para realizar estas acciones con muchos menos trámites. Los proyectos que impulsan el movimiento DeFi, permiten evitar a los intermediarios que se llevan la mayor parte de las ganancias de estas transferencias. Es muy probable que también sea más rápido y seguro: las transferencias se procesarán sin preguntas y con tarifas relativamente más bajas en comparación con los bancos. Por ejemplo, la transferencia de Ether en la red

Ethereum a cualquier parte del mundo costaría entre 15 segundos y 10 minutos dependiendo de varios factores (congestión de la red etc) [4], junto con una pequeña tarifa, normalmente. La red Ethereum que es de las más utilizadas para transacciones, tiene unas tarifas “elevadas”, con una media situada alrededor 11$, debido al elevado uso de la red; pero hay una gran variedad de opciones con tarifas insignificantes, como por ejemplo la red Solana, que posee de media unas tarifas de 0,000005 dólares por transacción [8].

2.1.3 Accesibilidad

Lo más probable es que cualquier persona que esté leyendo este trabajo, esté dado de alta en algún banco y tenga acceso a los servicios financieros que ofrecen los bancos: abrir una cuenta de ahorros, pedir un préstamo, realizar inversiones etc. Sin embargo, también hay muchos más que no son tan afortunados y no tienen acceso ni siquiera a la cuenta de ahorros más básica. El Banco Mundial estima que, en 2017, había 1.700 millones de personas que no poseian una cuenta en una institución financiera y más de la mitad de ellas son de países en desarrollo [9]. Provienen principalmente de hogares pobres y algunas de las principales razones para no tener una cuenta bancaria se deben a problemas de pobreza, geográficos y de confianza.

Para los 1.700 millones de personas no bancarizadas, el acceso a la banca es difícil, pero DeFi tiene el potencial de hacerlo más fácil. Acceder a DeFi Dapps solo requiere que una persona tenga un teléfono móvil y acceso a Internet, en lugar de pasar por los largos procesos de verificación. El Banco Mundial estima que dos tercios de los 1.700 millones de personas no bancarizadas tienen acceso a teléfonos móviles [10] y las DeFi Dapps pueden suponer la entrada de numerosas personas para acceder a productos financieros de una forma sencilla, a diferencia de los bancos tradicionales. DeFi representa un movimiento revolucionario que busca impulsar productos financieros sin fronteras, sin censura y accesibles para todos. Los protocolos DeFi no discriminan a nadie y nivelan el campo de juego para todos.

2.1.4 Centralización y transparencia

No se puede negar, que las instituciones financieras reguladas tradicionales que cumplen con las leyes y regulaciones gubernamentales, como los bancos, son algunos de los lugares más seguros para depositar fondos. Pero no están exentos de fallos, incluso los grandes bancos pueden quebrar. Washington Mutual con más de $188 mil millones [11] en depósitos y Lehman Brothers con $639 mil millones [12] en activos quebraron en 2008. Sólo en los Estados Unidos, se han registrado más de 500 quiebras bancarias [13].
Los bancos son uno de los puntos centralizados de quiebra del sistema financiero: la caída de Lehman Brothers desencadenó el inicio de la crisis financiera de 2008. La centralización del poder y los fondos en manos de los bancos es peligrosa mirando los incidentes pasados.
La transparencia también se relaciona con esto: no hay forma de que los inversores habituales sepan completamente lo que hacen las instituciones financieras. Algunos ejemplos son los eventos que ocurrieron antes de la crisis financiera de 2008, las

diferentes agencias de calificación crediticia que otorgaron calificaciones AAA (las inversiones más seguras y con una rentabilidad relativamente buena) a valores respaldados por hipotecas de alto riesgo [14]…
Es diferente con DeFi, con los protocolos construidos sobre blockchains públicas como Ethereum, que son en su mayoría de código abierto, con fines de auditoría y transparencia. Ello se debe a que, por lo general, tienen organizaciones de gobierno descentralizadas para garantizar que todos sepan lo que está sucediendo y que ningún mal actor pueda tomar malas decisiones por sí solo.
Los protocolos DeFi están escritos como líneas de códigos; no se puede engañar a los códigos, ya que trata a todos los participantes por igual sin discriminación. Los códigos se ejecutan exactamente como están programados, y cualquier defecto se hace evidente rápidamente, ya que está abierto al escrutinio público. Al final del día, la mayor fortaleza de DeFi radica en poder eliminar intermediarios y operar sin censura.

2.1.5 Problemas de la centralización

Cuando se habla de centralización [15] se hace referencia a un punto donde el control y el poder está centrado en una persona, grupos de personas, entidad, grupos de entidades etc. En el caso de las finanzas, básicamente este control y poder recae en los bancos, que como se ha notado durante el paso del tiempo, tienen una gran influencia social, económica y política. Históricamente, la centralización en finanzas se había llevado a cabo para tener una estabilidad en los procesos de finanzas globales, debido a que se consideraba más segura y estable que la gestión personal. Estos sistemas, además eran de gran ayuda para las transferencias internacionales, debido al alcance de la infraestructura. Pero existe un problema: El sector financiero no es tan estable como se pensaba. Si se es realista, se puede deducir que los sistemas financieros centralizados se ven afectados por una variedad de problemas como el fraude, la falsificación, los procesos de préstamos y más.
Un argumento obvio a esta línea de razonamiento en cuanto a desventajas del sistema bancario actual, apuntaría a la extraordinaria geografía de internet y fungibilidad del dinero, y su capacidad para buscar oportunidades de préstamos e inversión dondequiera que se encuentren. Por muy extendidas que estén estas instituciones centralizadas en la sociedad actual, aún existen grandes brechas en la accesibilidad, aspecto extremadamente importante a resolver.
Según este punto de vista, un sistema financiero espacialmente centralizado por sí mismo no tiene implicaciones adversas para el suministro de préstamos o capital social a pequeñas empresas en regiones periféricas: lo que importa a las decisiones de préstamos e inversiones de los bancos centralizados y los mercados de capitales no es la ubicación de las empresas que buscan financiación, sino sus perfiles de riesgo-rendimiento. Con las finanzas descentralizadas no sucede, lo único que se debe de tener es una garantía suficiente para cubrir el préstamo, en caso de pérdida del dinero del préstamo. Da igual a quien se le haya dado el préstamo, que quieras hacer con el dinero, todos esos problemas son dependientes de tus decisiones.
Es complejo entrar y hacerse hueco en el sistema financiero actual, sobre todo a nivel de empresa; hay mucha competencia y en cuanto los intereses personales interfieran con los de una entidad mayor, esta mayor potencia económica arrebatará el poco poder de decisión y de libertad que esa nueva competencia poseía.

2.2 DeFi

Las Finanzas Descentralizadas o DeFi [16], es el movimiento que permite a los usuarios utilizar servicios financieros como préstamos, trading etc., sin la necesidad de depender o confiar en entidades centralizadas. Estos servicios financieros son ofrecidos vía Dapps [17] (Aplicaciones descentralizadas), las cuales la gran mayoría, aunque cada vez menos, están desplegadas y ejecutadas en la red Ethereum [18]. DeFi no es un único producto o una compañía, es un conjunto de productos y servicios que actúa como reemplazo de las instituciones centralizadas que van desde los bancos, seguros, bonos, mercados etc
Para que funcionen y se ejecuten de forma correcta las DeFi Dapps, necesitan tener valor monetario, ya sea en forma de garantía, de liquidez etc., bloqueados en los contratos inteligentes o *smart contracts* [19]. El valor total bloqueado en las DeFi Dapps se conoce normalmente como *Total Value Locked* [20]. El TVL al inicio de 2019 se encontraba alrededor de 290 millones de dólares, pero este 2021 ha llegado a alcanzar los 45 Billones de dólares [21], como se puede observar en la Ilustración 1. El elevado crecimiento del TVL sirve de indicador para visualizar el rápido crecimiento y potencial que tiene el ecosistema DeFi.

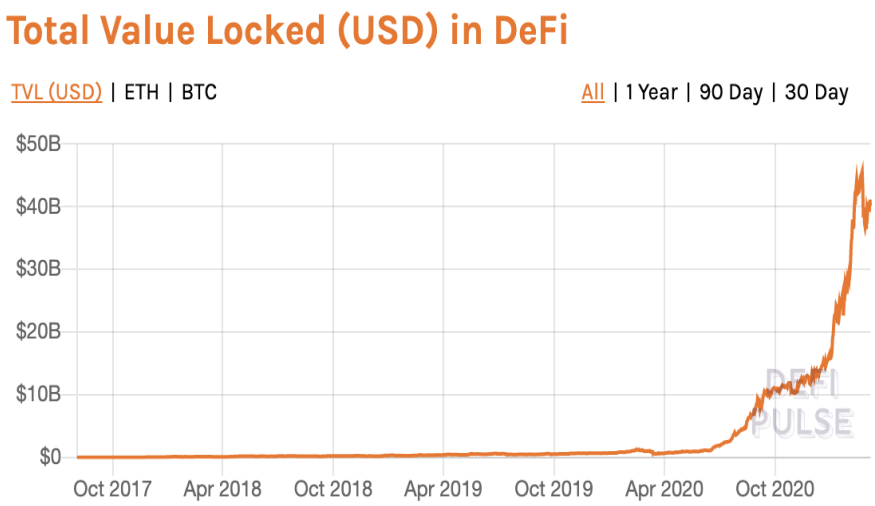

Ilustración 1. (2021). Valor total bloqueado en DeFi. Fuente: https://defipulse.com/

2.2.1 Ecosistema

Independiente de toda la información que se esté dando, es un sector de alto riesgo para invertir y se puede observar que las DeFi se sitúan en un estado en el que están en pleno desarrollo experimental, con muchos proyectos que están mejorando día a día. Es un sector que nació hace unos pocos años y las personas aún se sienten un poco reticentes a entrar en este mundo de nuevos y complejos conceptos. Pero, en la época en la que se encuentra la sociedad, la era de la información y de la tecnología, este sector noparará de evolucionar y seguramente dentro de unos años sea irreconocible respecto a cómo es hoy en día. Una conclusión de todo es que estas

aplicaciones descentralizadas han surgido para revolucionar el sistema financiero tradicional y los servicios que ofrecen estos, eliminando el uso de cualquier intermediario, porque con el uso correcto de la tecnología, la mayoría de los problemas actuales se pueden solucionar.

2.2.2 Descentralización

En este subsubapartado, se van a separar los grados de descentralización en varias categorías. Los componentes comunes entre todos los protocolos de préstamos DeFi incluyen custodia, precios, inicio de llamadas de margen, provisión de liquidez de llamadas de margen, determinación de la tasa de interés y desarrollo de protocolos. Con base en el número de estos componentes que están descentralizados, se asigna una categoría en el continuo de descentralización. Este sistema de categorización [22], aunque simple, es sorprendentemente poderoso para capturar el grado de control que los equipos detrás de los protocolos tienen sobre los activos retenidos.

1. **Centralizado:** Custodiado, usa tarifas centralizadas, tipos de interés que han sido determinados centralizadamente, proveedores de liquidez centralizados para las operaciones con margen...

2. **Grado 1 DeFi:** Estos productos DeFi son *non-custodial* [23], es decir, que están custodiados por ti, en tu billetera, sin la necesidad de que esté en el *exchange* o custodiado por un tercero. Los precios de las comisiones son centralizados, el margen del apalancamiento va a estar centralizado, la liquidez que provees estará centralizada, los tipos de interés serán determinados de forma centralizada, la gestión y desarrollo de la plataforma recae sobre un grupo de personas unidas entre sí, que conforman una entidad.

3. **Grado 2 DeFi:** Estos productos DeFi son *non-custodial* y además añaden un componente descentralizado adicional que puede estar entre los siguientes: los precios de las comisiones, los tipos de interés [24] o el desarrollo de la plataforma, pero todo lo demás permanecería centralizado.

4. **Grado 3 DeFi:** Estos productos DeFi son *non-custodial*, no necesitan permisos para realizar actividades de apalancamiento, proveer liquidez a la plataforma, pero los precios de las comisiones y los tipos de interés son consensuados de forma centralizada y la plataforma está dirigida de forma centralizada, tanto a nivel de desarrollo para las actualizaciones como para la gestión de la Dapp.

5. **Grado 4 DeFi:** Estos productos DeFi son *non-custodial*, no necesitan permisos para realizar actividades de apalancamiento, proveer liquidez a la plataforma y los precios de comisiones son descentralizados, no obstante, los tipos de interés son consensuados de forma centralizada al igual que la dirección de la plataforma, las actualizaciones y el desarrollo de estas mismas.

6. **Grado 5 DeFi:** Estos productos DeFi son *non-custodial*, no necesitan permisos para realizar actividades de apalancamiento, proveer liquidez a la plataforma y

los precios de comisiones son descentralizados, en este grado a estos se le suma, los tipos de interés, pero la gestión de la plataforma sigue recayendo en un grupo de personas, incluyendo las actualizaciones y el desarrollo de estas mismas.

7. **Grado 6 DeFi:** Todos los componentes de estos protocolos DeFi, incluyendo el desarrollo, son descentralizados. Realmente no existen proyectos en este grado de descentralización, pero poco a poco irán medrando para alcanzar esta descentralización, pero esto no solo depende de una entidad, depende de una gran comunidad de desarrolladores y personas que quieran construir un proyecto egregio.

Actualmente, la mayoría de las aplicaciones DeFi Dapps se sitúan en la categoría de Semi-descentralizadas. Se ha dicho que un sistema es tan descentralizado como su componente más central, y aunque hay algo de verdad en esto, la descentralización se irá expandiendo.

2.2.3 Stablecoins

Los precios de las criptomonedas son conocidos por su gran volatilidad. Es común que las criptomonedas tengan unas revalorizaciones o depreciaciones intradía de un 10-30%. Para mitigar esta volatilidad, fueron creadas las monedas estables [25] que están vinculadas a otros activos estables como el dólar, estas son USDT, USDC, DAI etc. Tether (USDT) fue una de las primeras stablecoins que se fundaron. Cada USDT en teoría debería estar respaldado por el emisor por valor de 1 dólar. Los usuarios deben confiar en que esto se cumple a la perfección, por eso es por lo que a veces existe una desconfianza.
Las monedas estables descentralizadas tienen como objetivo resolver este problema de confianza. Este tipo de monedas se crean normalmente a través de un método de sobregarantía, operan completamente en libros de contabilidad descentralizados, se rigen por organismos autónomos descentralizados y sus reservas pueden ser auditadas públicamente por cualquier persona.
Estas monedas no son aplicaciones descentralizadas como tal, pero son de vital importancia para hacer que las aplicaciones DeFi sean mucho más accesibles para todo el mundo y poder tener un depósito de valor estable [26].

2.2.4 Préstamos

Pedir préstamos a los bancos lleva consigo muchas restricciones [27], como tener una buena calificación crediticia y tener una garantía suficiente que te respalde, para que dé confianza a los bancos de que tiene suficiente valor en el caso de no poder pagar la deuda.
Los préstamos descentralizados disipan esta barrera, permitiendo a cualquiera utilizar como garantía sus activos digitales y usarlos para obtener préstamos, eso si, se deben de tener los activos suficientes para que puedan respaldar a lo que quiera pedir prestado. Por otra parte, un individuo puede obtener rentabilidad de sus activos participando en las *lending pools* [28]. Con esta descentralización no es necesario

tener una cuenta bancaria o una calificación crediticia que exprese que se es un buen sujeto al que dejar dinero. En la Ilustración 2 se puede observar la evolución del TVL en plataformas de préstamos o que los incluyen.

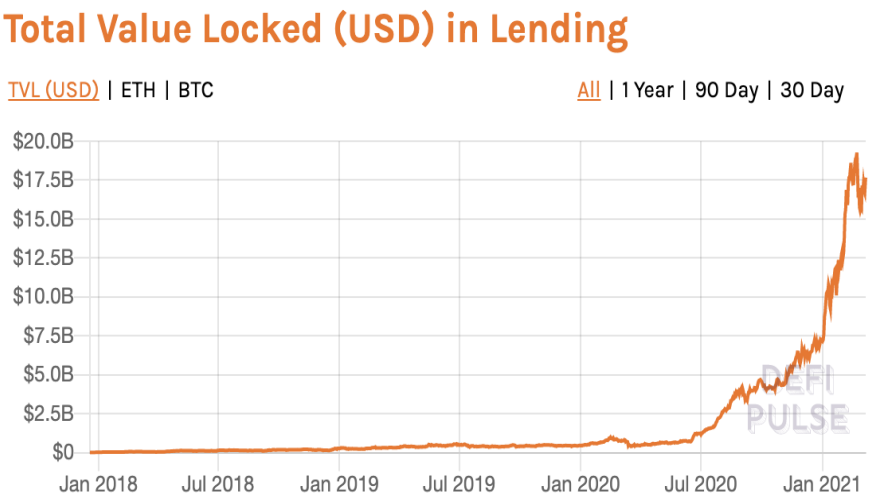

Ilustración 2. (2021). Valor total bloqueado en préstamos. Fuente: https://defipulse.com/

2.2.5 Exchanges

Exchanges [29] como Coinbase o Binance están centralizados, es decir, que el poder de una gran cantidad de funciones relacionadas con el mercado lo tienen las diferentes personas que componen estas empresas y son los que custodian los activos que van a ser intercambiados. Los usuarios de estos exchanges en verdad no tienen un control total, aunque existen diferentes hardwares que proporcionan una seguridad extra a sus activos, pero por el mero hecho de ponerlos en manos de los exchanges pueden ser hackeados perfectamente y no será la primera vez ni la última que suceda.
Los exchanges descentralizados tienen como objetivo resolver este problema permitiendo a los usuarios intercambiar criptomonedas sin renunciar a la custodia de sus monedas. La clave reside en que no es necesario almacenar fondos en los exchanges, los usuarios no necesitan confiar en los exchanges para ser solventes. En la Ilustración 3, se puede observar el crecimiento exponencial del dinero bloqueado para añadir liquidez en los exchanges descentralizados.

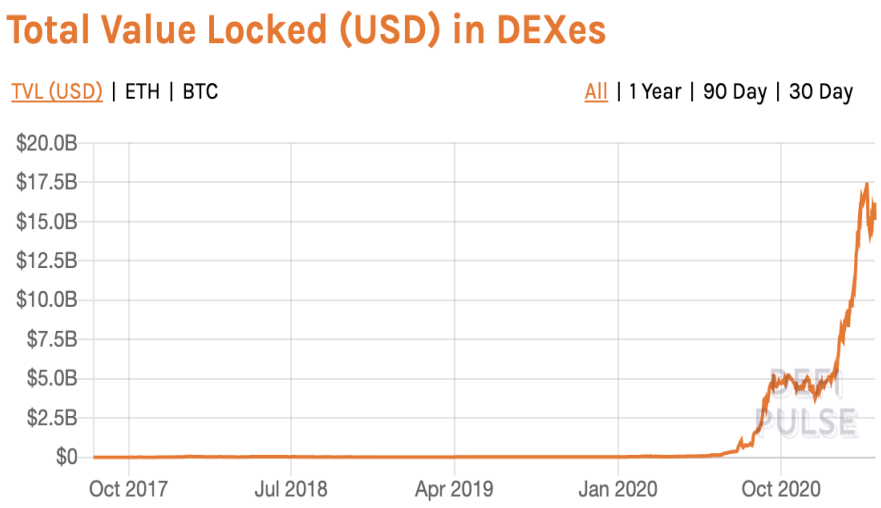

Ilustración 3. (2021). Valor total bloqueado en los DEXes. Fuente: https://defipulse.com/

2.2.6 Derivados

Los derivados financieros [30] son contratos cuyo valor es derivado de otro activo subyacente como las acciones, mercancías, divisas, índices, bonos o tipos de interés. Estos contratos son intercambiados normalmente en plataformas centralizadas, pero con la llegada de DeFi, estos se están empezando a intercambiar en exchanges derivados especializados en este tipo de productos financieros. En este tipo de productos es donde se produce el mayor volumen de intercambio diario. En la Ilustración 4, se puede analizar el aumento del valor total de los derivados financieros relacionados con las criptomonedas.

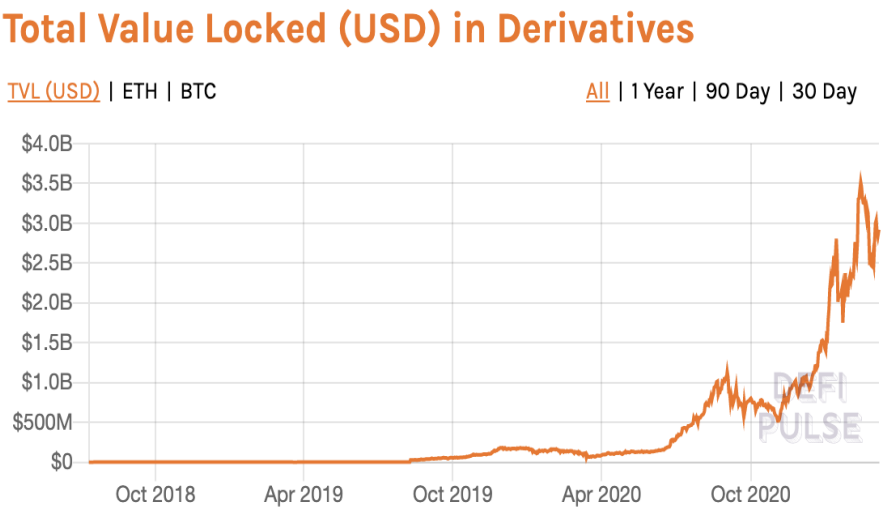

Ilustración 4. (2021). Valor total bloqueado en Derivados financieros. Fuente: https://defipulse.com/

3. Blockchain Ethereum

En este apartado se introducirá y explicará la red Ethereum, sus características y sus funciones, para que posteriormente se pueda entender porque las diferentes aplicaciones están implementadas en esta red y cómo funcionan gracias a las diferentes ventajas que ofrece Ethereum respecto a otras blockchains. Para entender el concepto de DeFi, primero se debe entender la red en la que están construidas, el porqué y qué se les permite hacer en ella.

3.1 Introducción

El concepto de Ethereum puede resultar para el oyente al principio un poco ambiguo, o quizás no. Esto es debido a que existen dos tipos de personas a las que se les puede describir la red Ethereum, una es la persona que ha escuchado hablar de Bitcoin y luego está el otro tipo de persona que no ha escuchado hablar sobre Bitcoin. Explicar Ethereum a la primera persona puede resultar un poco más sencillo, porque entiende lo que es y representa Bitcoin, una moneda digital *peer-to-peer*. Es decir, si se quisiera crear una moneda digital descentralizada se necesita algún tipo de base de datos para guardar cuánto dinero cada usuario posee. Este concepto se va a explicar con un simple ejemplo, si un usuario tiene 100 monedas digitales y se envía en primer lugar 100 monedas a un usuario y posteriormente se envía las mismas 100 monedas a otro usuario. Ambas transacciones son legales, pero si se combinan las dos se convierten en ilegales, porque se estaría convirtiendo 100 unidades de moneda digital en 200 y este es el clásico problema del *double-spending* [31].
Para resolverlo se necesita algún tipo de sistema que mantenga el rastreo de cómo estas monedas han sido gastadas, cuánto dinero tiene determinado usuario en un momento cualquiera y cuánto dinero tiene ese usuario permitido gastar en otro momento cualquiera. Esto se puede realizar fácilmente con un servidor centralizado, pero si se quiere implementar de algún modo para que el sistema sea descentralizado, fue y es un problema informático muy complejo de resolver. Una persona bajo el pseudónimo de Satoshi Nakamoto fue el primero en encontrar una solución a este problema, cuya solución fue realmente práctica en este contexto abierto y *permissionless,* esta solución fue llamada Bitcoin [32].

Ethereum viene de la idea de la denominada *cryptoeconomics* [33], es decir, de la combinación de algoritmos criptográficos como hashing, firmas digitales etc., y de incentivos económicos que mantienen a sistemas como Bitcoin en funcionamiento. Con esto se pretendía crear una red descentralizada con memoria, es decir, una base de datos descentralizada, para una gran variedad de diferentes aplicaciones con diferentes propósitos y funciones. Alrededor del año 2013, los programadores y usuarios implicados en la blockchain, se empezaron a dar cuenta de que la blockchain servía mucho más que para los pagos digitales peer-to-peer. Con esta ideología establecida, los usuarios empezaron a pensar que se podría implementar otro tipo de activos digitales, contratos inteligentes, acuerdos financieros, registros de identidad etc. Hay una gran cantidad de aplicaciones como para construir una blockchain para cada una de ellas, por lo tanto, la idea principal detrás de Ethereum es tener una blockchain que entienda un lenguaje de programación con un propósito general [35].

El ejemplo perfecto para este concepto es Android o iOS; en el móvil se tiene un sistema operativo como cualquiera de los mencionados anteriormente, en el interior de estos se pueden tener diferentes aplicaciones escritas en cualquier lenguaje de programación y cualquiera puede crear una aplicación o descargarla y ejecutarla. Este era el propósito general flexible que se pretendía llevar a Ethereum.

3.2 Ethereum

Ethereum es un concepto ambiguo. Ethereum no es solo dinero, también se puede utilizar como un emisor de activos, crowdfunding, registro de dominio, registro de títulos, juegos de apuestas, predicción de mercados, internet de las cosas y muchas más aplicaciones [35]. El problema es que, con el inicio de las criptomonedas, los protocolos eran creados para un producto o para un propósito. Bitcoin fue pensado para usarse como un método de pago digital, es decir, se creó para una aplicación concreta. En cambio, con Ethereum se pensó en hacer un protocolo en el que los usuarios pudieran construir las aplicaciones que quisiesen en él, es decir, que funcionara básicamente como un sistema operativo de propósito general.

Todos los nodos que componen Etherum procesan cada transacción y las guardan en su estado, como Bitcoin, al igual que utilizan el mismo mecanismo de consenso descentralizado, Proof of Work.
La red de Ethereum carga una tarifa (*gas fees*) por cada coste computacional que un contrato inteligente en ejecución realiza, pero cada bloque tiene un límite de tarifas de gas.
Cada transacción que se ejecuta en la red Ethereum contiene los siguientes campos [36]:

- **Nonce**
- **Gasprice** (Cantidad de Ether por unidad de gas)
- **Startgas** (Máximo de gas consumible)
- **To** (Dirección de destino)
- **Value** (Cantidad de Ether que quieras enviar)
- **Data** (Un array ilimitado que puedes rellenarlo con el contenido que desees)
- **V,r,s** (ECDSA, algoritmo de firma digital)

El nonce es muy interesante, se trata de un número que caracteriza a cada transacción, ya que cada una debe tener un incremento único, nonce. La primera transacción que envías desde una cuenta debe de tener un nonce de 0, la segunda de 1, la tercera de 2 etc. y la razón por la que esto se hace es para prevenir el *real replay attack*. Si Alice envía 10 Ether a Bob, tú no quieres que Bob coja esa transacción y la reinserte dentro de la blockchain 10 veces para enviarse a sí mismo 100 ether.

Una estructura de datos que se utiliza en Ethereum y generalmente en la blockchain son los Árboles Merkle [37]. Estos permiten pruebas verificables de que una transacción en particular se ha incluido en un bloque en particular. El principio general es que cada bloque tiene cientos de transacciones y si se quiere verificar que esa transacción en particular se ha incluido en ese bloque, no se tiene que descargar todo

el bloque. Lo único que se debe hacer es descargar una rama de este árbol, este árbol es del tipo árbol hash, donde cada nodo del árbol es el hash de los dos nodos que están situados debajo suya, por lo tanto, lo único hay que hacer es descargar esta parte específica del árbol que baja hasta nuestra transacción y se podrá verificar los hashes que van hasta arriba de la rama. Así, no se tienen que verificar todos los hashes, únicamente los que son relevantes para esa rama en particular y si todos esos hashes son correctos, sabes que la transacción que se buscaba está en ese árbol en particular y que se encuentra en ese bloque en particular.

3.3 Componentes de Ethereum

Ethereum tiene varios componentes que la hacen innovadora. El entendimiento de estas tres piezas esenciales empleadas en la red Ethereum es de vital importancia, debido a que juntas hacen que esta blockchain funcione correctamente y siga su propósito principal. El primer componente son los contratos inteligentes, por otra parte, está Ether y, por último, la Ethereum Virtual Machine.

3.3.1 Contratos inteligentes

Los contratos inteligentes o *smart contracts* [38] funcionan en base al principio “if this, then that”. Cuando una condición se cumple, el contrato llevará a cabo la operación programada.
Múltiples contratos inteligentes son combinados para que sean interoperables entre sí. Esto se utiliza en las conocidas Aplicaciones Descentralizadas, para que de esta forma sea capaz este contrato de realizar procesos computacionalmente más complejos.
Hay dos tipos diferentes de cuentas en Ethereum [39]: cuentas de propiedad externa (EOA) y cuentas de contrato. Los EOA son controlados por los usuarios, a menudo a través de un software como una aplicación de billetera que es externa a la plataforma Ethereum. Por el contrario, las cuentas de contrato están controladas por un código de programa (contratos inteligentes) que ejecuta la Ethereum Virtual Machine. En resumen, las EOA son cuentas simples sin ningún código asociado o almacenamiento de datos, mientras que las cuentas de contrato tienen código asociado y almacenamiento de datos. Las EOA están controladas por transacciones creadas y firmadas criptográficamente con una clave privada, mientras que las cuentas de contrato no tienen claves privadas y, por lo tanto, se "controlan a sí mismas" de la manera predeterminada prescrita por su código de contrato inteligente. El concepto de “Contratos inteligentes” se utiliza para referirse a programas informáticos inmutables que se ejecutan de forma determinista en el contexto de una máquina virtual Ethereum como parte del protocolo de red Ethereum, es decir, en la computadora mundial descentralizada de Ethereum.

Características [40]:

- **Programa:** Los contratos inteligentes son piezas de software. El término contrato no tiene un significado legal en este contexto.

- **Inmutable:** Una vez implementado, el código de un contrato inteligente no puede cambiar. A diferencia del software tradicional, la única forma de modificar un contrato inteligente es implementar una nueva instancia.
- **Determinista:** El resultado de la ejecución de un contrato inteligente es el mismo para todos los que lo ejecuten, dado el contexto de la transacción que inició su ejecución y el estado de la blockchain Ethereum en el momento de la ejecución.
- **Contexto EVM:** Los contratos inteligentes operan con un contexto de ejecución muy limitado. Pueden acceder a su propio estado, el contexto de la transacción que los llamó y cierta información sobre los bloques más recientes.
- **Descentralización:** El EVM se ejecuta como una instancia local en cada nodo de Ethereum, pero debido a que todas las instancias del EVM operan en el mismo estado inicial y producen el mismo estado final, el sistema en su conjunto opera como una única "computadora mundial".

Los contratos inteligentes suelen redactarse en un lenguaje de alto nivel, como Solidity [41]. Pero para que se ejecuten, deben compilarse en el “bytecode” de bajo nivel que se ejecuta en el EVM. Una vez compilados, se despliegan en la plataforma Ethereum mediante una transacción especial de creación de un contrato, que se identifica como tal al enviarse a la dirección especial de creación de contrato, llamada 0x0.
Cada contrato se identifica mediante una dirección de Ethereum, que se deriva de la transacción de creación del contrato en función de la cuenta de origen y el nonce. La dirección de Ethereum de un contrato se puede utilizar en una transacción como destinatario, enviando fondos al contrato o llamando a una de las funciones del contrato. Se debe tener en cuenta que, a diferencia de las EOA, no hay claves asociadas con una cuenta creada para un nuevo contrato inteligente. Como creador del contrato, no obtiene ningún privilegio especial a nivel de protocolo (aunque puede codificarlos explícitamente en el contrato inteligente). Ciertamente, no recibe la clave privada de la cuenta del contrato, que de hecho no existe; podemos decir que las cuentas de contrato inteligente son dueñas de sí mismas.
Es importante destacar, que los contratos sólo se ejecutan si son solicitados por una transacción. Todos los contratos inteligentes en Ethereum se ejecutan, en última instancia, debido a una transacción iniciada desde una EOA. Un contrato puede llamar a otro contrato que puede llamar a otro contrato, y así sucesivamente, pero el primer contrato en dicha cadena de ejecución siempre habrá sido llamado por una transacción de una EOA. Los contratos nunca se ejecutan "por sí mismos" o "en segundo plano". Los contratos permanecen inactivos hasta que una transacción desencadena la ejecución, ya sea directa o indirectamente como parte de una cadena de llamadas contractuales. También vale la pena señalar que los contratos inteligentes no se ejecutan "en paralelo" en ningún sentido; la computadora mundial Ethereum puede considerarse una máquina de un solo subproceso.
Las transacciones son atómicas, se cancelan o se revierten con éxito. Una terminación exitosa de una transacción significa diferentes cosas en diferentes escenarios [42]: (1) si una transacción se envía desde una EOA a otro EOA, entonces se registran los cambios en el estado global (por ejemplo, saldos de cuentas) realizados por la transacción; (2) si se envía una transacción desde una EOA a un contrato que no invoca ningún otro contrato, entonces se registra cualquier cambio en el estado global (por ejemplo, saldos de cuenta, variables de estado de los contratos) (3) si se envía

una transacción de un EOA a un contrato que sólo invoca otros contratos de una manera que propaga errores, luego se registra cualquier cambio en el estado global (por ejemplo, saldos de cuentas, variables de estado de los contratos); y (4) si una transacción se envía desde una EOA a un contrato que invoca otros contratos de una manera que no propaga errores, entonces sólo puede haber algunos cambios en el estado global registrado (por ejemplo, saldos de cuentas, variables de estado de contratos con errores), mientras que otros cambios en el estado global no se registran (por ejemplo, variables de estado de los contratos con errores). De lo contrario, si se revierte una transacción, todos sus efectos (cambios de estado) se “revierten” como si la transacción nunca se hubiera ejecutado. Una transacción fallida todavía se registra como si se hubiera intentado, y el Ether gastado en gas para la ejecución se deduce de la cuenta de origen, pero por lo demás no tiene otros efectos sobre el contrato o el estado de la cuenta.

Como se mencionó anteriormente, es importante recordar que el código de un contrato no se puede cambiar. Sin embargo, un contrato se puede "eliminar", eliminando el código y su estado interno (almacenamiento) de su dirección, dejando una cuenta en blanco. Cualquier transacción enviada a esa dirección de cuenta después de que se haya eliminado el contrato, no resulta en ninguna ejecución de código, porque ya no hay ningún código para ejecutar. Para eliminar un contrato, se ejecuta un código de operación EVM llamado SELFDESTRUCT (anteriormente llamado SUICIDE) [43]. Esa operación cuesta “gas negativo”, un reembolso de gas, incentivando así la liberación de recursos del cliente de la red de la eliminación del estado almacenado. Eliminar un contrato de esta manera no elimina el historial de transacciones (pasado) del contrato, ya que la blockchain en sí es inmutable. También es importante tener en cuenta, que la capacidad de SELFDESTRUCT sólo estará disponible si el autor del contrato programó el contrato inteligente para que tenga esa funcionalidad. Si el código del contrato no tiene un código de operación SELFDESTRUCT o es inaccesible, el contrato inteligente no se podría eliminar.

3.3.2 Ether

Ether es la moneda nativa (token) de la blockchain Ethereum [44]. Es decir, esa moneda es la que se utiliza dentro de la blockchain Ethereum. Ether es el carburante necesario para que la red Ethereum siga con su correcto funcionamiento. Ether, al fin y al cabo, es software programado en la red Ethereum y sirve como medio de pago, ya sea porque se quiere pagar a otra persona, porque se necesita pagar comisiones a la red, por utilizarla etc. El Ether se usa normalmente para pagar, como se ha comentado anteriormente, las comisiones por ejecutar las aplicaciones descentralizadas en Ethereum. Se puede pensar que ejecutar contratos inteligentes es como ir en coche, para que el coche funcione se necesita gasolina, para ejecutar un contrato se necesita usar Ether para pagar unas tarifas conocidas como *Gas Fees*.

3.3.3 Ethereum Virtual Machine (EVM)

La EVM [45] es una máquina virtual que ejecuta una forma especial de código llamado *EVM bytecode*, análogo a la CPU de su ordenador. Aquí se va a explicar cómo se escriben los contratos inteligentes para ejecutarse en el EVM.

Si bien, es posible programar contratos inteligentes directamente en bytecode, pero el bytecode de EVM es bastante difícil de manejar y muy difícil de leer y de comprender para los programadores. En cambio, la mayoría de los desarrolladores de Ethereum utilizan un lenguaje de alto nivel para escribir programas y un compilador para convertirlos en bytecode [46].
Cualquier lenguaje de alto nivel podría adaptarse para escribir contratos inteligentes, pero adaptar un lenguaje arbitrario para que sea compilable al código de bytes de EVM es un ejercicio que puede llevar a fallos y, en general, generaría cierta confusión. Los contratos inteligentes operan en un entorno de ejecución minimalista y altamente restringido (el EVM). Además, debe estar disponible un conjunto especial de funciones y variables del sistema específicas de EVM. Como tal, es más fácil construir un lenguaje de contratos inteligentes desde cero que hacer un lenguaje de propósito general adecuado para escribir contratos inteligentes. Como resultado, han surgido varios lenguajes de propósito especial para programar contratos inteligentes.
Ethereum tiene varios lenguajes de este tipo, junto con los compiladores necesarios para producir código de bytes ejecutable por EVM.

En general, los lenguajes de programación se pueden clasificar en dos amplios paradigmas de programación: declarativo e imperativo, también conocidos como funcionales y procedimentales, respectivamente [47]. En programación declarativa, escribimos funciones que expresan la lógica de un programa, pero no su flujo. La programación declarativa, se utiliza para crear programas donde no hay efectos secundarios, lo que significa que no hay cambios de estado fuera de una función. Los lenguajes de programación declarativos incluyen Haskell y SQL. La programación imperativa, por el contrario, es donde un programador escribe un conjunto de procedimientos que combinan la lógica y el flujo de un programa. Los lenguajes de programación imperativos incluyen C ++ y Java. Algunos lenguajes son "híbridos", lo que significa que fomentan la programación declarativa, pero también se pueden utilizar para expresar un paradigma de programación imperativo. Dichos híbridos incluyen Lisp, JavaScript y Python. En general, cualquier lenguaje imperativo puede usarse para escribir en un paradigma declarativo, pero a menudo resulta en un código poco elegante. En comparación, los lenguajes declarativos puros no se pueden utilizar para escribir en un paradigma imperativo. En los lenguajes puramente declarativos, no hay "variables".
Si bien la programación imperativa es más utilizada por los programadores, puede ser muy difícil escribir programas que se ejecuten exactamente como se espera. La capacidad de cualquier parte del programa para cambiar el estado de cualquier otra hace que sea difícil razonar sobre la ejecución de un programa e introduce muchas oportunidades para errores. La programación declarativa, en comparación, facilita la comprensión de cómo se comportará un programa: dado que no tiene efectos secundarios, cualquier parte de un programa puede entenderse de forma aislada.
En los contratos inteligentes, los errores literalmente cuestan dinero. Como resultado, es de vital importancia redactar contratos inteligentes sin efectos no deseados. Para hacer eso, se debe poder razonar claramente sobre el comportamiento esperado del

programa. Por lo tanto, los lenguajes declarativos juegan un papel mucho más importante en los contratos inteligentes que en el software de propósito general. Sin embargo, como verá, el lenguaje más utilizado para los contratos inteligentes (Solidity) [48] es imperativo.

3.4 Características de Ethereum

La red Ethereum posee ciertas particularidades que la hacen diferente a las demás. Estas características son propiedades que hay que tener en cuenta a la hora de usar esta blockchain, porque se refieren a las tarifas que hay que pagar por usarla y al tipo de aplicaciones que se pueden programar encima de Ethereum, debido a la versatilidad de esta red.

3.4.1 Tarifas de Gas

En Ethereum, se necesita pagar una tarifa para que las transacciones y los contratos se ejecuten correctamente [49]. Esta tarifa es llamada Gas. En términos técnicos, Gas [50] se refiere a la unidad de medida respecto al coste computacional requerido para ejecutar una operación o un contrato inteligente. Cuanto más compleja sea la ejecución de la operación, más gas es requerido para realizar esa operación. Las *Gas fees* son pagadas completamente en ETH.
El precio del gas puede fluctuar en el tiempo y depende de la demanda de la red Ethereum. Cuanta más personas hayan interactuado con la blockchain Ethereum, ya sea haciendo transacciones o ejecutando contratos, debido a los limitados recursos computacionales en la red, el precio del gas subirá. Inversamente, cuando la red no esté tan demandada el precio se verá reducido.
Las tarifas de gas pueden ser colocadas manualmente, porque en una situación de congestión en la red, debido a la alta demanda, las transacciones con las tarifas más altas serán más prioritarias para su validación.
Los precios del gas son normalmente denotados en *gwei* [51]. 1 gwei = 0.000000001 ether

Por ejemplo, si se asume que la ejecución de un contrato requiere la transferencia de 21.000 ud. de gas y que la media del precio del gas es de 3 gwei, entonces,
21.000 gas x 3 gwei = 63.000 gwei = 0.000063 ETH.

3.4.2 Dapps

Una de las características principales de Ethereum, es el tipo de aplicaciones que se implementan gracias a ella, las Dapps, ya que Ethereum ofrece la posibilidad de usar su blockchain para programar aplicaciones sobre ella, dando lugar a numerosos tipos de aplicaciones.
Las Dapps [52] son interfaces que interactúan con la blockchain a través del uso de smart contracts. A simple vista, las Dapps se ven y se comportan como una web o una aplicación móvil, pero ellas están interactuando con la blockchain de diferentes formas. Entre esas diferentes variantes, está utilizar ETH para usar la Dapp, para el

almacenamiento de los datos del usuario dentro de la blockchain y así de esta forma serán inmutables; entre otras.
Las Dapps, están construidas encima de blockchains descentralizadas como ethereum y normalmente tienen los siguientes beneficios:

- **Inmutabilidad:** Nadie puede cambiar la información una vez está en la blockchain.
- **Tamper-proof:** Los contratos inteligentes publicados sobre la blockchain no pueden ser manipulados sin alertar a otro participante de la blockchain.
- **Transparencia:** Los contratos que conforman las Dapps son auditables para el público.
- **Disponibilidad:** Mientras la red Ethereum esté activa, las Dapps construidas en la red, van a mantenerse activas.

Pero las Dapps tienen también desventajas:

- **Inmutabilidad:** Los contratos inteligentes están escritos por humanos y pueden ser tan buenos como el humano que los haya escrito. Los errores humanos son inevitables e inmutables en los contratos inteligentes y tienen el potencial de tener errores compuestos y desembocar en un problema mayor.
- **Transparencia:** Los contratos auditables pueden ser también puntos de ataques de hackers con el fin de encontrar vulnerabilidades e información.
- **Escalabilidad:** Es el problema fundamental de la red Ethereum y el de muchas blockchains, debido a que las Dapps están limitadas respecto a la limitación que tiene la red en la que se ejecutan.

Las Dapps de Ethereum y de muchas más blockchains, normalmente se ajustan al concepto de DAO o intentan serlo, debido a que es una de las características que se busca al construir proyectos basados en la blockchain. DAO [53] es una Organización Autónoma Descentralizada la cual no está gobernada por una única persona/entidad, sino que está controlada a través de código programado. Este código está basado en contratos inteligentes y permite a las DAOs remplazar cómo están constituidas y gobernadas las organizaciones tradicionales. Como se ejecuta por medio de código, estará protegido ante la intervención humana y operará de forma transparente. No se verá afectada por la influencia que pueda haber de forma externa y las decisiones de gobernanza serán realizadas a través del voto por DAO token.

3.5 Caso práctico Ethereum

En este subapartado, se van a aplicar los conocimientos explicados anteriormente. Para ello, se va a usar Etherscan, que es un explorador de bloques, que permite a los usuarios ver la información sobre transacciones que se han enviado a la blockchain, verificar el código del contrato y visualizar los datos de la red. A continuación, se van a presentar los cuatro casos básicos de transacción, la transferencia entre dos usuarios, la transferencia para desplegar un contrato, la transferencia de tokens ERC20 y, por último, la transferencia entre un usuario y una cuenta de contrato. Con esto se pretende observar cómo funciona la red Ethereum por dentro y cómo se ejecutan los

diferentes tipos de transacciones, al mismo tiempo que familiarizarse con los términos y con el formato en el que se muestra la información de los diferentes contratos o transacciones.

Los componentes de una transacción en Etherscan:

- **Transaction Hash:** Un identificador único que puede ser usado para localizar una transacción específica.
- **Status:** El estado actual de la transacción (Success, Failed o Pending).
- **Block:** El número del bloque en el que la transacción fue incluida.
- **Timestamp:** La hora en la que el bloque fue minado en el formato UTC.
- **From:** La cuenta de origen que envía la transacción.
- **To:** La cuenta a la que la transacción va dirigida.
- **Value:** La cantidad de Ether incluida en la transacción.
- **Transaction Fee:** La cantidad de Ether pagados al minero por procesar la transacción.
- **Gas Limit:** El límite máximo de la cantidad de trabajo computacional y almacenamiento que el remitente está dispuesto a gastar en la transacción.
- **Gas Used by Transaction:** La cantidad de trabajo computacional y almacenamiento que se ha usado en la transacción.
- **Gas Price:** La cantidad de Ether a pagar por unidad de gas.
- **Nonce:** El recuento de transacciones enviadas fuera de la cuenta.
- **Input Data:** Información que se transmite a un contrato inteligente cuando se envía una transacción a su dirección. Sin embargo, si la transacción está creando un contrato, el código de bytes del contrato se coloca en el campo de datos de entrada.

Presentación del programa a utilizar

El programa que se va a usar para este caso práctico y que va a ser usado en otros apartados se llama Etherscan. La url del programa es la siguiente: https://etherscan.io/

La ilustración 5 muestra la página principal de la aplicación Etherscan, donde se puede observar las diferentes funciones de las diversas partes que contiene la página. En la zona de arriba (Home, Blockchain, Tokens, Resources, More) se utiliza cuando deseamos realizar una consulta mas específica sobre un proyecto determinado, sobre un token en concreto, etc.

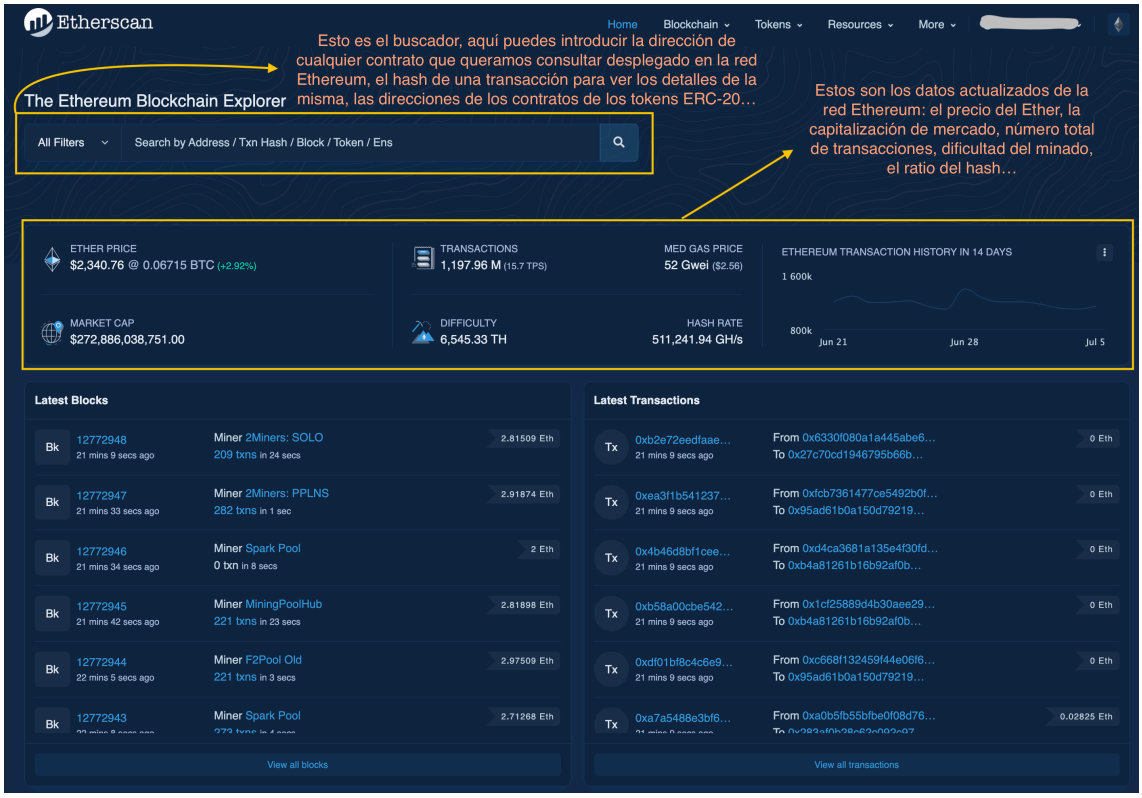

Ilustración 5. (2021). Explicación página principal de Etherscan.

Transferencia de Ether entre dos EOA

Una vez presentada la página web, se procede a insertar el hash de una transacción escogida al azar. A continuación, se puede observar que es una transacción entre dos cuentas de usuarios, en cuya transacción se está enviando un monto específico de Ether de un usuario a otro. Esto se sabe porque el Input Data está vacío, el To address no está etiquetado como una dirección de contrato y porque el Value está completado.

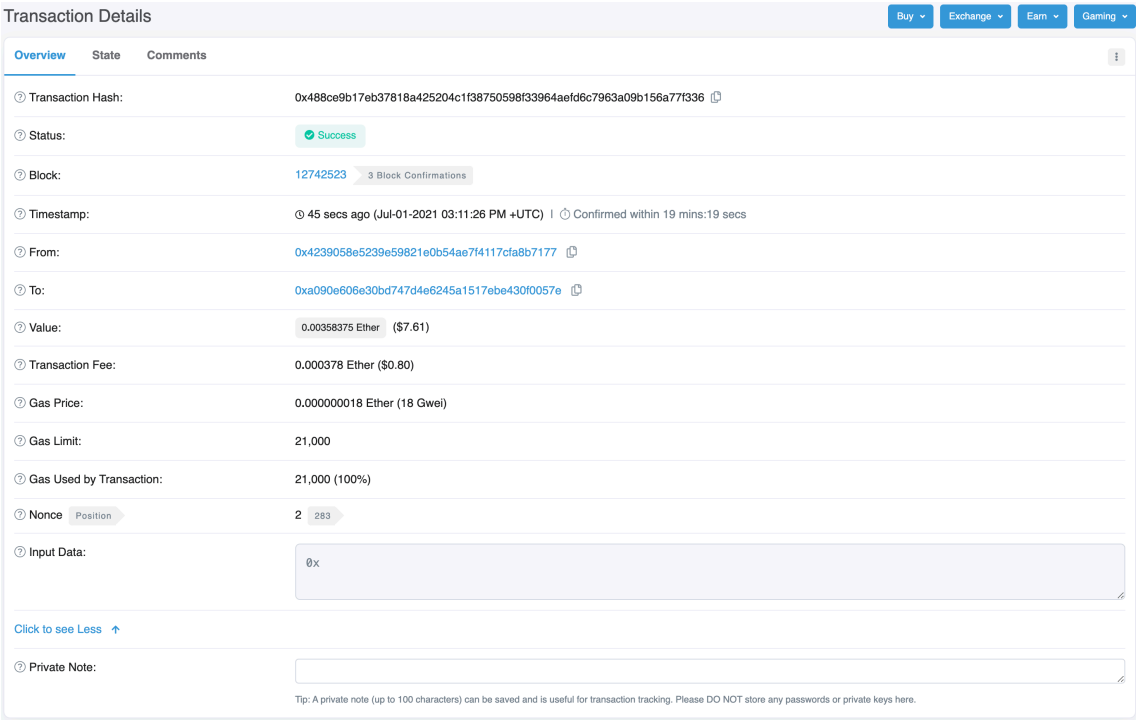

Ilustración 6. (2021). Detalles de la transacción. Fuente: https://etherscan.io/tx/0x488ce9b17eb37818a425204c1f38750598f33964aefd6c7963a09b156a77f336

Cuando se mueve Ether, se le está diciendo a la red Ethereum que disminuya el balance de la cuenta de usuario “A” e incremente el balance de la cuenta de usuario de “B”. Si la transacción es válida, el estado global de Ethereum se actualiza. En términos de gas, una transferencia estándar de Ether de una EOA a otra EOA cuesta 21,000 gas, que podemos ver que es la cantidad utilizada.

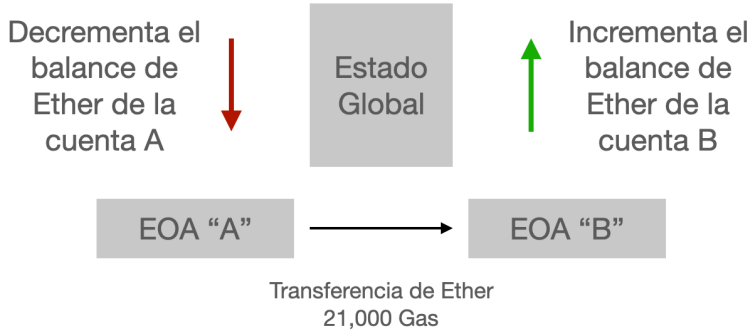

Ilustración 7. (2021). Ejemplo ilustrativo de la transacción de Ether entre dos EOA

Transferencia de los Tokens ERC20

Una de las mayores diferencias entre la transferencia de tokens ERC20 y la transferencia de Ether, es que la transacción de ERC20 está dirigida a la dirección del contrato del token, en vez de a la cuenta a la que se enviaría el Ether. En la transacción aleatoria que se presenta a continuación, el campo del Input Data incluye la función a la que se ha llamado (en este caso es la función “transfer”). Además, los inputs de la función, que incluye la dirección del destinatario junto con la cantidad de tokens que queremos enviar en formato hexadecimal. Etherscan califica la cuenta “To” como la dirección del contrato Tether y añade un campo llamado “Tokens Transferred” para mostrar los datos de entrada en un formato más legible para las personas que quieran consultar los datos de la transacción.

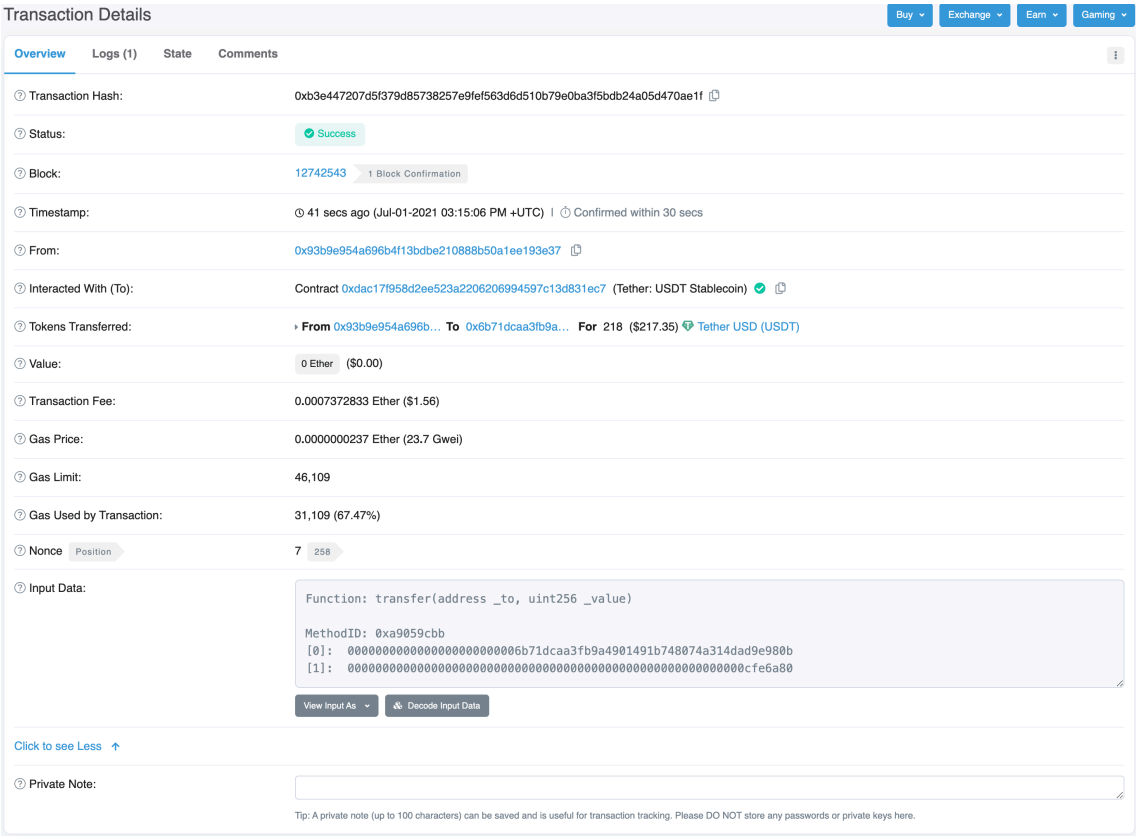

Ilustración 8. (2021). Detalles de una transacción de tokens ERC20. Fuente: https://etherscan.io/tx/0xb3e447207d5f379d85738257e9fef563d6d510b79e0ba3f5bdb24a05d470ae1f

Normalmente, el campo de “Value” se encuentra vacío, debido a que únicamente se necesita actualizar los saldos del contrato. Por último, los saldos del contrato pueden variar dependiendo de cómo ha sido implementado el contrato.

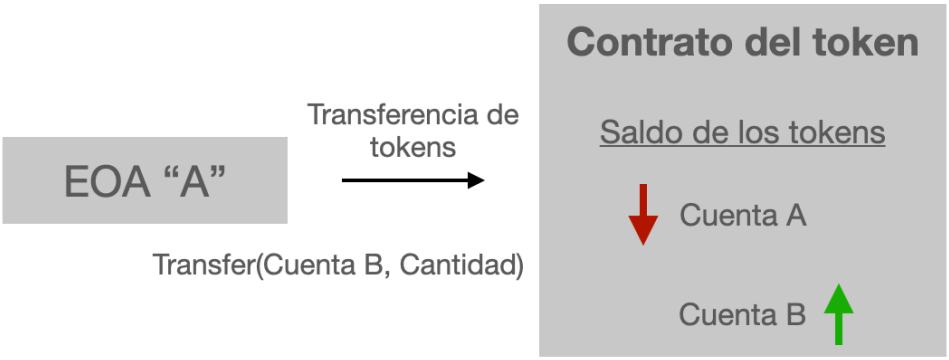

Ilustración 9. (2021). Ejemplo ilustrativo de la transacción de tokens ERC20

Una cuenta EOA creando un Contrato

A continuación, se muestra la transacción que ha creado un contrato. La diferencia más notable para las transacciones de creación de contratos es que los datos de entrada contienen el bytecode de la lógica del contrato. Podemos ver que la dirección del contrato se muestra en el campo “To” con "Created" junto a él.

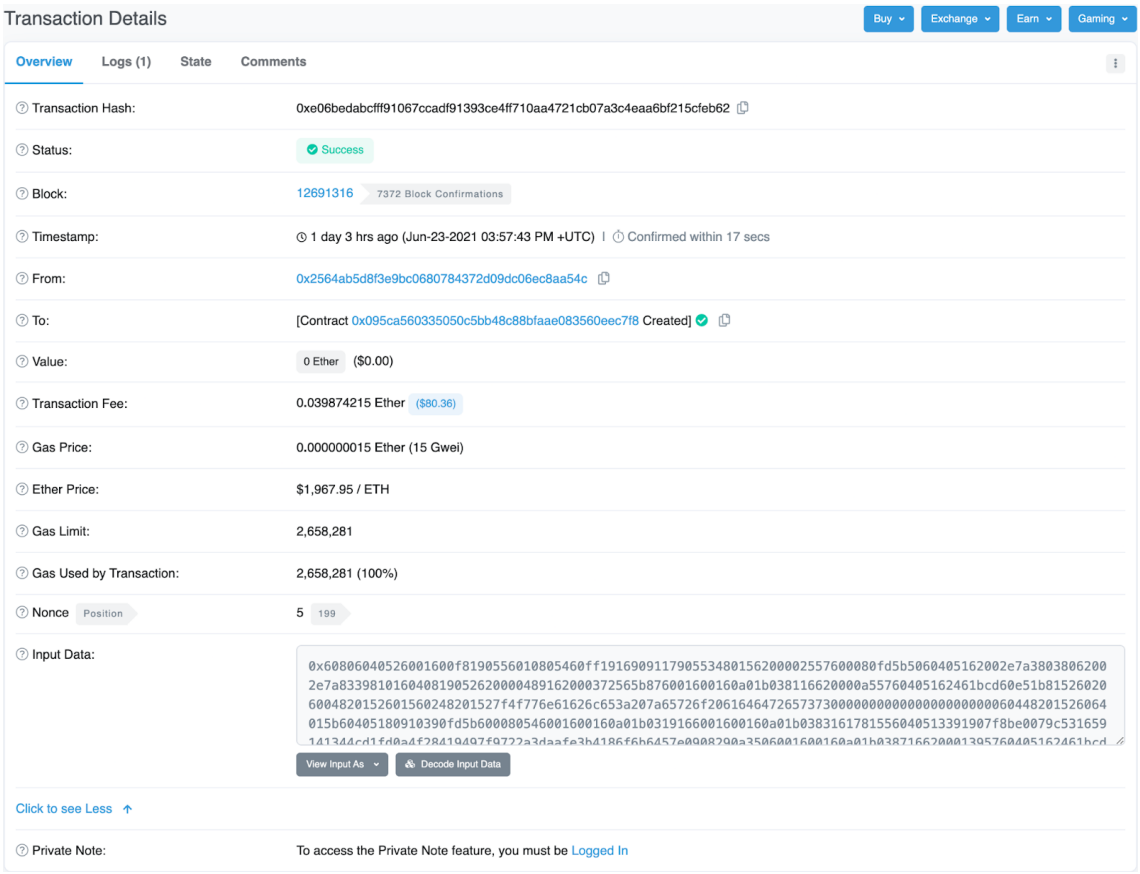

Ilustración 10. (2021). Detalles de una transacción de una cuenta EOA creando un contrato. Fuente: https://etherscan.io/tx/0xe06bedabcfff91067ccadf91393ce4ff710aa4721cb07a3c4eaa6bf215cfeb62

Para realizar esto, el contrato se debe compilar y generar el bytecode que represente el contrato. Después de esto, así es como se vería la transacción para desplegar el contrato inteligente.

```
> web3.fromWei(eth.getBalance(eth.accounts[0]))
100
> var bytecode =
    "0x6080604052600160f81905560108054460ff191690911790553480156200002557600080fd5b5060405162002e7a38038062002e7a8339810
    160408190526200004891620003725650b876001600160a01b038116620000a55760405162461bcd60e51b8152602060048201526015602482015
    27f4f776e61626c653a207a65726f206164647265737300000000000000000000000060448201526064015b60405180910390fd5b6000805460016
    00160a01b0319166001600160a01b038316178155604051339190 7f8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b645
    7e0908290a3506001600160a01b038716620001395760405162461bcd"
undefined
>
> eth.sendTransaction({
..... from: eth.accounts[0],
..... data: bytecode,
..... gas: 2658281
.....})
"0xe06bedabcfff91067ccadf91393ce4ff710aa4721cb07a3c4eaa6bf215cfeb62"
```

Ilustración 11. (2021). Visualización del envío de la transacción a través de la red Ethereum.

Como de normal, se ve que se devuelve el hash de la transacción. Con este hash, se puede examinar los detalles de la transacción usando eth.getTransaction() y eth.getTransactionReceipt().

Transferir Ether desde una EOA a una Cuenta de Contrato

Después de implementar un contrato, una EOA puede ejecutar las funciones definidas en este contrato. Nuevamente, se implementa enviando una transacción Ethereum.

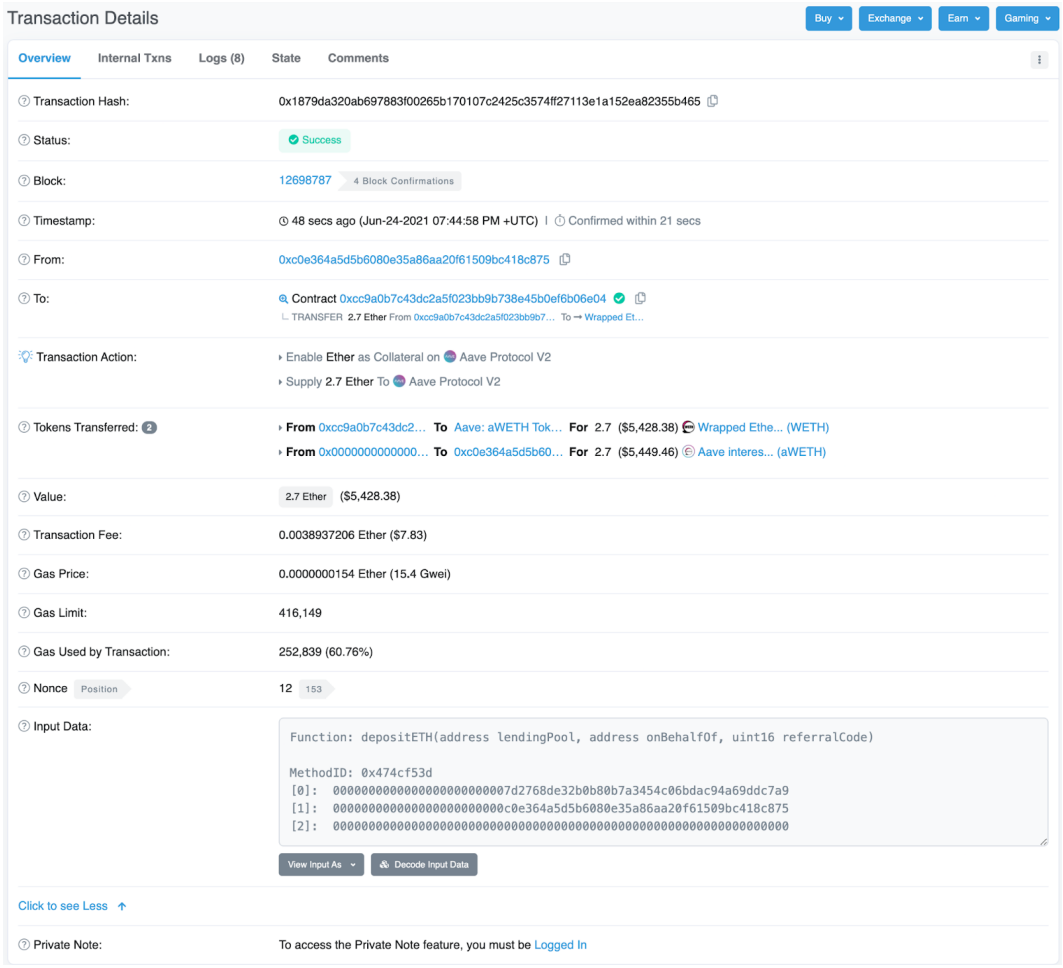

Ilustración 12. (2021). Detalles de una transacción desde una EOA a una cuenta de contrato. Fuente: https://etherscan.io/tx/0x1879da320ab697883f00265b170107c2425c3574ff27113e1a152ea82355b465

Al ver la transacción presentada anteriormente, se puede ver que alguien hizo un depósito de Ether en la billetera del contrato aWETH de Aave, que requirió 252,839 gas. Esto se debe a que la billetera del contrato también emite un evento al recibir Ether, lo que eleva el costo del gas a más de 21,000.

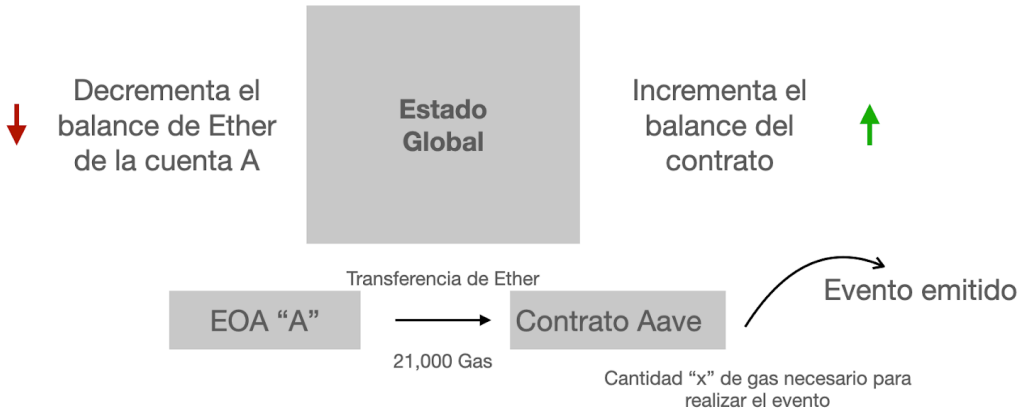

Ilustración 13. (2021). Ejemplo ilustrativo de la transacción de tokens desde una EOA a una cuenta de contrato.

Es por eso, por lo que es importante saber a qué tipo de cuenta se está enviando antes de asumir que el costo del gas será de 21,000 gas o, de lo contrario, la transacción podría quedarse sin gas. Además, puede haber efectos secundarios dañinos al enviar una transacción a un contrato con el que no está familiarizado, porque los contratos pueden reenviar mensajes a otros contratos. Lo que significa, que llamar a una función o simplemente depositar Ether en un contrato malicioso, podría ejecutar código que podría producir un resultado negativo.

Se debe asegurar siempre, que el contrato al que se está a punto de enviar una transacción es fiable y establecer un límite de gas razonable.

4. Stablecoins descentralizadas (Protocolo Maker)

En este apartado, se va a tratar el concepto de monedas estables y el rol de vital importancia que poseen en el sistema actual. Para ello, se ha escogido como ejemplo el Protocolo Maker, una de las primeras plataformas en ofrecer una moneda estable en el mercado, respaldada por criptoactivos. Se explicará cómo a partir de contratos inteligentes ha sido posible crear una plataforma de estas dimensiones; piezas de código que han creado una comunidad que valorada en millones de dólares en transacciones diariamente.

4.1 Introducción

El precio de las criptomonedas es extremadamente volátil, para mitigar esta volatilidad, las stablecoins están vinculadas a otros activos estables como el dólar estadounidense. Desde entonces, las monedas estables o *stablecoins* han evolucionado rápidamente para ser un componente fuerte de DeFi, convirtiéndose en una parte fundamental para este ecosistema modular.
Hay diferentes stablecoins listadas hoy en día, el top 5 son [54]:

1. Tether (USDT): 40.000M $ (Market Cap.)
2. USD Coin (USDC): 10.000M $ (Market Cap.)
3. Binance USD (BUSD): 4.000M $ (Market Cap.)
4. Dai (DAI): 3.000M $ (Market Cap.)
5. TerraUSD (UST): 1.600M $ (Market Cap.)

Este apartado, se va a centrar en las monedas que están vinculadas al dólar estadounidense, porque no todas las stablecoins son iguales, debido a que cada una utiliza mecanismos diferentes para mantenerse vinculada al dólar. Hay tres tipos de vinculación, el primero es el conocido como *fiat-collateralized*, el segundo es el *crypto-collateralized* y el último son las conocidas como *algorithmic stablecoins*. Las stablecoins mas importantes utilizan el sistema *fiat-collateralized* para mantenerse vinculadas al dólar.

3 tipos de stablecoin [56]

- **IOU:** La organización IOU le propone al usuario que deposite su confianza en el sistema centralizado tradicional; si se le ofrece un activo con valor de 1$, lo guardaran mediante un custodio centralizado y a cambio ofrecen un token con el mismo valor. Si se necesita de vuelta el activo que se ofreció en primera instancia, se debe devolver el token que la organización centralizada intercambió por el activo. El usuario confía explícitamente en que el custodio cuidará de sus activos.

- **Estabilidad basada en algoritmos [57]:** Con esta solución estable basada en algoritmos, el usuario deberá depositar su confianza en la implementación y ejecución de estos algoritmos. Explicado de forma muy resumida, ya que no es nuestro foco de atención en este trabajo, funcionan respecto al precio del

token, es decir, si el precio del token es muy alto, aumentarán la oferta y reducirán la demanda. Si el precio del activo es bajo, aumentarán la demanda y reducirán la oferta. El usuario explícitamente confía en lo que hace este mecanismo desplegado por la organización, que responderá de manera oportuna y apropiada para mantener el sistema y, por definición, su token estable.

- ***Collateralized*:** Las organizaciones con garantías piden al usuario poner su confianza en el valor creado por el blockchain. Si el usuario cree que la economía de la blockchain prosperará, también lo harán los tokens de la blockchain. Luego, esos tokens se utilizan para garantizar el suministro de monedas estables en esta economía. Independientemente de la dinámica de gobierno utilizada para la estabilidad, los usuarios depositan su confianza ante todo en la garantía prometida antes que en cualquier otra cosa.

La principal diferencia entre estas soluciones reside en donde depositan la confianza los usuarios y por ende el mecanismo de estabilidad de la stablecoin.
Para simplificarlo, se va a estudiar la stablecoin DAI, debido a que es la moneda descentralizada con más relevancia. USDT y USDC, son monedas centralizadas, pero se va a comentar cómo se mantienen vinculadas de formas diferentes al dólar.

Tether (USDT) [57], se mantiene vinculada a 1$ manteniendo reservas de 1$ por cada token Tether generado. Las reservas de Tether, se mantienen guardadas en instituciones financieras y los usuarios tendrán que confiar en Tether respecto a que tengan todos los dólares que afirman que tienen por cada token Tether "proporcionado". Tether es por lo tanto, una stablecoin centralizada por medio del sistema fiat-collateralized.

La moneda USDC [58] fue emitida por el Centre Consortium, impulsada por el exchange de criptomonedas Coinbase y Circle Internet Financial. USDC es la única moneda estable actualmente admitida por Coinbase. Está construido sobre la blockchain Ethereum como un token ERC-20. Se vincula al dólar de la misma forma que lo hace USDT. El USDC está vinculado 1:1 a dólares estadounidenses (USD) reales y se mantiene en cuentas bancarias de reserva. Está sujeto a auditorías periódicas para garantizar que se mantenga en un dólar real. Así es cómo se puede confiar en que el valor de USDC seguirá siendo de 1$ independientemente de lo que suceda.

Dai (DAI) [59] por otra parte, está garantizada (*collateral*) a través del uso de criptomonedas como Ethereum. Su valor está vinculado a 1$ a través de protocolos votados por una organización autónoma descentralizada y contratos inteligentes. En cualquier momento, la garantía para generar DAI puede ser validada fácilmente por los usuarios. DAI, es una stablecoin descentralizada mediante el sistema de crypto-collateralized.
DAI, es una stablecoin usada normalmente en el ecosistema DeFi, es la preferida para operaciones en los sistemas DeFi, préstamos etc. Para entender DAI y entrar en mayor profundidad respecto al tema, a continuación, se va a introducir su plataforma, MakerDAO, que es la responsable del funcionamiento de esta criptomoneda.

4.2 El Protocolo Maker

Maker [60] es una plataforma de contratos inteligentes que se ejecuta en la blockchain de Ethereum y tiene dos tokens: la stablecoin Dai (vinculada a 1$), y luego su token de gobernanza, Maker (MKR).
Dai fue lanzada en noviembre de 2019 y es conocida como una moneda que puede ser emitida a raíz de utilizar como garantía diferentes criptomonedas como Ether (ETH) y Basic Attention Token (BAT), entre otras.
Maker (MKR) [61], es el token de gobernanza de la plataforma MakerDAO y puede usarse para votar mejoras en la plataforma a través de Maker Improvement Proposals (MIP). Maker es un tipo de organización conocida como Organización Autónoma Descentralizada (DAO).
El protocolo Maker es una de las dapp más grandes de la blockchain de Ethereum. Este protocolo observaba problema y ciertas necesidades en el sector de las criptomonedas, el cual era que la moneda descentralizada más utilizada era el Bitcoin y la moneda más utilizada en el mundo es el dólar. ¿Es el dólar igual de estable que el Bitcoin? La respuesta es no. Por esta razón, Maker quiso hacer una moneda descentralizada y que fuera el equivalente a 1$.
El Protocolo Maker es gestionado por personas de todo el mundo que tienen su token de gobernanza, MKR. Mediante un sistema de gobernanza científica, que incluye encuestas de gobernanza y votaciones ejecutivas, los tenedores de MKR gestionan el Protocolo y los riesgos financieros de Dai, para garantizar su estabilidad, transparencia y eficiencia [62]. Un token MKR bloqueado en un contrato de votación equivale a un voto.

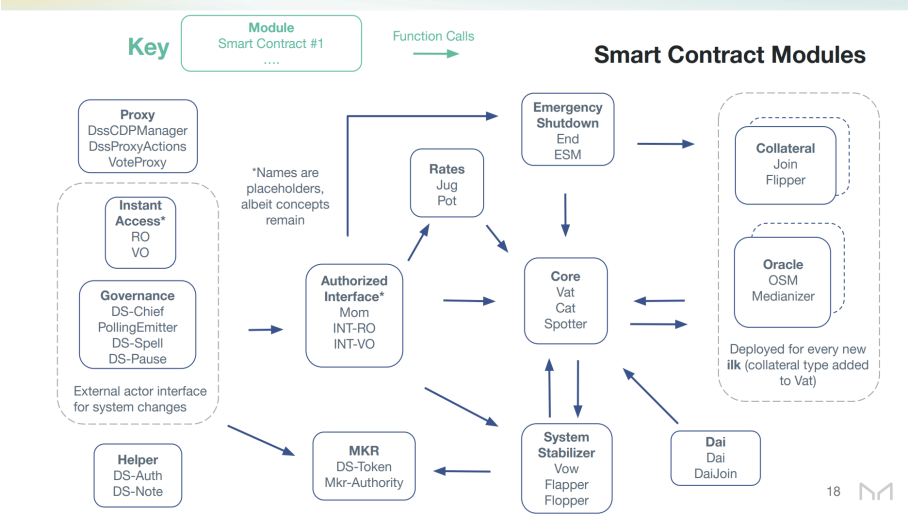

Ilustración 14. (2021). The Maker Protocol Smart Contract Modules System. Fuente: https://docs.makerdao.com/

El protocolo Maker interactúa tanto internamente como con los usuarios a través de contratos inteligentes. La Ilustración 14, es un esquema que explica de qué forma está

organizado internamente el protocolo Maker y de qué forma están relacionados los módulos de contratos inteligentes. Los contratos inteligentes están organizados en módulos, con funciones y objetivos diferentes entre ellos y en conjunto representan el funcionamiento de la stablecoin DAI y de MakerDAO.
A continuación, se explicarán algunos de los diferentes módulos de contratos inteligentes y sus objetivos [63] para tener una idea general de cuáles son sus funcionalidades internas:

Core Module

Este módulo contiene el estado del Protocolo Maker y sus mecanismos centrales a la hora de realizar operaciones cotidianas.

Componentes:

Vat: Esta parte contiene las primitivas fundamentales del Protocolo Maker:

- Base de datos - Parámetros de riesgo como Dai, garantías y balance de deudas
- Sistema de contabilidad - Operaciones básicas de contabilidad para mantener actualizada la base de datos
- Gestión de los Vaults - Ajuste de la garantía y de la deuda (Creación de Dai)
- Fungibilidad de los Vaults - Transferencia, dividir y fusionar Vaults

El Vat no tiene dependencias externas, alberga la interfaz pública para la gestión de Vaults, que permite a los usuarios hacer ajustes en sus balances. También contiene una interfaz pública para la fungibilidad de los Vaults. Excluyendo estas interfaces, el Vat es accesible únicamente a través de módulos de *trusted smart contracts.*

Cat: Es la interfaz pública para confiscar los Vaults que no son seguros y tramitar su garantía incautada mediante las subastas.
Si el valor del activo subyacente cae por debajo de la cantidad requerida, la relación de garantía (valor en USD del activo / valor en USD Deuda Dai) disminuye. Para incrementar este ratio y prevenir la insolvencia del sistema, el generador toma (a través de Cat) la garantía y la vende por Dai en una subasta (Flipper).

Spotter: Permite a los actores externos actualizar el precio en los Vat de los diferentes tipos de garantías.
El Spotter, es simplemente un contrato de interfaz en el que los actores externos obtienen el precio de mercado actual de los *Oracle module* para el tipo de garantía especificado. El Vat lee el precio de mercado del spotter.

Collateral Module

Este módulo es desplegado para cada tipo de garantía nueva que se añada al Vat. Contiene todos los adaptadores y contratos de subasta para cada tipo de garantía.

Componentes:

Join: El adaptador Join, se usa para depositar/retirar garantías desbloqueadas dentro del Vat. Para mantener la seguridad del sistema, solo los trusted smart contracts pueden añadir/borrar valor hacia / desde el Vat. Un adaptador Join es un trusted smart contract que se usa para depositar garantías desbloqueadas dentro del Vat. La ubicación de la garantía depositada/bloqueada en los Vaults se encuentra en el adaptador Join.

Flipper: Este apartado es básicamente la casa de subastas de la garantía. Cada subasta está relacionada con un Vault previo.

Dai Module

El Dai Module contiene la representación del token dai y sus adaptadores.

Componentes:

Dai: Contiene la base de datos de los dueños de los tokens Dai, la lógica de transferencia, aprobación y el suministro.
Dai es una extensión del DS-Token, un contrato dentro de DappSys, una biblioteca segura, simple y flexible para sistemas de contratos inteligentes.
DSToken es una implementación que admite el estándar ERC20, pero con algunas adiciones que complementan el diseño del Protocolo Maker:

- Adición de funciones de genera y quema (con la autorización adecuada) -> para controlar el suministro de tokens
- "push", "pull" y "move" alias para operaciones de transferFrom -> mejora la legibilidad
- Aprobación de asignación binaria -> menor gas y mayor seguridad

DaiJoin: DaiJoin es un adaptador donde se crean todos los tokens Dai. El propietario del Vault interactúa con DaiJoin para generar los tokens Dai que se les asignaron en el depósito, así como para quemar los tokens Dai + las tarifas acumuladas contra su Vault. Es decir, DaiJoin es un *trusted smart contract* que se utiliza para depositar Dai en el Vat. Toda emisión y quema de tokens Dai ocurre en DaiJoin.

System Stabilizer Module

Cuando el valor de una garantía que respalda a Dai se desploma por debajo del nivel de liquidación, la estabilidad del sistema está en riesgo. Este módulo se encarga de proporcionar esa estabilidad al sistema incentivando a los Keepers por ello.

Componentes:

Vow: El Vow representa el balance del Protocolo Maker, como receptor tanto del superávit del sistema como de la deuda del sistema. Su función es cubrir los déficits mediante subastas de deuda y liquidar los excedentes mediante subastas de excedentes. Cuando los Vaults son escogidos por el Cat, su deuda es asumida por Vow como Sin, la unidad de deuda del sistema, y se coloca en la cola de Sin. Si este Sin no es cubierto por una subasta dentro de un tiempo de espera, el Sin evoluciona y ahora se considera una deuda para el Vow.

Flopper: Es la casa de subasta de las deudas del sistema. Después de la realización de la subasta, el Flopper envía el Dai recibido al Vow para cancelar la deuda. El Flopper genera tokens MKR para el mejor postor.

Flapper: Es la casa de subastas del superávit. Después de que termine la subasta, el Flapper quema los tokens MKR del mejor postor y envía los Dai internos al respectivo postor.

Oracle Module

El valor de la garantía en el Vault se deriva de su precio global en USD del mercado libre. Para ello se implementa un módulo de Oracle para cada tipo de garantía y proporciona datos de precios para un tipo de garantía correspondiente al Vat. Las direcciones incluidas en la lista blanca transmiten actualizaciones de precios fuera de la cadena, que se introducen en un *Medianizer* antes de ingresar al OSM. El Spotter lee del OSM.

Componentes:

Medianizer: Para un tipo de garantía específico, retorna la mediana del valor de varios precios que le ha enviado la Omnia Relayer Network.

OSM: Los usuarios autorizados pueden establecer un valor después de un período de tiempo (por ejemplo, una hora). Para proteger el sistema de un atacante que obtiene el control de la mayoría de los oráculos, OSM impone una demora de 1 hora en las fuentes de precios, lo que deja suficiente tiempo para que la comunidad de gobierno de MKR analice los datos y reaccione.

Governance Module

Este módulo contiene los contratos que facilitan los votos MKR, proposiciones de ejecución y seguridad del voto del Protocolo Maker.

Componentes:

DS-Chief: Un contrato de votación básico que otorga acceso root del Protocolo Maker a un “Chief” elegido (dirección). A través de la votación de aprobación, los votantes bloquean su MKR y votan con un peso relativo a la oferta pendiente de MKR. Los

Spells (propuestas) son un tipo de objeto de propuesta y se envían a DS-Chief como propuestas ejecutivas, que pueden realizar cambios en el protocolo (ajustar parámetros de riesgo, actualizar adaptadores, agregar nuevos tipos de garantías, etc.) Cualquiera puede crear un hechizo, y los poseedores de MKR pueden votar por paquetes de Spells, llamados Slates. En cualquier momento, el Spell con la mayor aprobación es el "Chief" elegido, tiene acceso y puede configurar el Protocolo Maker a través de Mom, el contrato de interfaz de administrador para Maker Governance.

PollingEmitter: Es un tipo de contrato con menos peso que el anterior, que se usa para los votos en los *Maker Governance polls*. Tanto las polls, como los votos de estas son hechos emitidos; cualquiera puede crear una encuesta (poll) y emitir votos. Los votos se cuentan fuera de la blockchain mediante la lectura de la cantidad de MKR que posee la dirección en DS-Chief, que se encuentra directamente en la dirección, así como cualquier cantidad que se encuentre en el poder de voto asociado con la dirección del votante.

De esta forma, es cómo funciona una DAO, mediante diferentes contratos inteligentes que interactúan entre ellos, con diferentes funcionalidades, son capaces con la ayuda de los usuarios de llevar el control de una aplicación. Es increíble ver cómo se ha alcanzado el nivel de escribir piezas de código inmutables para llevar el orden total en una organización y que prospere de la forma en la que lo ha hecho MakerDAO. Al fin y al cabo, esto se podría resumir como contratos inteligentes dentro de contratos inteligentes que interactúan con otros contratos inteligentes y así sucesivamente. Con esta explicación se espera que se pueda ver el potencial que este tipo de aplicaciones tiene y cómo pueden encajar en el mundo actual.

4.3 Componentes del Protocolo Maker

Para entender el Protocolo Maker, es necesario explicar las partes con mayor relevancia dentro de él. En este subapartado, se introducirán los diferentes componentes que constituyen todo el sistema MakerDAO. Hay más componentes que son altamente relevantes, pero se han escogido los que se piensa que pueden ayudar a comprender el sistema como un conjunto que trabaja de forma síncrona.

4.3.1 Dai

Dai [64], se ha convertido en una piedra angular para aplicaciones descentralizadas que ayudan a expandir el movimiento DeFi (descentralización financiera).
La stablecoin Dai, es una criptomoneda descentralizada, imparcial y respaldada por la garantía cuyo valor está vinculado al dólar estadounidense. Dai es guardado en billeteras que están respaldadas por la blockchain Ethereum y otras blockchains más. Todos los Dai que están circulados han sido emitidos mediante los Maker Vaults, que están respaldados por un superávit de activos que sirven como garantía.
Los usuarios pueden emitir Dai depositando criptoactivos en los Maker Vaults, que están dentro del Protocolo Maker. Depositar garantías dentro de los Maker Vaults permite emitir Dai y que entre en circulación por el mercado.

Todos los Dai que están en circulación en el mercado, están respaldados por un exceso de garantía, es decir, que el valor de la garantía es mayor que la deuda emitida en Dai, además todas las transacciones son publicadas y visibles en la red Ethereum.

Propiedades [66]:

- **Cobertura:** Durante períodos de alta volatilidad, Dai ofrece una forma de guardar el valor de tus activos sin tener que salirse del ecosistema de las criptomonedas.
- **Especulación:** Es más difícil rastrear los beneficios y pérdidas cuando intercambias activos debido a que uno aumenta de valor, pero el otro también puede aumentar, por ejemplo, el par BTC/ETH. Crear pares en los que esté involucrado DAI reduce el riesgo de los mercados.
- **Productos Financieros:** DAI puede ser usado como garantía para varios tipos de instrumentos financieros y también puede ser aceptado como pago de deuda.
- **Comercio:** Las transacciones de Dai son ejecutadas en minutos e independientemente de la situación de las dos partes involucradas. Es una muy buena solución para el comercio, transacciones internacionales y remesas.
- **Predicción de Mercados:** La compra de un activo siempre lleva intrínseco a él una volatilidad y un valor futuro que no se puede predecir, con la criptomoneda DAI se puede estimar que su valor se mantendrá estable y puede funcionar como reserva.
- **Pagos:** El uso de las criptomonedas día a día en la actividad económica, puede escalar correctamente si se posee un activo estable como medio de intercambio. DAI encaja en esta necesidad a la perfección.

A parte de todas estas propiedades, se puede guardar como medio de ahorro y ganancia de intereses mediante una función del Protocolo Maker llamada Tasa de Interés de Dai (DSR) [66].

4.3.2 Maker Vaults

Todos los activos colaterales aceptados, pueden aprovecharse para generar Dai en el Protocolo Maker mediante contratos inteligentes denominados Maker Vaults [67]. Los usuarios pueden acceder al Protocolo Maker y crear Vaults mediante varias interfaces de usuario distintas.
En los Vaults es necesario que haya un superávit de garantía y que el dueño del Vault se mantenga por encima del mínimo del Ratio de Liquidación para evitar que su garantía se vea liquidada por pérdida de valor. Adicionalmente, el Techo de Deuda es impuesto por el Protocolo Maker para cada tipo de Vault [68].
La cantidad máxima de Dai que puede ser generada para el intercambio para un tipo de garantía, se conoce como el Techo de Deuda. Este número no es absoluto y tiene que ver con el total de la oferta disponible de ese tipo de garantía. El Techo de Deuda [69] ayuda a mitigar el riesgo de crear un mercado con ausencia de liquidez.
Liquidación es el proceso de vender la garantía para cubrir la cantidad de DAI generada en el Vault y que ha sido prestada como deuda. La liquidación ayuda a asegurar que el DAI siempre esté respaldado por una cantidad de garantía que se

puede cubrir vendiendo la garantía cuando esta llegue al mínimo de Ratio de Garantía para ese tipo de garantía.
Los Keepers [70], se crearon para ser incentivados por mantener que ese superávit de garantía exista siempre y que el valor de un Vault no esté al descubierto.
Durante el proceso de Liquidación que se verá como se realiza posteriormente, se vende la garantía necesaria para cubrir la deuda y la Penalización por Liquidación, así si hay una garantía restante que no ha sido necesaria vender, estará disponible para el dueño del Vault para que pueda ser retirada en caso de necesidad [71].

- Ratio de Liquidación = (Cantidad de Garantía × Precio de la Garantía) ÷ Dai Generado × 100

- Precio de Liquidación = (Dai Generado × Ratio de Liquidación) / Cantidad de Garantía

La Penalización por Liquidación [72] es una tarifa que se paga por los dueños de los Vaults cuando su garantía alcanza el Precio de Liquidación. La Penalización por Liquidación se añade a la deuda que el dueño del Vault ya tenía, que resulta en más garantía vendida en la subasta. Estas penalizaciones previenen los ataques a las subastas, que permite a un atacante encontrar una vulnerabilidad en la subasta del Protocolo Maker y realizar unas ganancias a su favor.
Cabe destacar, que cada activo colateral depositado requiere su propio Vault. Por este motivo, algunos usuarios son propietarios de varios Vaults con diferentes tipos de garantías y diferentes niveles de colateralización.

4.3.3 Tasa de Interés de Dai

El Dai Savings Rate (DSR) [73], es una tasa variable que es obtenida al bloquear Dai en el contrato inteligente DSR.
Su propósito es permitir a la gobernanza Maker influenciar en la oferta y demanda de Dai mediante los cambios en la política monetaria de la organización.
Los poseedores de Dai, pueden ganar intereses automáticamente al bloquear sus Dai en el DSR.
Con esta fórmula, podremos saber qué rentabilidad podríamos esperar:

A = P (1 + r) ^ t
A = valor final de tu depósito
P = cantidad de depósito inicial
r = tasa de interés anual (decimal)
t = el número de años en el que ese depósito va a permanecer en el DSR

El DSR es un parámetro global que se puede subir o bajar para influir en la demanda de Dai. Aumentar el DSR incentiva a los usuarios a tener más Dai, lo que lleva a una mayor demanda de Dai, mientras que reducir el DSR tiene el efecto contrario de reducir la demanda de Dai. Esto se refleja en el precio de mercado de Dai, si Dai se cotiza por debajo de un dólar, entonces el DSR puede aumentarse para aumentar la demanda de Dai, lo que aumentaría el precio de Dai. Por el contrario, si Dai cotiza por

encima de un dólar, entonces el DSR puede reducirse para reducir la demanda de tenencia de Dai, lo que puede ayudar a reducir el precio de Dai.

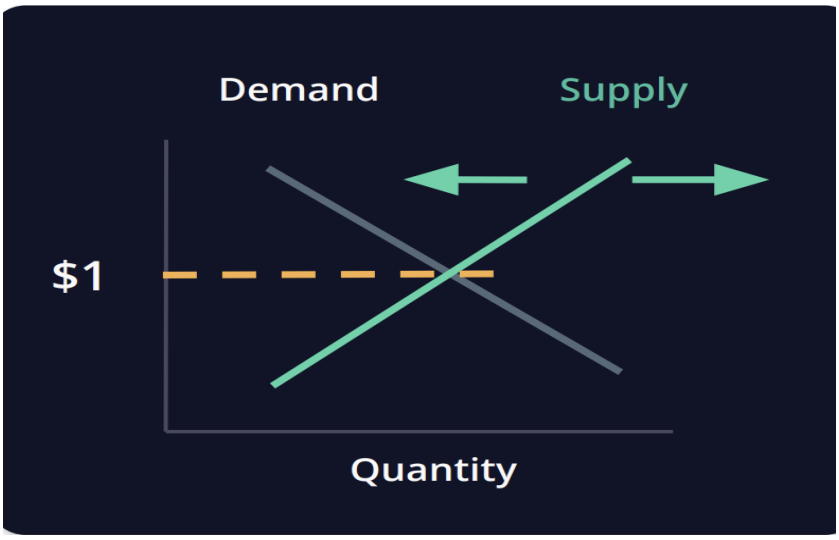

Ilustración 15. Curva de oferta y demanda. Fuente: https://docs.makerdao.com/

En la Ilustración 15, se observa de forma intuitiva cómo la oferta y la demanda influyen en el precio del activo y como manipulando cualquiera de las dos variables se puede conseguir alcanzar el precio objetivo. El sistema fue creado para que los usuarios del protocolo usaran estas técnicas para asegurarse de que el precio permaneciera lo más próximo a 1$.

4.4 Características del Protocolo Maker

Cada protocolo presente en la red Ethereum, presenta unas características diferentes, que hace al protocolo único. Aquí, se expondrán las diferentes cualidades que tiene este protocolo y cómo están implementadas, para entender qué hace este protocolo con mayor profundidad, cómo se organiza por dentro y cómo la unión de estas características hace que este protocolo esté sobreviviendo a los cambios constantes que se producen en el espacio de la blockchain.

4.4.1 Gobernanza del protocolo Maker

El token MKR permite a los titulares votar sobre los cambios y actualizaciones en el Protocolo Maker [74]. Es importante destacar que cualquier persona, no solo los tenedores de MKR, pueden presentar propuestas para una votación con MKR.
Es probable que las modificaciones aprobadas por los votantes para las variables de gobernanza del Protocolo no entren en vigor de inmediato, sino que podrían demorarse hasta 24 horas si los votantes optan por activar el Módulo de Seguridad de Gobernanza (GSM) [75]. La demora les daría a los tenedores de MKR la oportunidad de accionar un apagado y así proteger el sistema, de ser necesario, contra una propuesta de gobernanza malintencionada (como, por ejemplo, ante una propuesta

que altere los parámetros sobre colaterales en contra de las políticas monetarias establecidas o que permita desactivar los mecanismos de seguridad).
El objetivo de la gobernanza es, proteger la integridad y estabilidad del sistema Maker mediante el uso de una gestión y procesos efectivos. La finalidad de la gobernanza es lograr ese objetivo mediante la construcción de una comunidad de gestión de riesgos científica, descentralizada y abierta.
En la práctica, el proceso de la Gobernanza de Maker, incluye encuestas de propuestas y votación ejecutiva. La encuesta de propuestas se lleva a cabo para establecer un consenso aproximado en cuanto a la opinión de la comunidad antes de que se emita un voto ejecutivo. Esto, ayuda a garantizar que las decisiones de gobernanza se consideren de forma exhaustiva y se tomen por consenso antes del propio proceso de votación.
A nivel técnico, los contratos inteligentes gestionan cada tipo de voto. Un contrato de propuesta es un contrato inteligente con una o más acciones de gobernanza válidas programadas. Solo se puede ejecutar una vez. Cuando se lleva a cabo, aplica inmediatamente los cambios a las variables internas de gobernanza del Protocolo Maker. Después de la ejecución, el contrato de propuesta no puede volver a utilizarse. Toda dirección de Ethereum puede hacer uso de contratos de propuestas válidos. Los tenedores de tokens de MKR, pueden entonces emitir votos de aprobación de la propuesta que desean elegir como propuesta activa. La dirección de Ethereum que tenga el mayor número de votos de aprobación se elige como propuesta activa. La propuesta activa, tiene acceso administrativo a las variables de gobernanza interna del Protocolo Maker para luego modificarlas [76].

Responsabilidades de los tenedores de MKR [77]:

- Techo de deuda
- Tarifa de estabilidad
- Relación de liquidación
- Sanción de liquidación
- Duración de la subasta de colaterales
- Duración de la oferta en la subasta
- Oferta mínima en subasta

Y mitigar [78]:

- Un ataque malicioso a la infraestructura del contrato inteligente por parte de un actor malintencionado
- Un evento de cisne negro
- Errores imprevistos de precios e irracionalidad del mercado
- Abandono de los usuarios por soluciones menos complicadas

El rol de los titulares del token MKR [79]

Esta sección describe el rol de los titulares del token MKR y su influencia en el gobierno del Protocolo Maker. Los titulares de los MKR son responsables de la gobernanza del sistema, estableciendo el estado de la organización y defendiendo frente a propuestas que no persiguen los objetivos del protocolo. La gobernanza

describe cómo se controla una organización y quién es responsable ante las partes interesadas de esa organización.

Los titulares de los tokens deben ser activos en el sistema, debido a que son los encargados de realizar las propuestas de cualquier cambio en el sistema. Las propuestas son introducidas a la comunidad, discutidas, puestas en encuestas y llevadas a votación si fuera necesario.
Los titulares de los tokens eventualmente gestionaran la función de riesgo del sistema mediante la votación.
El mecanismo de gobernanza tiene dos tipos de propuestas:

- **Propuestas proactivas**, que incluyen debate, resolución y una implementación automatizada
- **Propuestas reactivas**, que incluyen una intervención en el sistema.

Un ejemplo de gobernanza proactiva es, el proceso de aceptar un nuevo token como garantía y desplegar los parámetros de riesgo asociados con él. Un ejemplo de gobernanza reactiva es, aumentar o disminuir la exposición a una forma de garantía debido a aumentos o disminuciones en la liquidez.

4.4.2 Mecanismo de estabilidad de precios

Por último, se va a explicar lo cinco niveles de mecanismos de estabilidad presentes en MakerDAO [80]:

Superávit de garantía

Ratio de garantía: La cantidad de Dai que puede ser generado es dependiente del ratio de garantía.
ETH ratio de garantía = 150%
BAT ratio de garantía = 150%
Básicamente, esto quiere decir que con un ratio de garantía de 150% es que para generar 100$ de Dai, se tiene que depositar un mínimo de 150$ en ETH o en BAT.

Liquidaciones Automáticas de los CDP [81]

Esto es que, si el valor de el colateral baja más que de un umbral mínimo, la liquidación automática se pone en marcha. En el proceso de liquidación, al valor de la deuda se le suma la tarifa por estabilidad y la penalización por liquidación. Esto quiere decir que se tendrá los Dai que se hayan pedido prestados y los Ether después de restarle el valor de la tarifa de estabilidad y la tarifa por liquidación. La tarifa por estabilidad es como la tasa de interés que se le paga al banco y será cargada al balance a la hora de pagar la deuda. La penalización por liquidación se realiza para castigar a los usuarios por no llevar una buena gestión de su deuda y de su garantía y, de esta forma, ayudar al sistema a prevenir emitir Dai a usuarios con una insuficiencia de garantía.

El control de la oferta mediante incentivos

El arbitraje, tiene un gran papel a la hora de mantener el valor de un activo en el precio en el que en teoría debería estar y esto se consigue con dos mecanismos:

1. Confianza. Todo valor de un activo se basa en la confianza de los usuarios en que ese activo, debe tener ese valor. Por lo tanto, si la mayoría de los usuarios creen que el Dai debe tener un valor de 1$, va a tener el valor de 1$.
2. Grandes órdenes de compras y ventas por encima y por debajo de 1$ realizadas por una larga organización o por personas que quieren tener beneficios por la fluctuación del precio. Por ejemplo, debería haber una gran cantidad de órdenes de venta a precios de 1.01$ y grandes órdenes de compra a precios de 0.99$. El hecho de que la gente pueda ver esas compras y ventas en los exchanges, hace que aumente la confianza de los usuarios en su relación con el valor de 1$.

Esto es "descentralizado y autónomo" en el sentido de que muchas personas diferentes realizan estos pedidos debido a su propia confianza en la vinculación y el incentivo resultante.
La mayoría de los sistemas autónomos y descentralizados se basan en incentivos humanos.

Ajuste de la tarifa de estabilidad [82]

El segundo componente, de este mecanismo de control de la oferta, es el ajuste de una tarifa de estabilidad. Los titulares de MKR pueden ajustar la tarifa de estabilidad en función del precio dinámico de DAI.
Un aumento en la tarifa de estabilidad da, como resultado, un mayor costo de endeudamiento para los usuarios de CDP, lo que frena el suministro de DAI al hacer que el uso de CDP sea menos atractivo. Por el contrario, una disminución en la tarifa de estabilidad (costo de los préstamos) incentivará la creación adicional de DAI, actuando como una herramienta de política para ajustar el crecimiento de la oferta.

Dilución de los tokens MKR [83]

MKR, el token de gobernanza de MakerDAO, se utiliza en algunas ocasiones para el impago de deudas del sistema. Los dueños de este token, son incentivados por llevar a cabo la estabilización del precio de Dai. Cuando una liquidación automática falla, el sistema se ve resentido por un periodo de tiempo hasta que se soluciona esa deuda, mediante la emisión y la venta de tokens MKR en el mercado y así poder repagar la deuda que estaba abierta. En esta ocasión, con la emisión de tokens MKR, su valor puede verse afectado debido al aumento de la oferta, por eso se incentiva a los usuarios por llevar al sistema por el camino óptimo.

Emergency Shutdown

De este apartado ya hemos hablado anteriormente, pero se puede clarificar este aspecto con lo que sucedió en marzo del 2020. En períodos de alta volatilidad se

puede producir lo que se conoce como el “Black Swan Event” o Cisne negro, que es un evento impredecible y extremo que puede causar graves consecuencias. En el caso de ETH y BAT, en marzo del 2020 con la caída de la bolsa, el precio de ETH y BAT se desplomaron más de un 50% causando una oleada de liquidaciones y un apagón de emergencia. Es un proceso que se utiliza como último recurso para resolver la plataforma Maker apagando el sistema. El proceso se utiliza para asegurarse de que los titulares de los titulares de Dai y los usuarios que bloquearon su dinero, reciban el valor neto de los activos a los que tienen derecho.

4.5 Caso práctico en MakerDAO

Esta vez, en este apartado práctico, se va a mostrar como están registrados todos los contratos de MakerDao en la red Ethereum y cómo encontrarlos, usando la herramienta Etherscan que se explicó en el caso práctico anterior. Con todo esto, se pretende enseñar cómo están desplegados todos los contratos que forman el sistema Maker, cómo interactúan entre ellos y que código tiene escrito cada contrato. Por otra parte, se va a mostrar cómo es la plataforma Maker y cómo realizar las principales acciones en esta.

Para encontrar los contratos registrados en MakerDAO, se han de mirar los proyectos Defi más importantes, en este caso, se selecciona Maker, como se muestra en la Ilustración 17. La ilustración 16, muestra la página principal de Etherscan, después de hacer clic en el recuadro señalado (More) y posteriormente seleccionar DeFi Leaderboard, donde se mostrarán las plataformas o contratos más usados en el ámbito DeFi. La ilustración 17 muestra la página que se despliega al seleccionar el apartado DeFi Leaderboard.

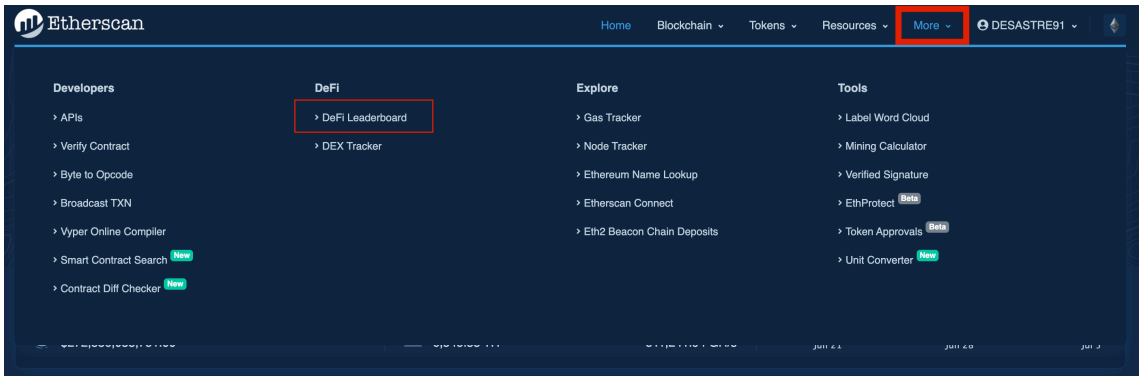

Ilustración 16. (2021). Cómo encontrar el DeFi LeaderBoard.

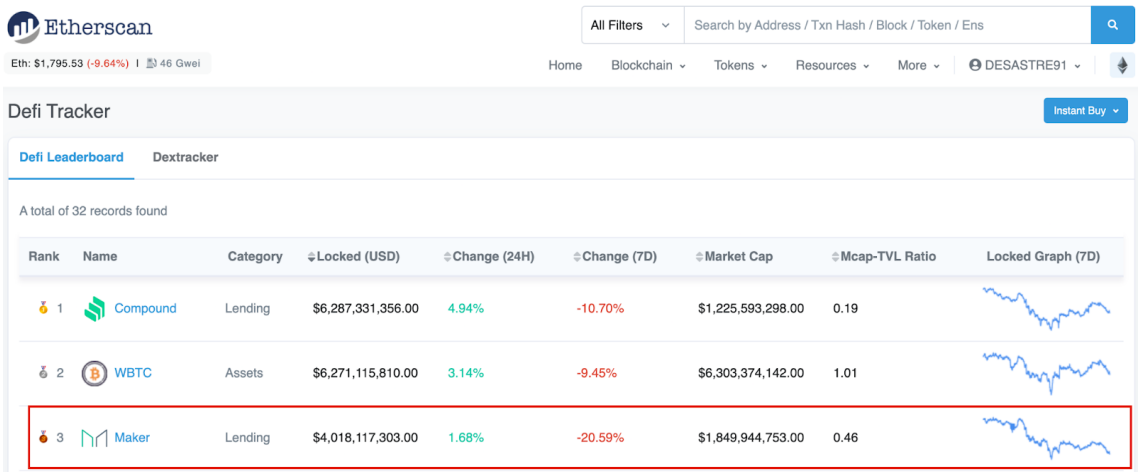

Ilustración 17. (2021). Defi Tracker. Fuente: https://etherscan.io/defi#defi-leaderboard

Después de seleccionarlo, se desplegará una página como la que se va a mostrar a continuación, Ilustración 17. Esta contiene todos los contratos relacionados con este proyecto, es decir, todos los contratos que conforman el sistema Maker, entre ellos se puede observar el de la stablecoin Dai, el del Token Maker, el del CDP Manager etc.

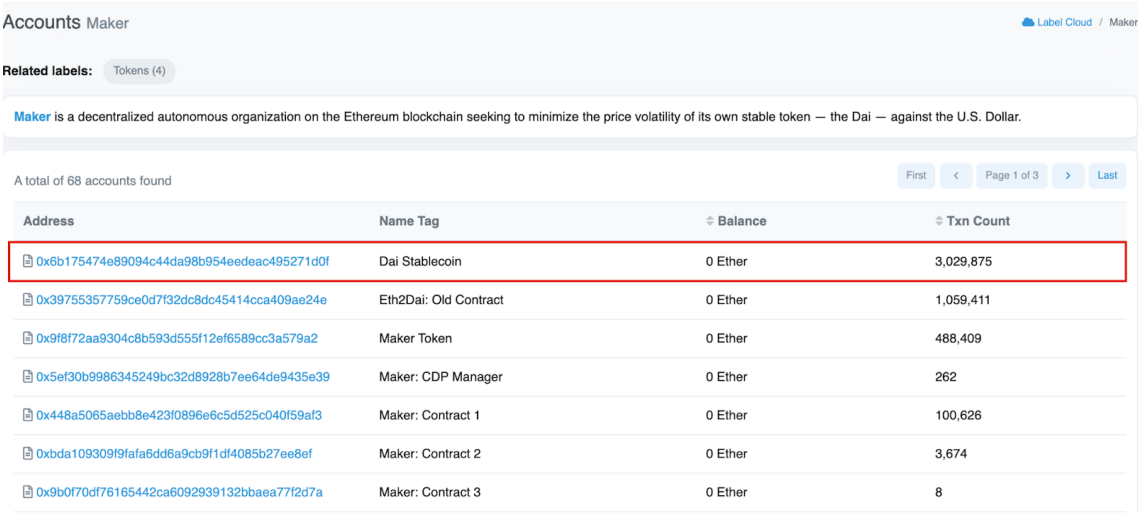

Ilustración 18. (2021). Contratos inteligentes desplegados en la cuenta de MakerDAO. Fuente: https://etherscan.io/accounts/label/maker

Si se hace click en el contrato del Token Dai, Ilustración 18, situado dentro del recuadro rojo, se accede a todos las transacciones que hayan involucrado a este contrato. Si se va al apartado Contract, se puede inspeccionar el código del contrato, todos sus métodos, atributos etc., como se muestra en la imagen que viene a continuación, también más abajo se puede observar el contrato en formato ABI.

El acrónimo ABI significa Application Binary Interface. Un contrato inteligente se almacena como bytecode (= datos binarios) en la blockchain bajo una dirección específica también conocida como dirección de contrato. Se necesita la ABI para

acceder al bytecode, porque la ABI define qué funciones se pueden invocar, así como obtener una garantía de que la función devolverá datos en el formato que espera. Si una aplicación web quiere interactuar con un contrato inteligente desplegado en la blockchain necesita: Una dirección de contrato y la ABI. La ABI contiene únicamente información sobre las funciones y los eventos. A continuación, la Ilustración 19 presenta los conceptos mencionados anteriormente.

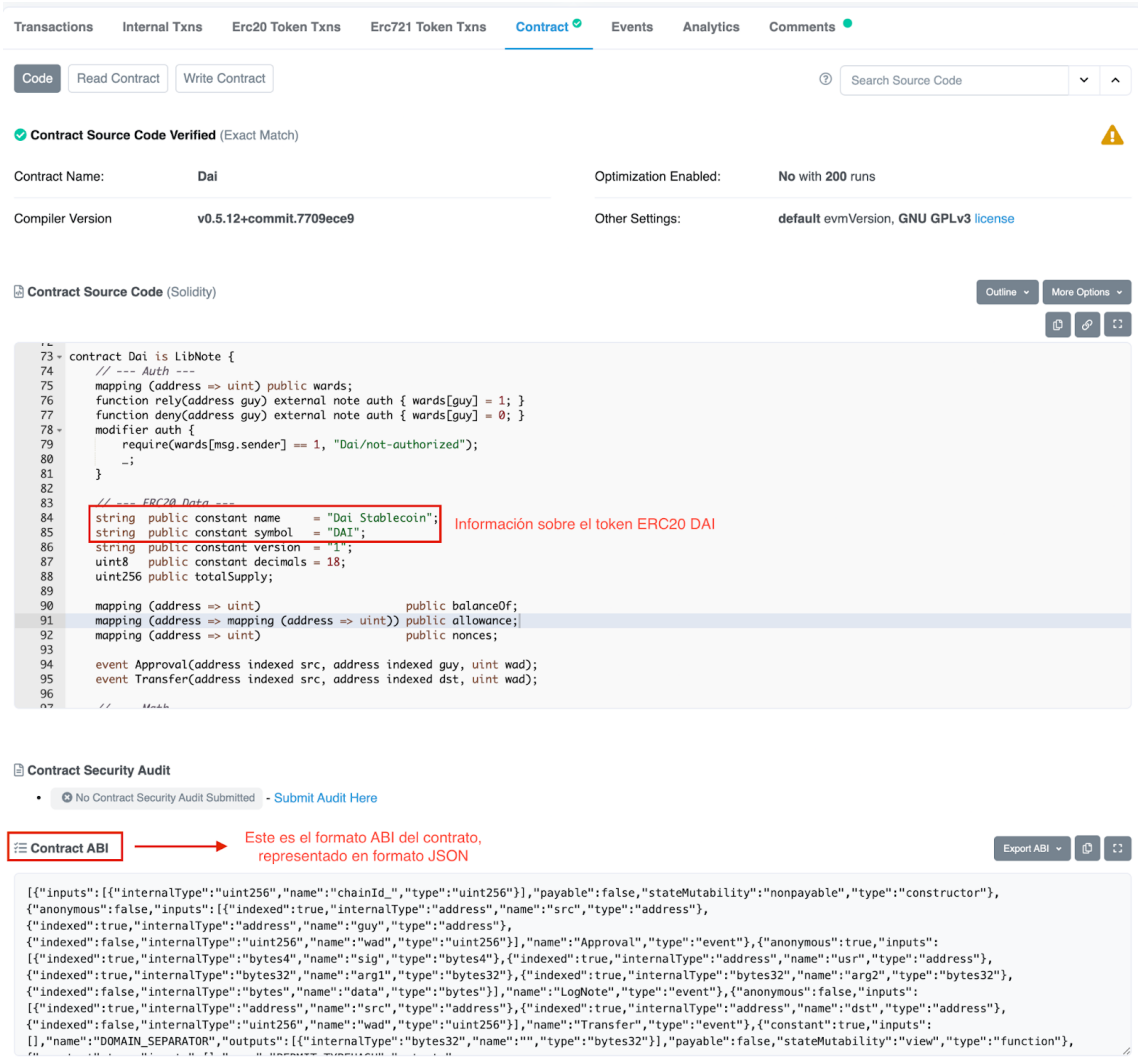

Ilustración 19. (2021). Contrato Dai Stablecoin en Solidity y en formato ABI. Fuente: https://etherscan.io/address/0x6b175474e89094c44da98b954eedeac495271d0f#code

Uso de la plataforma Maker: Guía paso a paso

Para proporcionar una descripción general de Maker, vamos a observar cómo podemos generar nuestro propio Dai, que es la acción que normalmente se realiza en la plataforma. En la plataforma Maker (www.oasis.app), podemos pedir prestado Dai poniendo una garantía en el Vault. Suponiendo que ETH actualmente vale $ 2000, podemos bloquear 1 ETH en el Vault y recibir un máximo de 1333 DAI con un ratio de garantía del 150%.

No debemos extraer el máximo de Dai que tengamos permitido, sino dejar un margen en caso de que el precio de ETH disminuya. Aconsejamos dar una brecha más amplia para garantizar que nuestro Ratio de garantía se mantenga siempre por encima del 150%. Esto asegura que nuestro Vault no se liquidará y no se nos cobrará la multa por liquidación del 13% en caso de que ETH baje de precio.

Si hay interés en como utilizar la plataforma Maker, hemos incluido una guía paso a paso sobre cómo generar DAI.

Cómo generar nuestros propios Dai

Para entender los siguientes pasos que vamos a realizar, se ha proporcionado una ilustración con la que se pretende realizar un símil respecto a las finanzas centralizadas, de esta forma se hará más sencillo el entendimiento del motivo por el cual los usuarios buscamos generar Dai y el proceso para hacerlo.

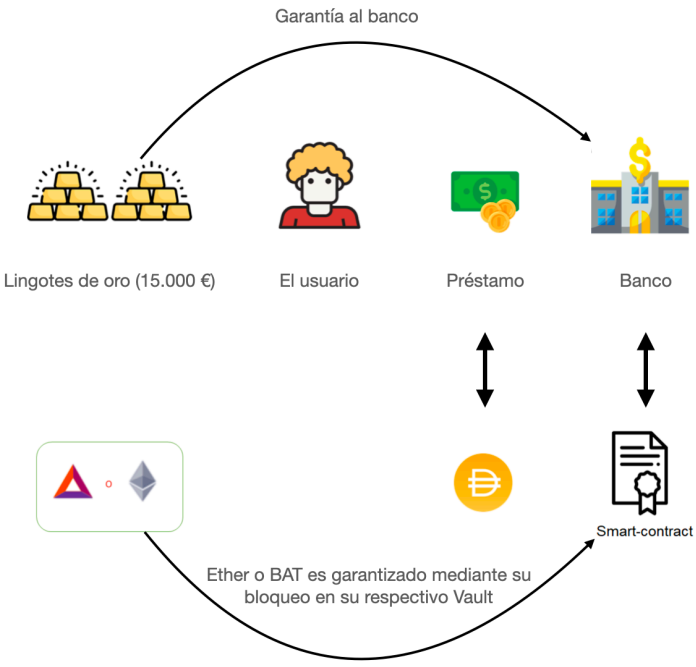

Ilustración 20. (2021). Comparación ilustrativa del funcionamiento de Maker con las finanzas tradicionales.

Paso 1:

- En la ilustración 21 podemos observar la página principal de Oasis: https://oasis.app/
- Debemos hacer clic en Abrir un Vault de Maker
- Se nos pedirá que conectemos nuestra billetera. Conectar nuestra billetera es gratis, lo único que necesitaremos hacer es firmar una transacción que saldrá automáticamente nada más hagamos clic, como muestra la Ilustración 22.

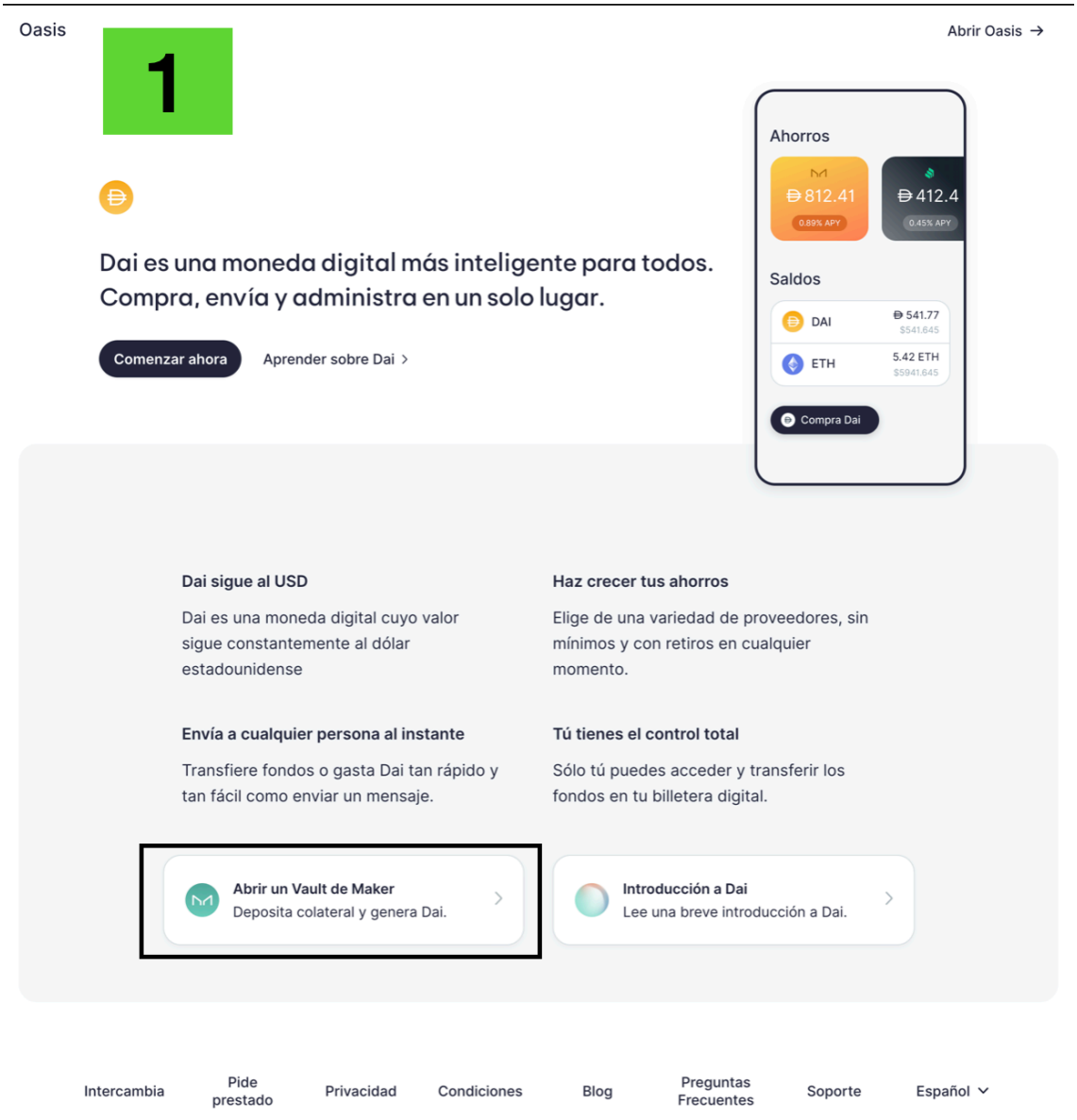

Ilustración 21. (2021). Página principal Oasis app. Fuente: https://oasis.app/

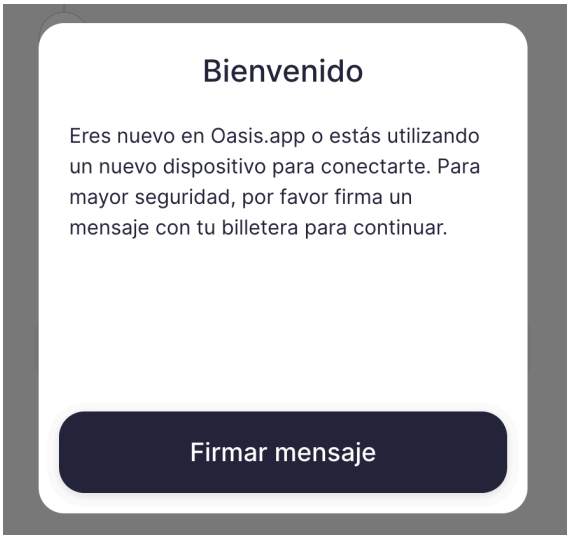

Ilustración 22. (2021). Ejemplo del mensaje a firmar por usar por primera vez un token en Maker.

Paso 2:

- Cuando hagamos clic en Crear un Vault de Maker, deberemos hacer lo que muestra la Ilustración 23 y seleccionar “Open Vault”

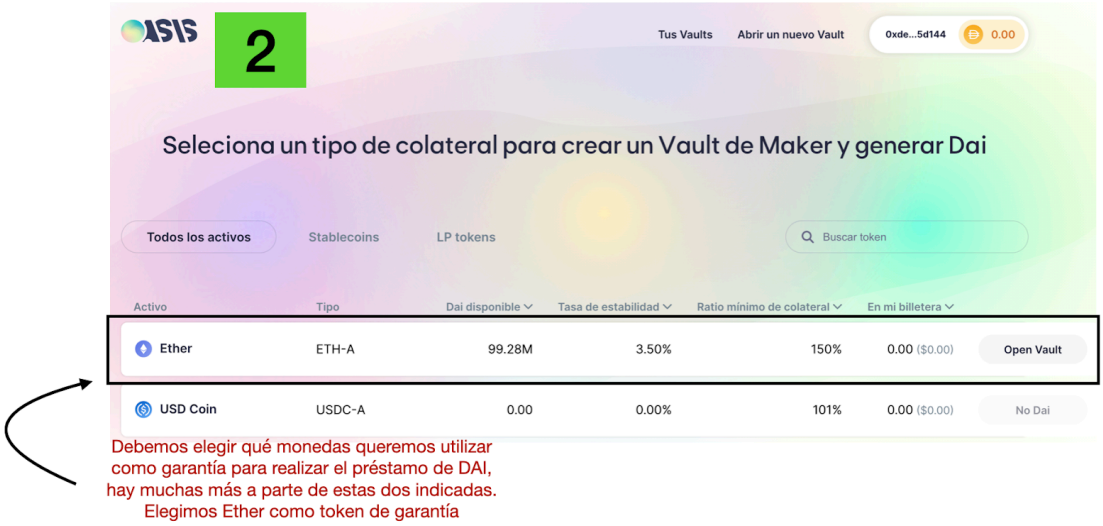

Ilustración 23. (2021). Selección del tipo de Vault para depositar una determinada de garantía.

Paso 3:

- En este ejemplo, seleccionamos Ether como garantía para generar los Dai
- Hay que insertar la cantidad que deseemos bloquear en el Vault (Ilustración 24), cuanto mayor sea el monto bloqueado, más Dai podremos generar

- Por último, deberemos hacer clic en “Configurar Proxy” y seguir las instrucciones que nos aparezcan, como muestra la Ilustración 24.

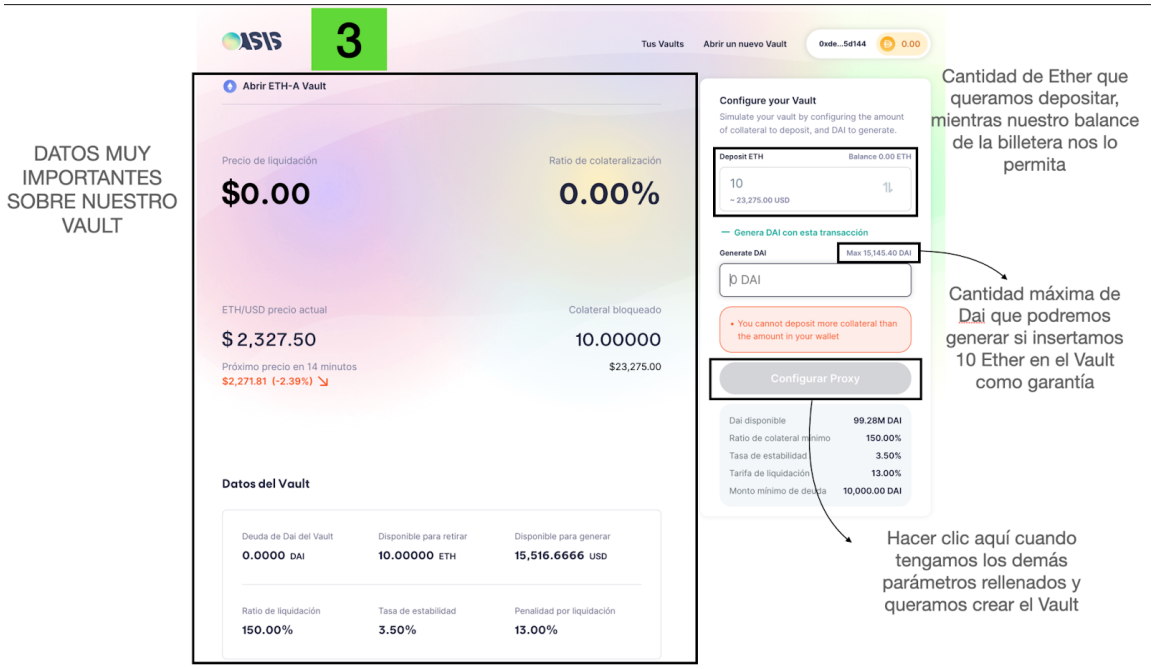

Ilustración 24. (2021). Explicación ilustrativa de cómo generar el Vault seleccionado.

Hay varios datos a tener en cuenta en esta Ilustración 24, como son el “Precio de liquidación”, “Ratio de colateralización” y los “Datos del Vault”. Estos datos nos proporcionan una información muy valiosa respecto al estado de nuestro Vault, debido a que, si hay demasiada deuda en el Vault, podríamos llegar a perder alguna parte de nuestra garantía. Además de generar Dai, también podemos ahorrar en la plataforma Maker para ganar intereses sobre esos Dai generados.

5. Exchanges descentralizados

En esta parte del trabajo, se va a nombrar y explicar los innovadores exchanges descentralizados construidos en la blockchain. A raíz de una idea que propuso Vitalik Buterin en un foro de Reddit, Uniswap salió a la luz y se desarrolló con total éxito, hasta convertirse en el Exchange más usado de la blockchain a diario. Se van a introducir los conceptos matemáticos e informáticos que hacen que esto sea posible, así como los componentes y características que en conjunto forman Uniswap.

5.1 Introducción

Los Exchanges Centralizados (CEXs) permiten hacer largos intercambios debido a la gran elevada liquidez que poseen y aún así conlleva grandes riesgos porque los usuarios no son los que custodian esos activos que acaban de adquirir, son los propios exchanges quienes los custodian. En 2019 más de 290 millones de dólares fueron robados en el sector de las criptomonedas y hubo numerosas fugas de datos comprometiendo la información personal de más de 500.000 usuarios [84].
Cada vez más personas se están dando cuenta de estos problemas y están recurriendo a los Exchanges Descentralizados (DEXs). Este tipo de Exchange funciona mediante el uso de contratos inteligentes y las transacciones dentro de la red para reducir o eliminar la necesidad de un intermediario.
Hay 2 tipos de DEXs [85], los que están basados en un libro de órdenes (order book) o los que se basan en una reserva de liquidez (liquidity pool). La diferencia principal entre ambos exchanges, CEXs y DEXs, es que en los CEXs los activos que intercambies se van a guardar en el exchange y en el DEXs, los activos comprados van a estar en la propia cartera digital.
Sin embargo, uno de los mayores problemas a los que se enfrentan los DEXs es la liquidez. Es posible que los usuarios tengan que esperar mucho tiempo para que sus pedidos se completen en el libro de órdenes. Para resolver este problema, se introdujeron DEX basados en “liquidity pools”. Las liquidity pools [86] son esencialmente reservas de tokens en contratos inteligentes y los usuarios pueden comprar o vender tokens instantáneamente desde los tokens disponibles en la liquidity pool. El precio del token se determina algorítmicamente y aumenta para grandes operaciones. Las liquidity pools de los DEX se pueden compartir en múltiples plataformas de exchanges descentralizados y esto aumenta la liquidez disponible en cualquier plataforma.
Un ejemplo del que se va a hablar más tarde es Uniswap. Uniswap Exchange [87] es un protocolo de intercambio de tokens descentralizado construido en Ethereum que permite el intercambio directo de tokens sin la necesidad de utilizar un exchange centralizado. Cuando se utiliza un CEX, se debe depositar tokens en un exchange, realizar un pedido en el order book y luego retirar los tokens intercambiados.
En Uniswap, simplemente se pueden intercambiar sus tokens directamente desde la billetera sin tener que seguir los tres pasos anteriores. Todo lo que se necesita hacer es enviar los tokens desde la billetera a la dirección de contrato inteligente de Uniswap y se recibirá a cambio el token deseado en su billetera. No hay cartera de pedidos y el tipo de cambio del token se determina algorítmicamente. Todo esto se logra a través de las liquidity pools y el mecanismo automatizado de creación de mercado (AMM) [88].

Hay diferentes categorías de usuarios en el ecosistema del protocolo:

En primer lugar, están los especuladores, que usan el gran abanico de herramientas que el protocolo proporciona para intercambiar tokens e intentar sacar el máximo beneficio.
En segundo lugar, están los bots que realizan arbitraje. Estos bots programados lo que buscan es sacar el máximo beneficio mediante la búsqueda de los mismos tokens a diferentes precios, debido a que cada plataforma es independiente entre sí, cada una tiene su precio en particular. (Aunque pueda parecer que se aprovechan de los usuarios, estos bots en realidad ayudan a igualar los precios en los mercados de Ethereum más amplios y a mantener las cosas justas).
En tercer lugar, se sitúan los usuarios que buscan utilizar Uniswap para comprar tokens y utilizarlos en las diferentes aplicaciones descentralizadas que hay en la red Ethereum.
Por último, están los contratos inteligentes. Estas piezas de código son las que ejecutan las operaciones en el protocolo mediante la implementación de una funcionalidad de intercambio (desde productos como agregadores DEX hasta scripts personalizados de Solidity).
En todos los casos, las operaciones están sujetas a la misma tarifa fija por las operaciones en el protocolo. Es de vital importancia para aumentar la precisión de los precios e incentivar la liquidez, así el mercado se mantiene más equilibrado.

5.2 Uniswap

Uniswap es un protocolo de liquidez automática respaldado por una fórmula de producto constante e implementado en un sistema de contratos inteligentes no actualizables en la blockchain Ethereum [89]. Este protocolo obvia la necesidad de tener intermediarios de confianza para poder realizar las operaciones, priorizando la descentralización, resistencia a la censura y seguridad. Uniswap es un software de código abierto con licencia GPL. No hay ningún token, ni poder centralizado, ni tarifas que vayan a parar al bolsillo de los fundadores.
Cada contrato inteligente, o par de Uniswap, gestiona un grupo de liquidez compuesto por reservas de dos tokens ERC-20.

5.3 Componentes de Uniswap

Para continuar con la explicación, se deben dar a conocer cuáles son las piezas claves de este entorno de intercambio de criptoactivos, cuáles son sus funciones y en que principios están basados para que este nuevo producto sea tan innovador. Para ello, se van a explicar tres piezas esenciales las Liquidity Pools, los Automated Market Makers y los Liquidity Providers.

5.3.1 Liquidity Pools

Las liquidity pools [90] son reservas de tokens que se encuentran en los contratos inteligentes de Uniswap y están disponibles para que los usuarios intercambien tokens. Por ejemplo, al usar el par comercial ETH-DAI con 100 ETH y 20,000 DAI en las liquidity pools, un usuario que quiera comprar ETH usando DAI puede enviar

202.02 DAI al contrato inteligente Uniswap para obtener 1 ETH a cambio. Una vez que se ha realizado el swap, el grupo de liquidez se queda con 99 ETH y 20,202.02 DAI. Las reservas de fondos de las liquidity pools son proporcionadas por proveedores de liquidez que están incentivados para obtener una tarifa proporcional de la tarifa de transacción del 0.3% de Uniswap [91]. Esta tarifa se cobra por cada intercambio de token en Uniswap.
No hay restricciones y cualquiera puede ser un proveedor de liquidez []; el único requisito es proporcionar ETH y el token de negociación cotizado para intercambiarlo al tipo de cambio actual de Uniswap.
Aquí se adjunta la evolución de la liquidez que los proveedores han suministrado y bloqueado en las liquidity pools durante el año 2020 y 2021 en Uniswap, podéis observar en la Ilustración 25, que el crecimiento ha sido enorme y que deja de lado todas las expectativas que tenían los que confiaban en DeFi como un proyecto experimental a gran escala.

Ilustración 25. (2021). Liquidez total en Uniswap. Fuente: https://info.uniswap.org/#/

5.3.2 Automated Market Makers (AMM)

Automated Market Makers o AMM [92], son conocidos y han sido adoptados en numerosos contextos actuales, desde las finanzas hasta el mundo de los mercados de apuestas y recientemente ha sido propuesto como una forma eficiente de fijar los precios en el espacio de las criptomonedas. Su rol es fundamental y encontrar el protocolo correcto es la clave para el lanzamiento de cualquier nuevo mercado.
Existen muchos desafíos para encontrar el algoritmo adecuado, ya que debe ser compatible con las características específicas del mercado, como su liquidez, y sus características deben minimizar el alcance de las oportunidades de arbitraje y el comportamiento errático de los precios.
Por otra parte, los AMMs han sido estudiados en profundidad en la teoría de juegos algorítmicos, empezando por el “logarithmic market scoring rule” (LMSR) [93], a menudo usado en la práctica como AMM para predecir los mercados. Primeramente,

los AMMs deben tener unos proveedores de liquidez que depositen activos en un específico ratio fijado previamente, para que haya un gran flujo de dinero en el mercado, y a partir de aquí, poder predecir los posibles resultados del mercado. Un automated market maker proporciona una regla en la que especifica el coste de cambiar la distribución del estado actual a un estado nuevo deseado.
Normalmente, los LMSR (y AMM similares) están diseñados para predecir el resultado de algún conjunto de eventos (disjuntos) en lugar de predecir un precio específico.
Otro posible modelo para la fijación de precios de activos, introducido por primera vez por Uniswap, no requiere la capacidad de cambiar la oferta de un activo para medir su precio [94].

Los pares de tokens actúan como automated market makers, listos para aceptar el intercambio de un token por el otro mientras que la fórmula de producto constante se cumpla. Esta fórmula, es tan simple como x * y = k, esta expresión matemática establece que las operaciones no deben cambiar el producto (k) de los saldos de reserva de un par (x e y) [95]. Como la k permanece sin cambios, desde el marco de referencia de un comercio, a menudo se lo denomina invariante. Esta fórmula tiene la propiedad de que las operaciones más grandes (en relación con las reservas) se ejecutan a tasas exponencialmente peores que las más pequeñas. Entonces se puede deducir que, a mayor liquidez en el mercado, mayores intercambios de tokens se van a poder hacer sin que las tasas sean exponencialmente peores.
El mercado de producto constante es un mercado para intercambiar monedas del tipo a por monedas del tipo b (y viceversa). Este mercado tiene reservas Ra > 0 y Rb > 0, un producto constante k = Ra * Rb y una tarifa en forma de porcentaje (1 - γ)

Entonces, se ha deducido que una transacción en este mercado, intercambiando ∆b > 0 monedas b por ∆a > 0 monedas a, debe satisfacer:

$$(Ra - \Delta a)(Rb + \gamma \Delta b) = k$$

Después de cada transacción, las reservas se actualizan de la siguiente forma:

Ra → Ra − ∆a, Rb → Rb + ∆b, k → (Ra − ∆a) (Rb + ∆b).

Se requerirá siempre que Ra, Rb > 0, tal que cualquier intercambio que resulte en una reserva no positiva nunca se cumpla (de manera equivalente, se dice que dicho intercambio tiene un costo infinito).
El nombre de “mercado de producto constante” proviene del hecho, que cuando la tarifa es cero (γ = 1), cualquier intercambio ∆b a ∆a debe cambiar las reservas en el sentido en el que el producto Ra*Rb se mantiene igual a la constante k [96].
El truco consiste en aumentar asintóticamente el precio del token a medida que aumenta la cantidad deseada.
En última instancia, el precio pagado refleja cuánto cambia el tamaño de la operación en la relación x / y. Cuanto mayor sea el fondo de liquidez, más fácil es procesar pedidos más grandes (que es lo que cabría esperar, por supuesto), en la Ilustración 26 se muestra un ejemplo práctico para entender mejor la idea.

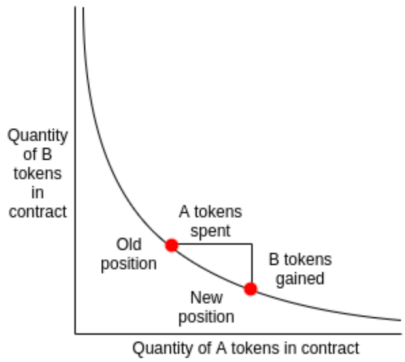

Ilustración 26. Ecuación que Uniswap adopta para calcular el tipo de cambio del token. Fuente: https://medium.com/block-journal/uniswap-understanding-the-decentralised-ethereum-exchange-5ee5d7878996

En la Ilustración 26, se puede observar la gráfica de la relación cantidad de tokens B, cantidad de tokens A y la k.

ETH Purchased	Cost per ETH	Total Cost in DAI	Premium	New DAI Liquidity	New ETH Liquidity	Product
				x	y	k
1	100.10	100.10	0.10%	100,100.10	999	100,000,000
10	101.01	1,010.10	1.01%	101,010.10	990	100,000,000
50	105.26	5,263.16	5.26%	105,263.16	950	100,000,000
100	111.11	11,111.11	11.11%	111,111.11	900	100,000,000
200	125.00	25,000.00	25.00%	125,000.00	800	100,000,000
500	200.00	100,000.00	100.00%	200,000.00	500	100,000,000
800	500.00	400,000.00	400.00%	500,000.00	200	100,000,000
999	100,000.00	99,900,000.00	99900.00%	100,000,000.00	1	100,000,000
1000	Infinity	Infinity	Infinity	Infinity	0	100,000,000

Ilustración 27. Variación de precio respecto a la compra. Fuente: https://cryptoturtles.substack.com/p/automated-market-maker-

En la ilustración 27, se puede ver como quedarían las compras de diferentes cantidades de Ethereum en un par ETH/DAI. A mayor cantidad de Ether comprados, más va a costar de media cada Ether, debido al desequilibrio de liquidez que está provocando en el mercado.
El mecanismo sería un contrato inteligente que contiene tokens A de tipo T1 y tokens B de tipo T2, y mantiene el invariante de que A * B = k para alguna constante k (en la versión donde la gente puede invertir, k puede cambiar, pero solo durante transacciones de inversión / retiro, no operaciones).

¿Cómo calcular el precio de un intercambio en Uniswap?
En el contrato donde se almacenan los tokens, tenemos tenemos 10 Eth y 500 Lisa tokens.

$x * y = k$
x = 10 Eth
y = 500 Lisa
k = 5000

Con estos datos, se desea comprar con 1 Eth la mayor cantidad posible de Lisa tokens. Con la compra de Lisa tokens a cambio de 1 Eth, en el contrato inteligente tendríamos ahora 11 Eth.

11 Eth * Y = 5000
Y = 454.5 Lisa

Es decir, que al final de esta transacción habrá en el contrato inteligente, 11 Eth y 454.5 Lisa tokens, por lo tanto, se habrá intercambiado 1 Eth por 45.5 Lisa tokens. Este ejemplo se realiza sin tarifas de intercambio.
¿Pero qué sucedería si se quisiera volver a intercambiar 1 Ether por tokens Lisa?

5000/12 = 416.6 Lisa
454.5 - 416.6 = 37.9 Lisa

Se puede observar que con esta última compra se ha intercambiado 1 Ether por 37.9 Lisa tokens, a esto se le llama *Price slippage* [97]. Esto es un ejemplo extremo del riesgo que hay en este mercado, pero se utiliza para que se pueda entender la importancia del instante en el que se compra cierto token y la cantidad que desees intercambiar. Con este slippage, entra en juego el *Front running*. Esta acción es de vital importancia, debido a que juega un papel fundamental sobre ganar más beneficio y aprovechar las ventajas del mercado. El Front running [98] es la acción de adelantarse a las otras personas que quieren hacer un trade, posicionándose el primero y que dicha transacción sea la primera que se ejecute, si un usuario paga más fees que otro usuario, la red va a priorizar la transacción del primer usuario para ser validada y obtendrá las ventajas de comprar antes que otros usuarios.
El precio marginal ofrecido por Uniswap (sin incluir las tarifas) en el momento t se puede calcular dividiendo las reservas del activo a por las reservas del activo b.

$$Pt = Ra_t/Rb_t$$

Dado que los usuarios que realizan arbitraje negociarán con Uniswap si este precio es incorrecto (por una cantidad suficiente para compensar la tarifa), el precio ofrecido por Uniswap tiende a seguir el precio de mercado relativo de los activos [99].

Para que en este documento se observe mejor cómo funciona el arbitraje en Uniswap, se va a poner un ejemplo de cómo sería el arbitraje óptimo en esta plataforma. Esta acción es de vital importancia debido a que es esencial que los precios de Uniswap tengan una correlación con los precios de los principales mercados.
En este ejemplo de arbitraje óptimo, tenemos dos monedas, a y b, las cuales pueden ser intercambiadas entre ellas a través de un mercado de referencia o del contrato inteligente situado en Uniswap. En este ejemplo, se va a buscar la maximización del beneficio realizado a través del intercambio de una cantidad de monedas prestadas Δb

de la moneda b, a una cantidad Δa de moneda a, a través del mercado Uniswap. Posteriormente, intercambiamos el Δa recibido por $\Delta b'$ y devolvemos el préstamo Δb para recibir el beneficio $\Delta b'$-Δb.
Si el beneficio es positivo ($\Delta b' - \Delta b > 0$), se dice que hay una oportunidad de arbitraje, debido a que se tiene la posibilidad de ganar dinero "gratis", es decir, sin asumir un riesgo aparente. El problema de este arbitraje óptimo tiene que ver con la cantidad máxima de beneficio que se puede sacar a través de este esquema.
En un mercado infinitamente líquido $\Delta b' = m_p \Delta a$ (donde $m_p$es el precio de mercado de referencia de la moneda a), se puede escribir que el problema de optimización que se busca es el siguiente:

maximize $m_p \Delta a - \Delta b$
subject to $\Delta a, \Delta b \geq 0$
$$(Ra - \Delta a)(Rb + \gamma \Delta b) = k,$$

con las variables de optimización $\Delta a \in R$ y $\Delta b \in R$, obligadas a ser no negativas. Pero en la práctica es más complicado, debido a la rapidez con la que se tiene que ejecutar y por la competencia. Con este ejemplo se pretende que se observe el objetivo que se busca con el arbitraje.

5.3.3 Proveedores de Liquidez

Cualquiera puede convertirse en un proveedor de liquidez (LP) para un par de tokens al depositar un valor equivalente de cada token subyacente a cambio de los tokens de la "piscina" (pool tokens) [100]. Estos tokens rastrean las cuotas de los LP de las reservas totales y se pueden canjear por los activos subyacentes en cualquier momento. A continuación, se pondrá un ejemplo para su mejor comprensión.
En la práctica, Uniswap aplica una comisión del 0,30% [101] a las operaciones, que se añade a las reservas. Como resultado, cada intercambio realmente aumenta la k. Esto funciona como un pago a los LP, que se realiza cuando queman sus tokens de grupo para retirar su parte de las reservas totales. En el futuro, esta tarifa puede reducirse al 0,25%, y el 0,05% restante se retendrá como un cargo para todo el protocolo.

El ecosistema de Uniswap se compone principalmente de tres tipos de usuarios: proveedores de liquidez, comerciantes y desarrolladores. Los proveedores de liquidez están incentivados a contribuir con tokens ERC-20 a grupos de liquidez comunes. Los comerciantes pueden intercambiar estos tokens entre sí por una tarifa fija del 0,30% (que va a los proveedores de liquidez). Los desarrolladores pueden integrarse directamente con los contratos inteligentes de Uniswap para impulsar interacciones nuevas y emocionantes con tokens, interfaces comerciales, experiencias minoristas y más.

Cuando un proveedor de liquidez agrega liquidez a la piscina, pero no solo puede suministrar liquidez a un lado del par. De lo contrario, cambiará la proporción y esencialmente establecerá un nuevo precio (lo cual es peligroso, ya que será arbitrado de inmediato y habrá pérdidas de dinero). Por ejemplo, si un proveedor de liquidez solo agrega 1,000 ETH y 0 DAI, entonces la nueva proporción del contrato es 100,000

/ 2,000 = 50. Los usuarios que hagan arbitraje impulsarán ese mercado hasta que la proporción vuelva a ser 100: 1. Los proveedores de liquidez deben suministrar una cantidad igual de ambos lados de un par comercial (y la interfaz Uniswap ayuda a garantizar que no se cometan errores).
Entonces, supongamos que después de agregar 10,000 DAI y 100 ETH (valor de mercado total de 20,000$), el fondo de liquidez ahora es 100,000 DAI y 1,000 ETH en total. Debido a que la cantidad ofrecida es igual al 10% de la liquidez total, el contrato acuña y envía al creador de mercado “tokens de liquidez” o pool tokens que le dan derecho al 10% de la liquidez disponible en el pool. Estos no son tokens especulativos para intercambiar [102]. Son simplemente una herramienta de contabilidad y teneduría para realizar un seguimiento de cuánto se les debe a los proveedores de liquidez. Si otros posteriormente agregan / retiran monedas, se acuñan / queman nuevos tokens de liquidez de modo que el porcentaje relativo de todos del grupo de liquidez sigue siendo el mismo.

5.4 Características de Uniswap

Con el paso del tiempo hay cada vez más competencia para Uniswap, más y más proyectos que pretenden aumentar su volumen y disminuir el de lo demás proyectos, con el fin de que su capitalización de mercado suba. Uniswap desde que se inició se ha mantenido en lo más alto, pero esto no quita que se haya de saber las características que tienen los exchanges descentralizados como este y los riesgos que se asume al adentrarte en él, se va a exponer uno de los mayores problemas a los que se enfrentan los usuarios que quieren apoyar a estos protocolos y por otra parte, se va a presentar un dilema ético respecto a los credenciales que se necesitan para acceder al uso de estos productos.

5.4.1 Pérdida impermanente

Alice deposita 1 ETH y 100 DAI en un fondo de liquidez. En este Automated Market Maker (AMM) en particular, el par de tokens depositados debe tener un valor equivalente. Esto significa que el precio de ETH es de 100 DAI en el momento del depósito. Esto también significa que el valor en dólares del depósito de Alice es de 200 USD en el momento del depósito. Además, hay un total de 10 ETH y 1,000 DAI en el grupo, financiados por otros LP como Alice. Entonces, Alice tiene una participación del 10% del grupo y la liquidez total es de 10,000.
Digamos que el precio de ETH aumenta a 400 DAI. Mientras esto sucede, los operadores de arbitraje agregarán DAI al grupo y eliminarán ETH hasta que la proporción refleje el precio actual. Se recuerda que los AMM no tienen “order books”, lo que determina el precio de los activos en el grupo es la relación entre ellos en el grupo. Si bien la liquidez permanece constante en el grupo (10,000), la proporción de los activos en él cambia.
Si ETH es ahora 400 DAI, la relación entre la cantidad de ETH y la cantidad de DAI en el grupo ha cambiado. Ahora hay 5 ETH y 2,000 DAI en el grupo, gracias al trabajo de los comerciantes de arbitraje.
Entonces, Alice decide retirar sus fondos. Como se sabe antes, tiene derecho a una participación del 10% en el grupo. Como resultado, puede retirar 0.5 ETH y 200 DAI,

por un total de 400 USD. Obtuvo buenas ganancias desde su depósito de tokens por valor de 200 USD, ¿verdad? Pero espera, ¿qué hubiera pasado si ella simplemente tuviera su 1 ETH y 100 DAI y no lo hubiera invertido proporcionando liquidez? El valor combinado en dólares de estas participaciones sería de 500 USD ahora.
Podemos ver que Alice habría estado mejor manteniendo sus posiciones en su custodio en lugar de depositar en el fondo de liquidez, a esto se le llama Pérdida impermanente [103].
Se puede observar que hay un beneficio cuando la pérdida impermanente es menor a las tarifas recolectadas por proveer liquidez y en la Ilustración 28, se muestra las pérdidas de los proveedores de liquidez por motivo de la variación del precio y del cambio en la liquidez total.
El beneficio se produce cuando, Pérdidas impermanentes < Tarifas recolectadas.

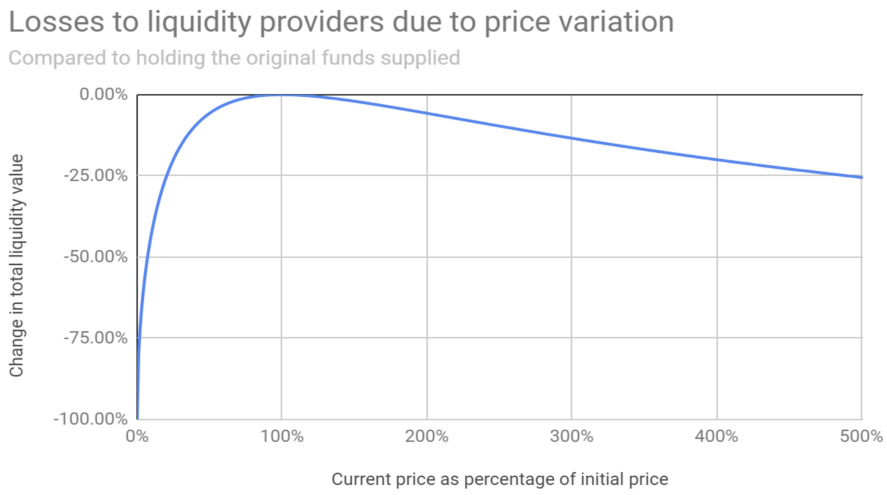

Ilustración 28. Pérdidas de los proveedores de liquidez debido a la variación del precio. Fuente: https://uniswap.org/docs/v2/advanced-topics/understanding-returns/

5.4.2 KYC

El “Know Your Customer” siempre ha sido una batalla ética entre si debería hacerse o no. El KYC es el proceso por el que los bancos obtienen la información de sus clientes lo que garantiza que los servicios bancarios y las regulaciones gubernamentales no se utilicen indebidamente [104]. El procedimiento se realiza cuando un cliente nuevo desea abrir una cuenta. Los bancos también necesitan actualizar esos datos periódicamente. Todos los proyectos que se nombran en este documento no necesitan KYC para utilizar sus servicios y son la competencia del sistema financiero actual.
El propósito del KYC es reducir el riesgo de robos, lavado de dinero, fraude financiero y la financiación a bandas criminales. Este proceso KYC conlleva saber el nombre y firmas autorizadas, condición jurídica de una entidad o persona, identidad de los titulares de la cuenta y otra información según el enfoque de riesgo.
Pero luego hay otro tipo de enfoque diferente donde apoyan que el KYC es una violación de la privacidad. Bitcoin y otras criptomonedas les han dado a esas personas la libertad de realizar transacciones de lo que quieran y cuando quieran, este tipo de

regulaciones como el KYC son solo el primer movimiento de los gobiernos y las instituciones financieras para imponer su poder sobre Bitcoin. Esto se entiende como que, en este sector, el usuario es su propio banco y es él quien maneja sus propios fondos.
Los bancos y entidades financieras tienen la posibilidad de manejar los fondos de otras personas para sacarles rentabilidad sin que ella sea consciente de ello, debido a que se le da permisos cuando firmas el contrato. Pero claro, el prescindir de regulaciones da pie a numerosos fraudes financieros y a diversas formas de manipulación. Así que ni una opción es tan buena, ni la otra es tan mala.
Muchos usuarios entran al mundo de las criptomonedas por la descentralización y el anonimato independientemente de las rentabilidades que se pueda obtener de ellas. Pero hay un concepto que está claro, el usuario debería ser el propietario de su propia información sin tener que dársela a terceros para que trafiquen con ella y que debido a quién sea o lo que se haya hecho en el pasado no puedas acceder a diferentes servicios cuando se necesiten.

5.5 Caso práctico Uniswap

Al ver el sitio web de Uniswap, es importante tener en cuenta que es mucho más que una simple interfaz. Uniswap estandariza cómo se intercambian los ERC20 con un conjunto de contratos inteligentes. Cualquiera puede crear una interfaz que se conecte a estos contratos y poder comenzar a intercambiar instantáneamente con todos los demás que estén usando Uniswap.
Hay dos tipos diferentes de contratos que componen Uniswap, como muestra la Ilustración 29. El primero se conoce como contrato de exchange. Los contratos de exchange contienen un grupo de un token específico y Ether, que los usuarios pueden intercambiar. El segundo tipo de contrato es el contrato Factory, que se encarga de crear nuevos contratos de exchange y registrar la dirección del token ERC20 en su dirección de contrato de exchange. En este apartado se van a mostrar los diferentes contratos de Uniswap y sus usos, además se va a realizar un pequeño recorrido por la plataforma Uniswap para mostrar cómo funciona y de que forma utilizarla.

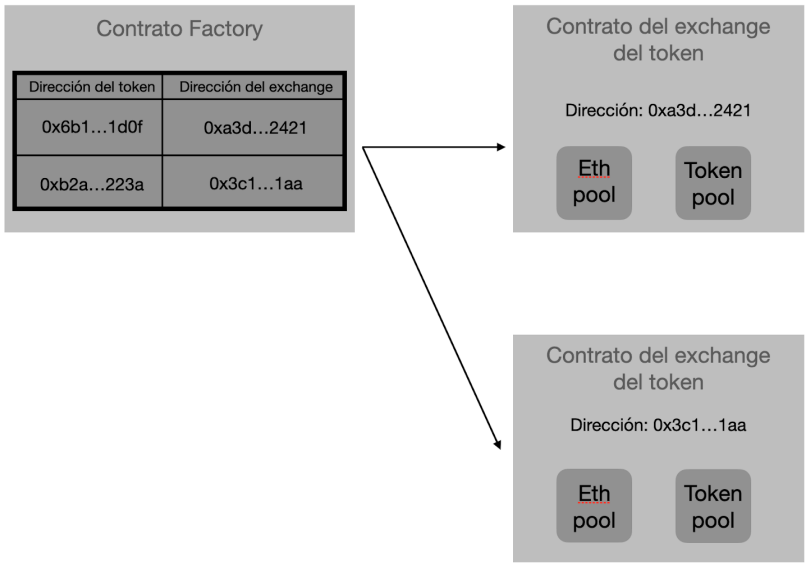

Ilustración 29. (2021). Ejemplo ilustrativo de los diferentes contratos en Uniswap.

Intercambio de tokens (swap) en Uniswap

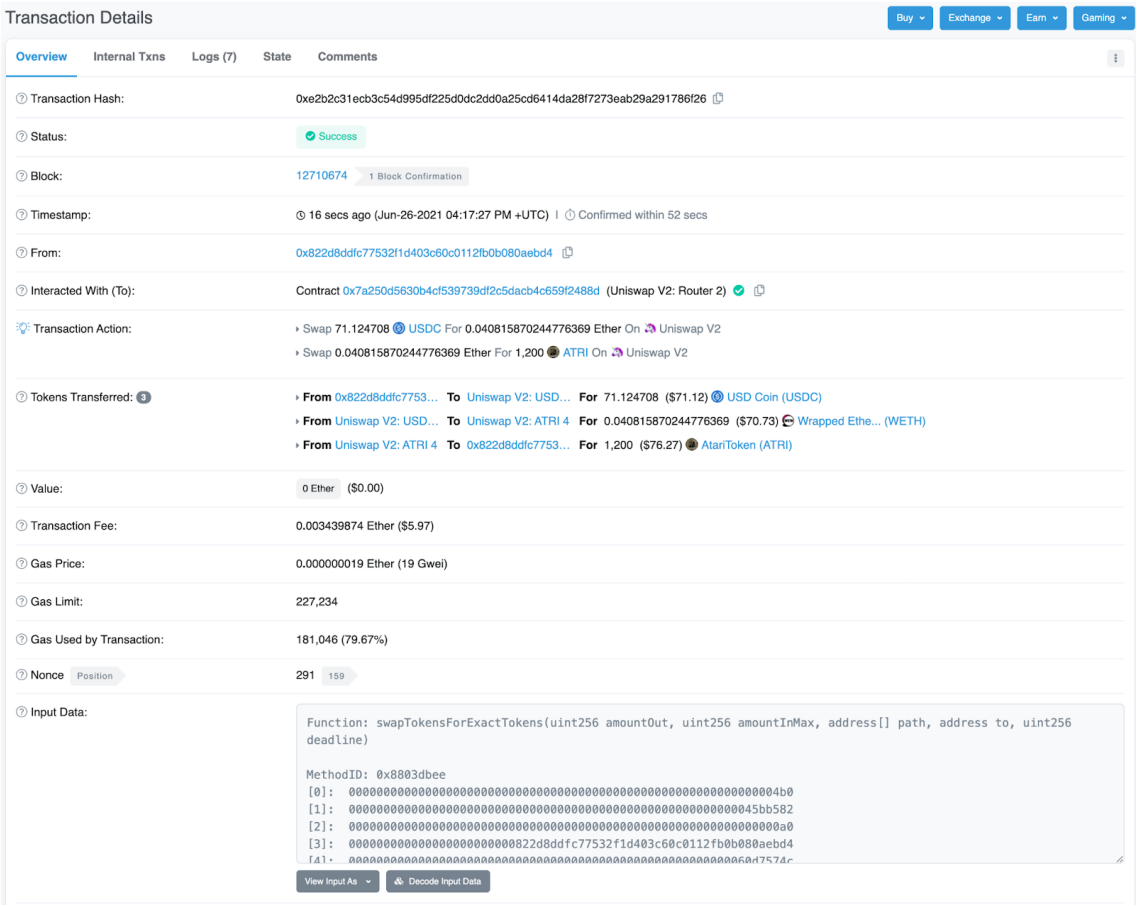

Ilustración 30. (2021). Interacción del intercambio de tokens con la red Ethereum a través de Uniswap. Fuente: https://etherscan.io/tx/0xe2b2c31ecb3c54d995df225d0dc2dd0a25cd6414da28f7273eab29a291786f26

Una transacción en Uniswap internamente se ve como en la imagen mostrada anteriormente, Ilustración 30. Se puede observar que un usuario con una dirección de billetera mostrada en el apartado From, ha cambiado 71.1 USDC tokens por 1,200 ATRI tokens, especificado en Transaction Action. Para ello, el proceso por el que pasa el intercambio de los tokens en este caso es el siguiente: en primer lugar, el usuario envía 71.1 USDC al contrato Uniswap, a continuación, el sistema automáticamente cambia esos USDC por el token WETH, que es un token que se comporta como el Ether interactuando con el contrato WETH. Esto se hace porque no hay un intercambio directo de USDC-ATRI, para realizar este intercambio el sistema cambia USDC por WETH y, por último, cambia WETH por ATRI, utilizando el respectivo contrato inteligente, y se lo envía a la dirección de billetera del usuario inicial.
Para realizar esto se utiliza la función indicada en el apartado Input Data, swapTokensForExactTokens(), que es la encargada de realizar el intercambio exacto de cualquier ERC20 token.

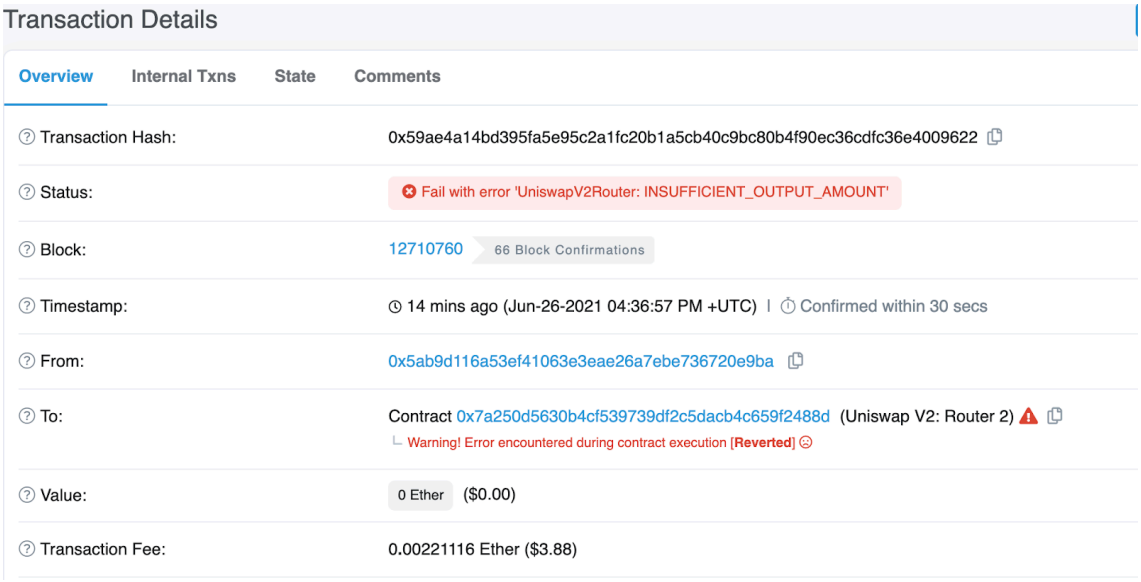

Ilustración 31. (2021). Ejemplo transacción fallida Uniswap. Fuente: https://etherscan.io/tx/0x59ae4a14bd395fa5e95c2a1fc20b1a5cb40c9bc80b4f90ec36cdfc36e4009622

En el caso de que la transacción sea fallida, Ilustración 31, no hay riesgo de perder las criptomonedas que se quiso intercambiar. Lo que hace Ethereum es que revierte la transacción y las criptomonedas se devuelven a la billetera original, eso sí, el gas que se utilizó para ejecutar esa transacción no es redimible, es decir, que no se va a poder recuperar.

Uso de la plataforma Uniswap: Guía paso a paso

En esta parte, se va a realizar una guía paso a paso de cómo realizar un Swap de tokens, cómo proveer liquidez y cómo terminar de proveer liquidez.

Swap de Tokens

Paso 1:

- Para entrar en la aplicación Uniswap debemos ir a su página web y seleccionar el apartado Swap, como se ve en la Ilustración 32: https://app.uniswap.org/#/swap
- Para empezar a usar Uniswap, deberemos conectar nuestra billetera, igual que hemos hecho en Maker, lo único que deberemos hacer es firmar una transacción que incluye los permisos de uso de la billetera que vayamos a asociar en la plataforma.

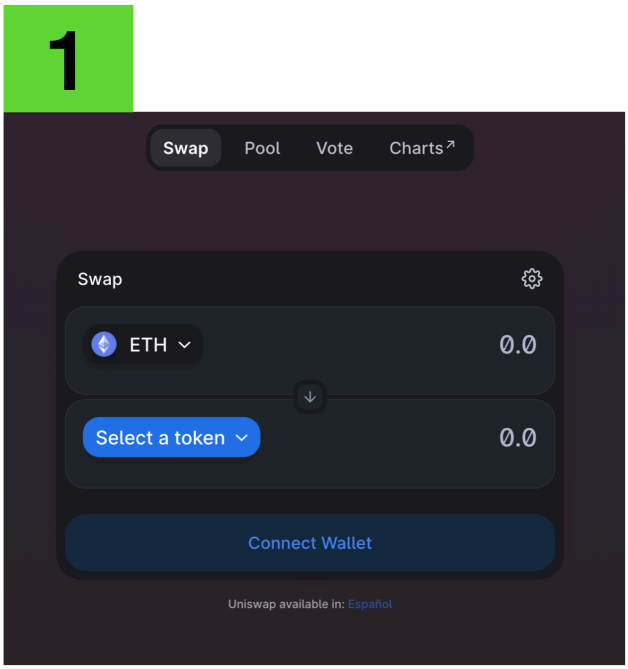

Ilustración 32. (2021). Interfaz Swap de Uniswap. Fuente: https://app.uniswap.org/#/swap

Paso 2:

- Después de conectar nuestra billetera, deberemos escoger que tokens nos gustaría intercambiar, en este caso, hemos optado por cambiar Ether por Dai (Ilustración 33).

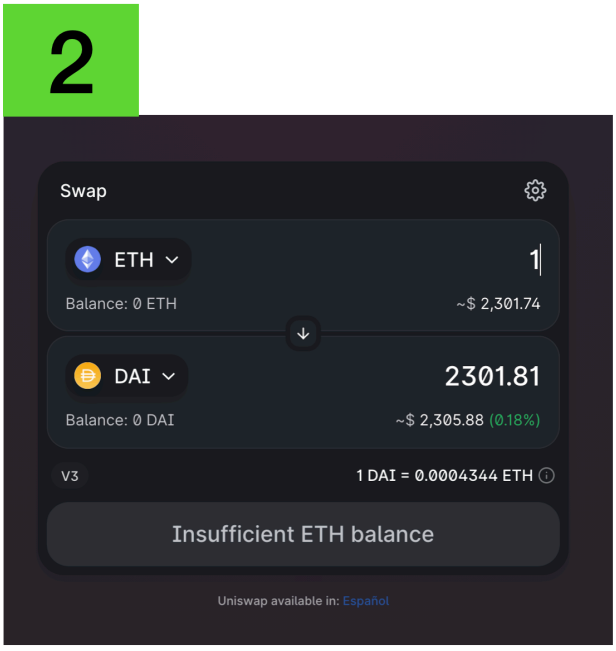

Ilustración 33. (2021). Ejemplo de Swap en Uniswap.

Después de esto, se debe dar al botón Swap (en este caso pone Insufficient ETH balance, porque no tenemos 1 Ether en la billetera).

Paso 3:

- Si es nuestra primera vez realizando una transacción del token que queremos intercambiar, necesitaremos desbloquearlo pagando una tarifa muy pequeña, Ilustración 34
- Una vez hayamos confirmado esta tarifa, nos aparecerá en pantalla otra transacción a confirmar.
- Una vez confirmemos esta última, tendremos los Dai en nuestra billetera.

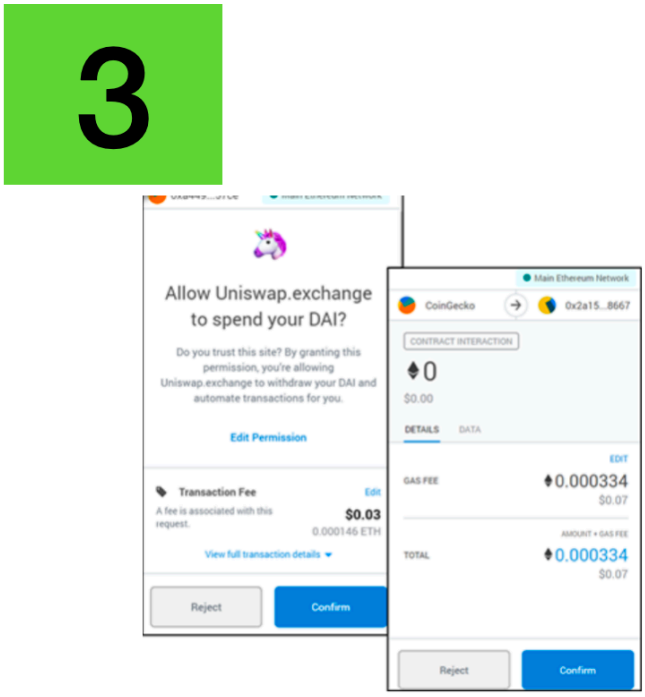

Ilustración 34. (2021). Transacciones que aceptar para completar el proceso de Swap.

Proveer Liquidez

Paso 1:

- Ir al apartado Pool y seleccionamos Añadir V2 Liquidez, se puede observar en la Ilustración 35.

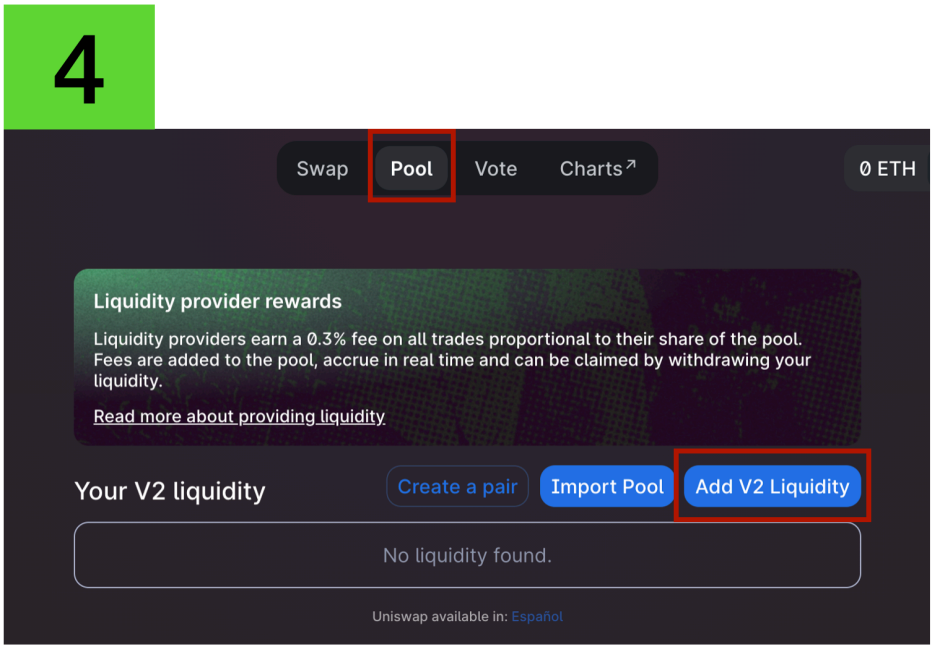

Ilustración 35. (2021). Interfaz de Uniswap para añadir liquidez.

Paso 2:

- Rellenar la cantidad de liquidez que deseamos proveer.
- Hay que suministrar la cantidad equivalente de Eth en Aave, es decir, en el momento en el que hemos realizado la Ilustración 36, si queremos añadir 1 Ether a la piscina de liquidez, debemos añadir también 6.80378 Aave por Ether que queramos añadir.
- Después de hacer clic en añadir liquidez, deberemos firmar otra transacción
- Una vez esto esté hecho, seremos unos proveedores de liquidez y podremos empezar a ganar nuestra parte proporcional de tarifas de intercambio.

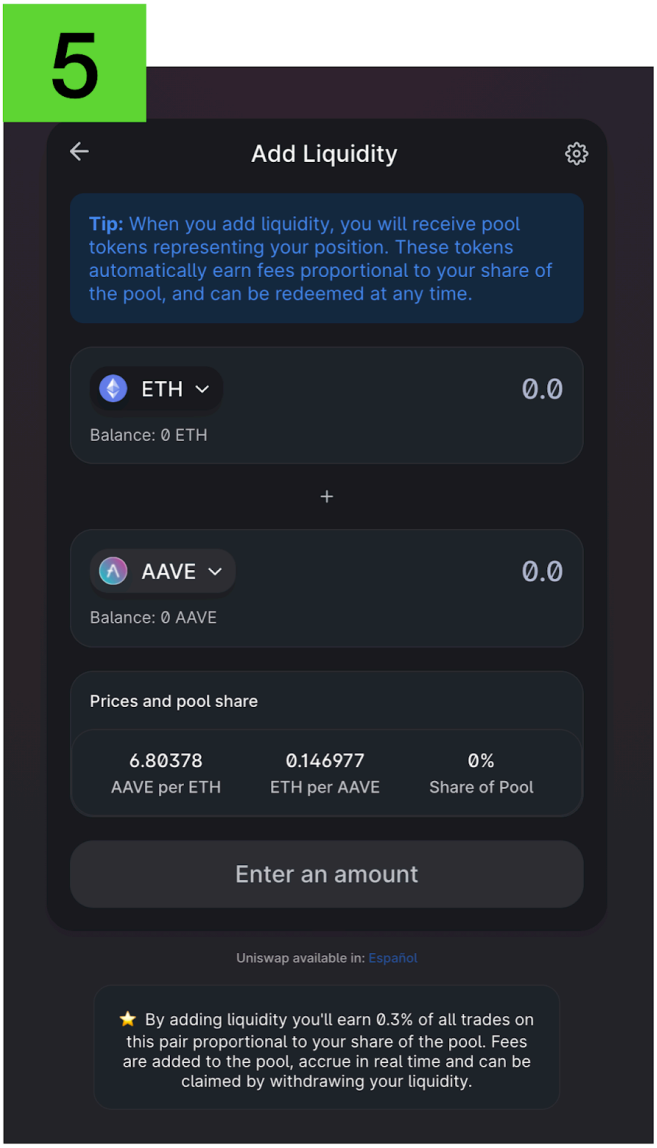

Ilustración 36. (2021). Ejemplo de cómo aportar liquidez a una piscina.

En el momento que deseemos, podemos dejar de proveer liquidez, yendo a la piscina en la que tenemos nuestros tokens y seleccionar el apartado Remove, Ilustración 37. Si realizamos esta acción probablemente vayamos a recuperar una cantidad diferente de tokens a los iniciales que suministramos, esto es debido a que el ratio del par de la piscina puede variar con el paso del tiempo.
Otro punto a tener en cuenta, es que cuando borramos nuestra liquidez, estamos intercambiando el porcentaje de Pool Tokens que tuviéramos, es decir, el porcentaje sobre la liquidez total que nos pertenece.

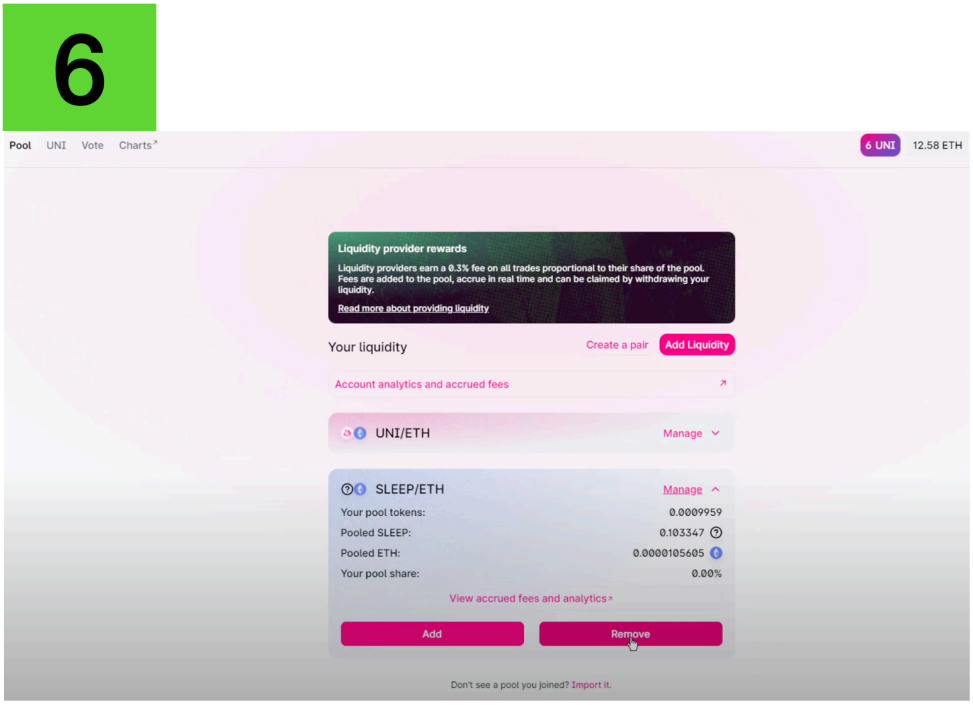

Ilustración 37. (2021). Ejemplo de cómo eliminar nuestra liquidez de una piscina determinada.

6. Préstamos descentralizados (Compound Protocol)

La columna vertebral principal del movimiento DeFi al igual que en la economía actual es el crédito, en la red Ethereum hay un protocolo que destaca por lo relevante que es en este campo, pero la diferencia respecto al tradicional crédito es, que en DeFi el crédito lo dan los usuarios para los usuarios. En este apartado se hablará de Compund, uno de esos protocolos, que principalmente está relacionado con los servicios financieros de pedir prestado y prestar criptomonedas.

6.1 Introducción

Uno de los servicios ofrecidos más comunes por la industria financiera son los préstamos de fondos, que fue posible gracias al concepto de crédito y garantía.
Se puede argumentar que la invención de los préstamos a escala comercial fue lo que generara un frenesí de actividad económica debido a la posibilidad de que los menos ricos adquirieran fondos. Así, la economía comenzó a crecer a un ritmo sin precedentes.

Sin embargo, este sistema requiere de alguna forma de confiar en una tercera persona (intermediario). El rol del intermediario es asumido por los bancos y la confianza se mantiene vía un intrincado sistema de crédito, donde el prestatario debe mostrar una garantía con la muestre que puede pagar el préstamo con el fin de ser calificado, entre una larga lista de requerimientos y de perfiles de riesgo que contiene el banco.

Esto ha derivado en varios retos y deficiencias en el sistema de crédito actual, como en criterios de financiación restrictivos, problemas geográficos o restricciones legales en cuanto a la accesibilidad de los bancos, grandes barreras para la aceptación de un préstamo y la exclusividad de que solo el rico disfruta de los beneficios del bajo riesgo y los elevados retornos de los préstamos.

En el entorno DeFi, estas barreras no existen debido a que no hay necesidad de la actuación de los bancos. Con las suficientes garantías, cualquiera puede tener acceso al capital que necesiten en el momento que sea necesario. Los préstamos de capital también son algo que ya no disfrutan sólo los ricos, todos pueden contribuir a un fondo de liquidez descentralizado que los prestatarios pueden tomar y devolver a una tasa de interés determinada algorítmicamente. En contraste, para solicitar un préstamo al banco uno tiene que pasar por las restricciones que tienen respecto a las políticas de Know-your-customer (KYC) y contra el lavado de dinero, en DeFi sólo es necesario que proporciones la garantía necesaria para pedir prestado.

Se explorará cómo este mecanismo de préstamos sin banco es posible con Compound Finance [105], un protocolo de préstamos de DeFi.

6.2 El Protocolo Compound

Los tipos de interés rellenan los espacios vacíos entre las personas con un superávit de activos que no pueden utilizar y las personas que no tienen activos (que sean productivos o que tengan un uso para la inversión); el intercambio del valor en ese momento de los activos beneficia a las dos partes, creando una suma que es igual a cero respecto a la riqueza. Los CEXs permiten a los clientes generar deuda para intercambiar activos blockchain con los “mercados de préstamos” que están construidos dentro de los exchanges. Son sistemas que están basados en la confianza que se tenga en el exchange y en la certeza de que no serán hackeados, manipulando los activos y perjudicando a los usuarios. Además, cuando pides prestado en estos exchanges los balances son virtuales; no se puede mover esa cantidad del activo on-chain, por ejemplo, usar los Ether prestados en un smart contract, haciendo imposible el acceso a las dApps.

Compound Finance [106] es un protocolo de mercado monetario de código abierto basado en Ethereum, donde cualquiera puede suministrar o pedir prestado criptomonedas sin problemas. Compound opera como una *liquidity pool* que está programada en la blockchain Ethereum. Los proveedores ofrecen activos en la *pool* y ganan intereses por prestar sus activos, mientras que los prestatarios piden un préstamo de la liquidity pool y pagan intereses sobre su deuda. En esencia, Compound cierra las brechas entre los prestamistas que desean acumular intereses de fondos inactivos y los prestatarios que desean pedir prestados fondos para el uso que necesiten o para su reinversión.

Compound es un protocolo dentro de la red Ethereum que establece los *money markets* [107], que son piscinas de activos que algorítmicamente derivan tipos de interés, basándose en la oferta y en la demanda del activo. Proveedores y prestatarios de un activo interactúan directamente con el protocolo, ganando o pagando una tasa de interés, sin tener que negociar los términos o la garantía con un tercero o con una contraparte. Cada money market es único para cada activo perteneciente a Ethereum.

No tienes que registrarte en Compound para empezar a usarla, eso es lo bonito de las aplicaciones de Finanzas Descentralizadas. A diferencia de las aplicaciones financieras tradicionales donde los clientes deben pasar grandes restricciones debido a la burocracia para poder empezar a usar sus servicios, los usuarios de Compound no necesitan registrarse para nada. Cualquier persona con una billetera de criptomonedas que esté validada por Compound, es decir, que sea compatible con Compound puede empezar a usar esta aplicación inmediatamente.

En su esencia, Compound reduce la dificultad para prestar o pedir prestado al permitir que los proveedores y prestatarios interactúen directamente con el protocolo para los tipos de interés sin necesidad de negociar los términos del préstamo (vencimiento, tasa de interés, contraparte y garantías), creando así un mercado monetario más eficiente.

6.3 Componentes del Protocolo Compound

En este punto, se van a explicar las principales acciones que se pueden llevar a cabo en el protocolo y que son las que realmente hacen que este funcione y, en segundo lugar, de que forma está implementado y que arquitectura sigue, para que el lector se pueda llevar una visión del conjunto más clara.

6.3.1 Funcionalidades del protocolo

Entre las acciones que se pueden realizar en el protocolo, las principales son el suministro de activos a Compound y los préstamos de esos activos suministrados por otros usuarios. Pero todo esto conlleva unos riesgos, que serán mencionados a continuación, que los usuarios han de asumir al interactuar con Compound.

Suministro de activos [108]

El protocolo Compound agrega el suministro de cada usuario; cuando el usuario provee un activo, se convierte en un recurso fungible. Este enfoque ofrece significativamente más liquidez que un préstamo directo; a no ser que todos los activos de un mercado se tomen prestados, los usuarios pueden retirar sus activos en cualquier momento.

Los cTokens representan tu balance dentro del protocolo y acumula intereses con el tiempo.
Una vez que deposites, recibirás las cantidades correspondientes en cTokens. Si suministras DAI, recibirás cDAI, si proporcionas ETH, recibirás cETH y así sucesivamente. El interés no se le distribuye de inmediato, sino que se acumula en los cTokens que ahora tiene y que puede canjear por el activo subyacente y el interés que representa.

Ejemplo

Imaginad que se suministra 1.000 DAI el 1 de enero de 2021 y que el APY ha sido constante durante el 2021 a 5%.

El 1 de enero de 2021: Se deposita 1.000 DAI. Se recibe 1.000 cDAI. Ratio del exchage 1 cDAI = 1 DAI.
El 1 de enero de 2022: Se retira 1.000 cDAI. Se recibe 1.050 DAI. Ratio del exchange 1 cDAI = 1.05 DAI (cDAI ha sido revalorizado en un 5%).

Préstamo de activos [109]

Compound permite a los usuarios pedir prestado a través del protocolo, usando cTokens como garantía, para poder usar ese préstamo donde se necesite dentro del ecosistema Ethereum. Lo único que es necesario para pedir prestado en Compound es que exista el mercado para el token que se desea pedir prestado. Es muy similar a

suministrar un activo, cada money market tiene un tipo de interés, establecido por el mercado, que determina el precio al que se presta cada activo.

Los activos sustentados por el protocolo se usan como garantía para pedir prestado a través del protocolo. Cada mercado tiene un factor de garantía, situado en el rango de 0 a 1, que representa la porción del activo subyacente que se puede tomar prestada. La suma del valor de los saldos de los tokens subyacentes de una cuenta, multiplicada por los factores de garantía, equivale a la capacidad de préstamo de un usuario.

Un usuario que desea pedir prestado y tiene suficiente balance en Compound como para hacerlo, debe llamar a la función borrow() en el respectivo contrato cToken. Esta función comprueba que la cuenta del usuario tenga el suficiente valor como para ponerlo como garantía, posteriormente actualizará el balance del usuario destinado para pedir prestado, se realizará una transferencia de esos tokens a la dirección Ethereum del usuario y se actualizará la tasa de interés del money market. Lo que se puede observar, es que constantemente son funciones programadas que se están llamando entre sí, todas escritas en contratos inteligentes que interactúan entre ellos.

Riesgos [110]

Participar en este protocolo conlleva sus riesgos, el mas común y el más importante es la liquidación de tu garantía. La liquidación se produce si el valor del préstamo pendiente de una cuenta excede su capacidad de préstamo, una parte del préstamo pendiente puede reembolsarse a cambio de la garantía cToken del usuario, al precio de mercado actual menos un descuento de liquidación.

La información requerida para encontrar cuentas al descubierto puede ser obtenida a través de la blockchain. Los smart contracts de Compound ofrecen información sobre las diferentes cuentas que participan en el protocolo. Los activos suministrados, el factor de garantía y los activos prestados determinan la *Account Health*. La *Account Health* [111] es el ratio entre los ETH que se tienen como garantía y los ETH que se han tomado prestados. Cuando el Account Health es inferior a 1, significa que la cuenta ha superado su capacidad como prestatario.

Toda la información necesaria para observar la account health de las diferentes cuentas está disponible en la blockchain. Compound ofrece una API pública que permite leer los estados de salud de las diferentes cuentas. Usando la API y llamando a la función *AccountRequest* [112] con el filtro “max_health”: {“value”: “1.0”}, los liquidadores pueden obtener la información de las diferentes cuentas que han excedido su capacidad como prestatarios.

Una vez que la cuenta es detectada, la liquidación se realiza llamando a la función liquidateBorrow () [113], función del smart contract que necesita los siguientes parámetros:

- La dirección de la cuenta que va a ser liquidada
- La cantidad de pago que va a pagar el liquidador

- El token de la garantía, representada por una dirección del smart contract de Compound para este token, que va a ser repagada por el liquidador, con un 5% de descuento

6.3.2 Implementación y arquitectura

En su esencia, Compound es un permite a las cuentas de Ethereum proveer servicios cómo prestamistas [114] y prestatarios [115], mediante el suministro o el préstamo de activos, mientras el interés es computado para cada acción como función sobre el tiempo. Los contratos inteligentes del protocolo podrán ser accedidos por cualquier usuario y su uso es completamente libre y gratuito tanto cómo para las máquinas, dApps y humanos.

Contratos cToken

Cada mercado está estructurado como un contrato inteligente que implementa la especificación del token ERC-20. El balance del usuario se representa mediante cTokens; el usuario puede generar cTokens a través del suministro de activos en el mercado mediante la función **mint(uint amountUnderlying)** o puede quemar esos cTokens para recuperar el activo subyacente del inicio mediante **redeem(uint amount).** El precio (tipo de cambio) entre los cTokens y el activo subyacente incrementa con el tiempo, debido al interés que se aplica sobre el monto prestado. A medida que aumenta el saldo total de préstamos del mercado (en función de la acumulación de intereses del prestatario), el tipo de cambio entre cTokens y el activo subyacente aumenta.
Estas son las diferentes funciones existentes en los contratos inteligentes para cada mercado de activos [116]:

- **mint (uint256 amountUnderlying):** Transfiere el activo subyacente dentro del mercado.
- **redeemUnderlying(uint256 amountUnderlying)**: Transfiere el activo subyacente fuera del mercado, actualizando el balance del usuario.
- **repayBorrowBehalf (address account, uint amount)**: Transfiere el activo subyacente dentro del mercado, para pagar la deuda que poseía.
- **liquidate (address borrower, address collateralAsset, uint closeAmount)**: Transfiere el activo subyacente dentro del mercado, actualiza el balance del prestatario, después transfiere los cTokens que se utilizaban como garantía desde el prestatario al msg.sender.

Partes Fundamentales

Price feeds [117]: Un Price Oracle mantiene el tipo de cambio actual para cada activo que se encuentre en Compound; este protocolo delega la habilidad de establecer el precio de los activos a un comité de piscinas relacionados con los 10 mejores exchanges. Estos tipos de intercambio son usados para determinar la capacidad como prestado y las garantías necesarias y para todas las funciones que requieran calcular el valor equivalente de una cuenta.

Comptroller [118]: El protocolo Compound no apoya a ciertos activos por defecto, en cambio, los diferentes mercados deben ser listados. Para realizar esta tarea, se utiliza una función de administrador, supportMarket (), que permite a los usuarios empezar a interactuar con el activo dentro del protocolo Compound. Cada función es validada a través de una capa de políticas del sistema, llamada Comptroller; este contrato inteligente lo que hace es validar la garantía y la liquidez, antes de que cualquier usuario proceda a realizar una acción.

6.4 Características del Protocolo Compound

En este punto, se va a enfatizar mucho en 2 aspectos, la seguridad y la gobernanza del protocolo, debido a que son dos características de vital importancia al ser un protocolo que mueve grandes cantidades de dinero y que es gobernado por los usuarios. Que menos, que saber la seguridad que asegura el dinero del usuario y cómo se administran todos esos recursos de los que se dispone para mantener una buena gestión de la plataforma. Por último, se van a introducir uno de los aspectos que hace que todo esto sea posible, las firmas digitales en Ethereum, cuyo papel es de alto valor, por las funciones que están implementadas en la gobernanza de Compound que implican realizar estas firmas por razones de autenticación.

6.4.1 Seguridad

El objetivo principal de este programa son las vulnerabilidades que afectan al Protocolo Compound on-chain, es decir, desplegado en la red Ethereum.

Este programa puede cambiar a medida que se implementan nuevos contratos o cuando los contratos existentes se eliminan del uso. Las vulnerabilidades en los contratos construidos sobre el protocolo por desarrolladores externos (como carteras de contratos inteligentes) no están dentro del alcance, ni tampoco las vulnerabilidades que requieren la propiedad de una clave de administrador.
La seguridad del protocolo Compound [119] es de las piezas más importantes para el equipo de desarrolladores, a través de terceras personas que realizan auditorías y consultores. Este esfuerzo invertido ha servido para crear un protocolo totalmente seguro y confiable. Todo el código de contrato y los saldos son verificables públicamente, y los investigadores de seguridad son elegibles para una recompensa por errores por informar vulnerabilidades no descubiertas.
Los participantes de este protocolo piensan en que el tamaño, la visibilidad y el tiempo son la verdadera prueba de la seguridad de un contrato inteligente.

El protocolo Compound fue desarrollado con una serie de especificaciones relacionadas con unos principios de seguridad básicos, verificados por diferentes empresas a través de integraciones en el sistema Compound.

Para obtener una visión clara sobre este apartado, se aporta el ejemplo de la empresa llamada Gauntlet [120], que ha construido una simulación basada en los mercados

para observar el rendimiento de la plataforma y su seguridad, a medida que los activos y el volumen de estos escalan con el tiempo.

Programa Bug bounty [121]

La seguridad es uno de los principios más importantes de este tipo de protocolos, así que se valora el aporte de los profesionales en seguridad informática, intentando mejorar este ecosistema proporcionando ayudas a los desarrolladores, para que así el ecosistema Ethereum sea lo más seguro posible. El protocolo Compound, aunque haya pasado por auditorías profesionales y verificaciones formales, depende de estos usuarios que se encargan de encontrar vulnerabilidades constantemente en estas nuevas tecnologías para que puedan ser descubiertas y gestionadas con la mayor brevedad posible.

Compound anima a la comunidad a auditar los contratos y la seguridad; también fomenta la difusión de cualquier problema que haya de una forma responsable, para que entre todos se pueda encontrar una solución y terminar con el contratiempo. Este programa se creó para reconocer el gran trabajo de la comunidad y de los investigadores independientes, es decir, que a cambio de los actos bondadosos que muchos usuarios realizan, también puedan esperar retornos económicos o de estatus del protocolo hacia ellos.

Recompensas: Compound ofrece unos premios por aumentar la seguridad del protocolo, por lo tanto, descubrimientos respecto la prevención de pérdida de activos, activos congelados, daños al usuario que vayan relacionados con la explotación de alguna vulnerabilidad, se verán recompensados económicamente. Las recompensas van desde 500 dólares hasta los 150.000 dependiendo del descubrimiento.

El alcance secundario del programa es el de recompensas por errores para las vulnerabilidades que afectan a la interfaz de Compount alojada en app.compound.finance y que posiblemente podrían resultar en hackeo de cuentas de usuario.

6.4.2 Gobernanza

El objetivo principal de la descentralización es permitir que el protocolo evolucione hacia una infraestructura financiera resistente, sin puntos débiles identificables y que pueda avanzar pase lo que pase, es decir, que no tenga dependencias reales en un grupo de usuarios. De esta manera, el protocolo puede continuar escalando con el crecimiento de todo el ecosistema criptográfico y durar para siempre, o al menos mientras exista Ethereum.

El protocolo Compound puede ser actualizado y configurado únicamente con los portadores de COMP tokens, los tokens de Compound, y por sus delegados [122]. Todos los cambios que se puedan realizar al protocolo, incluyendo la adición de nuevos mercados, ajustes en los parámetros del sistema, los algoritmos sobre el tipo de interés etc., deben pasar un proceso de propuesta y de votación que está especificado en los contratos inteligentes sobre la gobernanza del sistema.

COMP es un token que está relacionado 1 a 1 con el poder de voto en la gobernanza del protocolo. Los titulares de tokens COMP en sus billeteras Ethereum, pueden delegar sus derechos de voto en sí mismos o en cualquier otra dirección de Ethereum, utilizando una función en el contrato de token COMP ERC-20.

Conceptos clave [123]:

COMP — Es un token ERC-20 diseñado para establecer el peso de voto que tiene cada portador de estos. Cuantos más COMP tengas en tu billetera, más importancia tendrá la delegación del voto o el propio voto del usuario dentro del protocolo

Delegaciones — Los poseedores de COMP no pueden votar ni crear propuestas hasta que deleguen sus derechos de voto a una dirección. La delegación puede asignarse a una dirección en algún momento necesario, incluida la dirección del titular del COMP.

Propuestas — Una propuesta es un código ejecutable que modifica el protocolo y su funcionamiento. Para crear una propuesta, un usuario debe tener al menos el 1% de todos los COMP delegados en su dirección. Todas las propuestas están sujetas a un período de votación de 3 días. Si el proponente no mantiene el balance de sus votos durante el período de votación, cualquiera puede cancelar la propuesta.

Votación — Los usuarios pueden votar a favor o en contra de propuestas individuales una vez que hayan delegado los derechos de voto en su dirección.

Timelock — Todas las acciones de gobernanza y otras acciones administrativas deben permanecer en el Timelock durante un mínimo de 2 días, transcurrido ese tiempo se pueden implementar en el protocolo.

¿Qué se puede hacer con esta gobernanza de Compound?

Los desarrolladores de aplicaciones pueden crear sus propios flujos de trabajo e interfaces personalizados para promover y facilitar la participación de los usuarios mediante el uso de la gobernanza de Compound. Por ejemplo, las aplicaciones integradas con los mercados de tasas de interés de Compound pueden estar interesadas en agregar funciones de gobernanza, que incluyen:

- Alentar a los usuarios a delegar el poder de voto COMP a la dirección del equipo de la aplicación, para que el equipo pueda participar en la gobernanza en nombre de los usuarios.
- Presentar propuestas de gobernanza específicas a los usuarios para que los usuarios con COMP puedan votarlas directamente.
- Brindar a los usuarios información transparente sobre los próximos cambios potenciales que se podrían realizar en Compound.

6.4.3 Firmas digitales en Ethereum y EIP-712

Las firmas criptográficas son una parte clave de la blockchain. Se utilizan para demostrar que a un usuario le pertenece una dirección sin exponer su clave privada. Esto se usa principalmente para la firma de transacciones, pero también se puede usar para firmar mensajes [124].

Cuando se habla de firmas en la criptografía, hablamos de algún tipo de prueba de propiedad, validez, integridad, etc., por ejemplo, se pueden utilizar para:

- Demostrar que el usuario es el que dispone de la clave privada de una dirección (autenticación)
- Asegurarse de que el mensaje no ha sido manipulado por terceras personas.

Se utiliza un mensaje de entrada, una clave privada y un elemento secreto (generalmente) aleatorio, y obtenemos un número como resultado, que es la firma. Usando otra fórmula matemática, este proceso puede revertirse de tal manera que la clave privada y el secreto aleatorio sean desconocidos, pero pudiéndose verificar. Hay muchos algoritmos para esto, como RSA y AES, pero Ethereum (y Bitcoin) utiliza el algoritmo de firma digital de curva elíptica, o ECDSA. Se ha de tener en cuenta que ECDSA es solo un algoritmo de firma.

Usando la manipulación del punto de curva elíptica, podemos derivar un valor de la clave privada, que no es reversible. De esta manera podemos crear firmas que sean seguras y a prueba de manipulaciones. Las funciones que obtienen los valores se denominan *trapdoor functions* [125]: una *trapdoor function* es una función que es fácil de calcular en una dirección, pero difícil de calcular en la dirección opuesta (encontrar su antiimagen) sin información especial, llamada *trapdoor*.

Firmar y verificar usando ECDSA

Las firmas ECDSA [126] constan de dos números (enteros): r y s. Ethereum también usa una variable adicional v (identificador de recuperación). La firma se puede anotar como {r, s, v}.

Para crear una firma, necesita el mensaje para firmar y la clave privada (da) para firmarlo. En Ethereum, el hash generalmente se calcula con Keccak 256 [127]. Esto garantiza que la firma no se pueda utilizar para fines fuera de Ethereum.

Para verificar un mensaje, necesitamos el mensaje original, la dirección de la clave privada con la que se firmó y la propia firma {r, s, v}.

El proceso “simplificado” para recuperar la clave pública se ve así [128]:

- Calculate the hash for the message to recover.
- Calcular el punto R = (x1, y1) en la curva elíptica, donde x1 es r para v = 27, o r + n para v = 28.
- Calcular u1 = -zr-1 mod n, u2 = sr-1 mod n.

- Calcular el punto Qa = (xa, ya) = u1 × G + u2 × R.

Ahora Qa es el punto de la clave pública para la clave privada con la que se firmó la dirección. Podemos derivar una dirección de esta clave pública y verificar si coincide con la dirección proporcionada. Si es así, la firma es válida.

V es el último byte de la firma y es 27 (0x1b) o 28 (0x1c) [129]. Este identificador es importante porque, dado que estamos trabajando con curvas elípticas, se pueden calcular múltiples puntos en la curva sólo a partir de r y s. Esto daría como resultado dos claves públicas diferentes (por lo tanto, direcciones) que se pueden recuperar. La v simplemente indica cuál de estos puntos usar.

Transacciones firmadas [130]

El primer grupo de bytes de la transacción firmada contiene los parámetros de transacción codificados RLP y el último grupo de bytes contiene la firma {r, s, v}. Podemos codificar una transacción firmada de la siguiente forma:

Codificar los parámetros de la transacción: RLP (nonce, gasPrice, gasLimit, to, value, data, chainId, 0, 0).
Obtener el hash Keccak256 de la transacción sin firmar codificada con RLP.
Firmar el hash con la clave privada usando el algoritmo ECDSA.
Codificar la transacción firmada: RLP (nonce, gasPrice, gasLimit, to, value, data, v, r, s).

Se debe de tener en cuenta que el ID de la cadena está codificado en el parámetro v de la firma, por lo que no incluimos el ID de la cadena en sí en la transacción final firmada. Tampoco especificamos ninguna dirección “From”, ya que se puede recuperar de la propia firma. Esto se usa internamente en la red Ethereum para verificar las transacciones.

EIP-712: Tipo de estructura de datos de hash y firmas en Ethereum [131]

Esto hace que los datos de firma sean más verificables, presentándose de una manera legible por humanos.

EIP-712 define un nuevo método para reemplazar personal_sign: eth_signTypedData (siendo la última versión eth_signTypedData_v4). Para este método, tenemos que especificar todas las propiedades (por ejemplo, to, amount y nonce) y sus respectivos tipos (por ejemplo, address, uint256 y uint256), así como alguna información básica sobre la aplicación, llamada dominio.

El dominio contiene información como el nombre de la aplicación, la versión, el ID de la cadena, el contrato con el que estás interactuando y un *salt* (Un valor único de 32 bytes codificado tanto en el contrato como en la dApp como último recurso para distinguir la dApp de las demás). El contrato debe verificar esta información para asegurarse de que la firma de una aplicación no se pueda utilizar para otra. Esto resuelve el problema de un posible ataque de repetición.

Los datos para la transacción explicada anteriormente se asemejarían a esto:
0x1901fb502c9363785a728bf2d9a150ff634e6c6eda4a88196262e490b191d5067cceee
82daae26b730caeb3f79c5c62cd998926589b40140538f456915af319370899015d824e
da913cd3bfc2991811b955516332ff2ef14fe0da1b3bc4c0f424929

Consiste en los bytes EIP-191, el separador de dominio con hash, el tipo de transacción con hash y el input de la transacción. Se realiza el hash nuevamente de estos datos y se firman. Luego, se puede usar *ecrecover* para verificar la firma en un contrato inteligente.

Verificar firmas con los contratos inteligentes [132]

Lo que hace que las firmas de mensajes sean más interesantes, es que se puede usar contratos inteligentes para verificar las firmas ECDSA. Solidity tiene una función incorporada llamada ecrecover (que en realidad es un contrato precompilado en la dirección 0x1) que recuperará la dirección de la clave privada con la que se firmó un mensaje.

Lo que hace que algo como esto sea útil, es que un usuario tiene una forma sin tener que confiar en terceras partes para dar ciertos comandos a un contrato inteligente sin enviar una transacción. El usuario podría, por ejemplo, firmar un mensaje que diga: “Envíe 2 Ether de mi dirección a esta dirección”. Luego, un contrato inteligente puede verificar quién firmó ese mensaje y ejecutar ese comando, utilizando un estándar como EIP-712 y / o EIP-1077. La verificación de firmas en contratos inteligentes se puede utilizar en aplicaciones como:

- DEXes
- Contratos multifirmados

Hay dos métodos por los cuales un usuario puede delegar sus derechos de voto o emitir votos sobre propuestas: llamando a las funciones relevantes (delegate, castVote) directamente; o usando la funcionalidad de la firma (delegateBySig, castVotebySig).

Ejemplo:

Delegar por firma (delegateBySig) [133]: Al utilizar una firma EIP-712, los titulares de tokens COMP pueden delegar sus derechos de voto a cualquier dirección de Ethereum. El método delegateBySig del contrato inteligente de COMP está disponible para los usuarios que tienen una transacción de delegación firmada.
Un caso de uso de estas firmas podría ser que un delegado desee reclutar a titulares de COMP para delegar sus votos a dicho delegado y permitirles hacerlo con muy poca complicación.
El delegado puede crear una página web donde los usuarios firmen una transacción delegateBySig utilizando MetaMask y su clave privada, que luego se publicará en el servidor web del delegado. Más adelante, el delegado puede agrupar firmas en una

sola transacción de Ethereum y recopilar oficialmente los derechos de voto de sus electores mediante la ejecución del método delegateBySig.

6.5 Caso práctico en Compound: Liquidaciones y guía Compound

Esta sección explica los aspectos técnicos de la liquidación y presenta los detalles de una acción de liquidación real que se ha realizado. Además, también se va a realizar una introducción a cómo usar la plataforma Compound.

El proceso de liquidación:

Buscar cuentas que están en riesgo

Toda la información necesaria para encontrar cuentas con garantía insuficiente se puede obtener de la blockchain. Los contratos inteligentes de Compound brindan información sobre las cuentas participantes, la cantidad de fondos suministrados por una cuenta, así como los préstamos pendientes. Además, proporcionan el factor de garantía y el precio relativo de cada activo. Se establece un factor de garantía para cada activo y determina el porcentaje que puede pedir prestado contra la garantía. Un factor de garantía está siempre entre 0 y 1, por lo tanto, cada préstamo siempre está inicialmente sobregarantizado.

Cuando la *Account Health* es inferior a 1, significa que la cuenta ha superado su asignación como prestatario.

Aunque toda la información requerida sobre la *Account Health* está disponible públicamente en la blockchain, Compound proporciona convenientemente una API [134] pública que permite leer un resumen de las cuentas y su respectivo estado. De hecho, la API simplemente lee información de la blockchain y la presenta de una forma conveniente. Al usar la llamada API AccountRequest con el filtro "max_health": {"value": "1.0"}, los liquidadores pueden obtener información sobre todas las cuentas que han excedido su capacidad de endeudamiento. (el uso de un umbral superior a 1 para la consulta de estado, puede dar alertas tempranas sobre cuentas que están en peligro de liquidarse pronto).

Realizando la liquidación:

Una vez que se detecta una cuenta liquidable, la liquidación real se realiza llamando a la función liquidateBorrow (), [135] en el contrato inteligente con los siguientes parámetros, como se muestra en la Ilustración 38:

- La dirección de la cuenta liquidada.
- El monto de reembolso pagado por el liquidador
- El token de la garantía, representado por la dirección del contrato inteligente Compound para este token, que se reembolsará al liquidador, con un 5% de descuento.

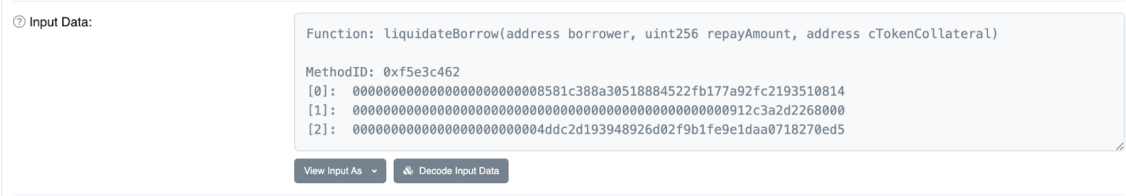

Ilustración 38. (2021). Ejemplo de una transacción para realizar una liquidación en Compound. Fuente: https://etherscan.io/tx/0xb7ba825294f757f8b8b6303b2aef542bcaebc9cc0217ddfaf822200a00594ed9

Para realizar la Liquidación, usamos la herramienta “Compound Liquidator” disponible públicamente, Ilustración 39. La herramienta muestra una lista de cuentas, ordenadas por su estado, utilizando la API de Compound mencionada anteriormente.

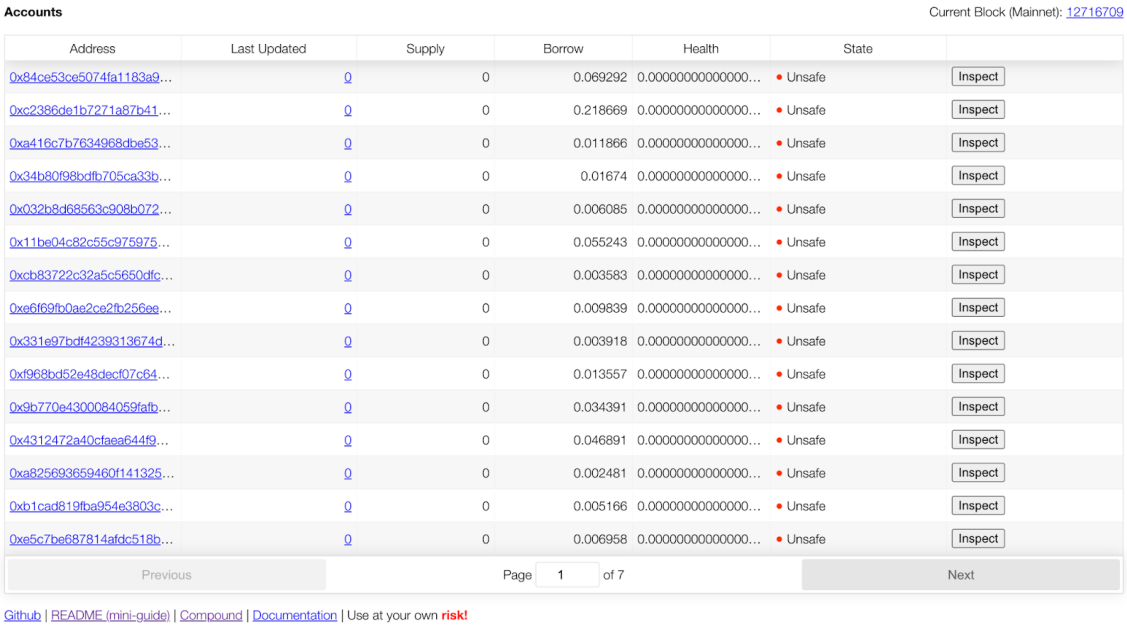

Ilustración 39. (2021). Programa usado para la liquidación. Fuente: https://chiragkhatri.me/compound-liquidator/

Las entradas con una puntuación de *Account Health* inferior a 1 se marcan como "Unsafe" y están sujetas a liquidación, Ilustración 40. Por ejemplo:

Ilustración 40. (2021). Ejemplo de cuenta “Unsafe” lista para ser liquidada.

Al presionar el botón "Inspect" se detallan las garantías y los préstamos actuales de la cuenta, Ilustración 41.

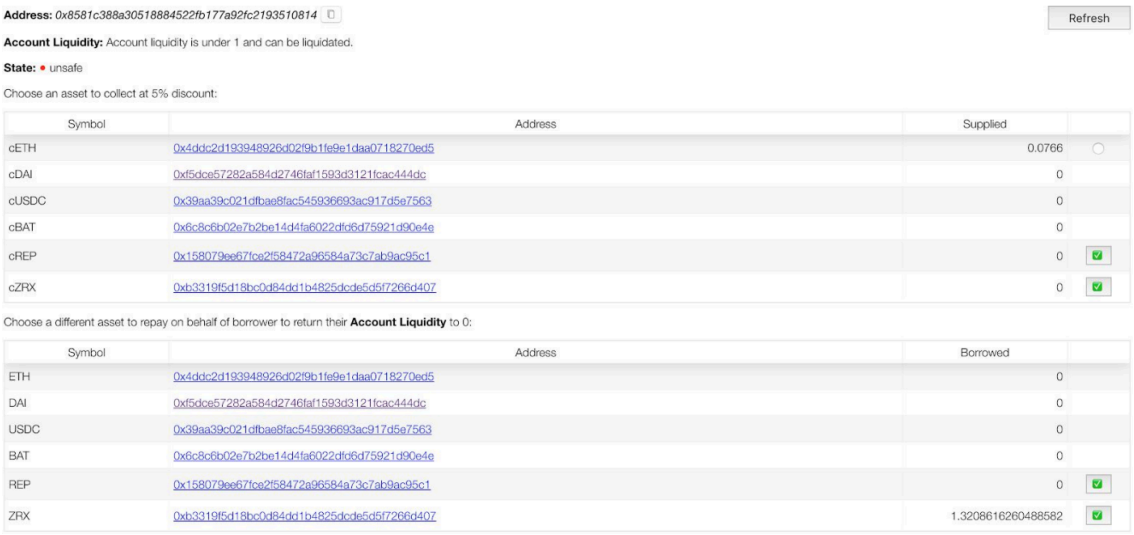

Ilustración 41. (2021). Detalles sobre los présamos de la cuenta y la cantidad del token a liquidar

El propietario de la cuenta ha pedido prestado algo de ZRX y tiene algo de ETH como garantía, Ilustración 42. Elegimos los detalles de liquidación: el token que nos gustaría reembolsar en nombre del prestatario y el token de garantía que se liquida y se recibe como recompensa.

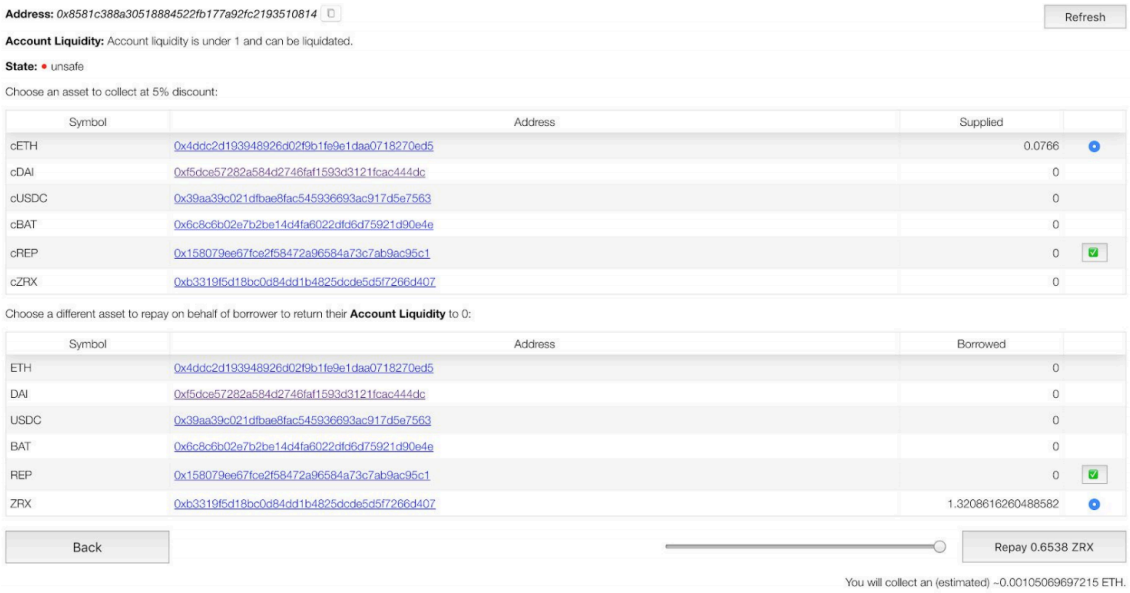

Ilustración 42. (2021). Seleccionando la cantidad del préstamo que se quiere repagar.

Se elige pagar el token ZRX y recibir ETH a cambio. Se elige el monto máximo reembolsable, mostrado en la Ilustración 42. Esto está limitado por el *close factor*, la cantidad máxima que puede liquidarse en una transacción. Actualmente, el factor de cierre es 0,5.

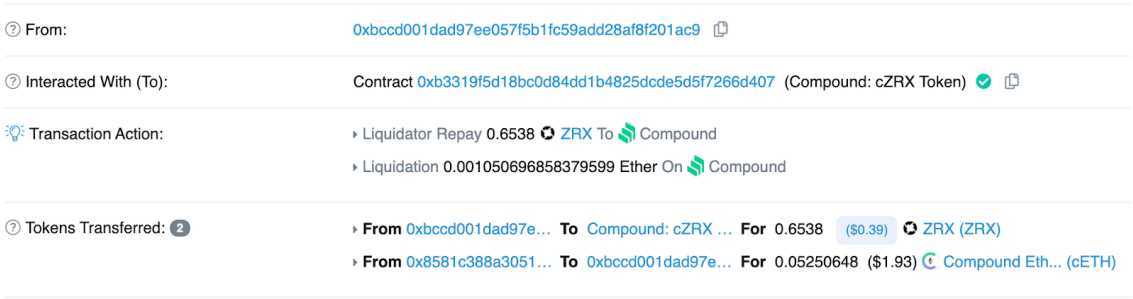

Ilustración 43. Transacción que representa la liquidación realizada.

La transacción se ejecuta, se paga una cierta cantidad de ZRX al mercado y recibimos cETH a cambio, como se observa en la Ilustración 43.

Nuestra cuenta de Compound ahora muestra que estamos suministrando Ether. El cETH se puede dejar en Compound y ganar interés, o canjear por ETH real. Como resultado de nuestra liquidación, la cuenta liquidada está ahora ligeramente por encima del punto de liquidación y la salud del sistema ha mejorado.

Entonces, ¿se ha hecho una fortuna con la prueba de concepto de liquidación? No tanto. Se ganó únicamente 0.01$, mientras se pagó 0.3$ en tarifas de transacción, lo que resultó en un resultado final negativo. Por supuesto, es el resultado esperado, ya que los liquidadores aprovechan rápidamente las oportunidades de liquidación rentables y desaparecen rápidamente, dejando solo las oportunidades de liquidación no rentables para quedarse.

Liquidaciones con contratos inteligentes

El proceso de liquidación a menudo implica pasos adicionales, ya que el liquidador puede necesitar intercambiar sus monedas actuales por la relevante para el reembolso y / o cambiar la garantía cobrada por otra moneda. En el caso que se describe a continuación, Ilustración 44, todo el proceso se automatizó mediante un contrato inteligente.

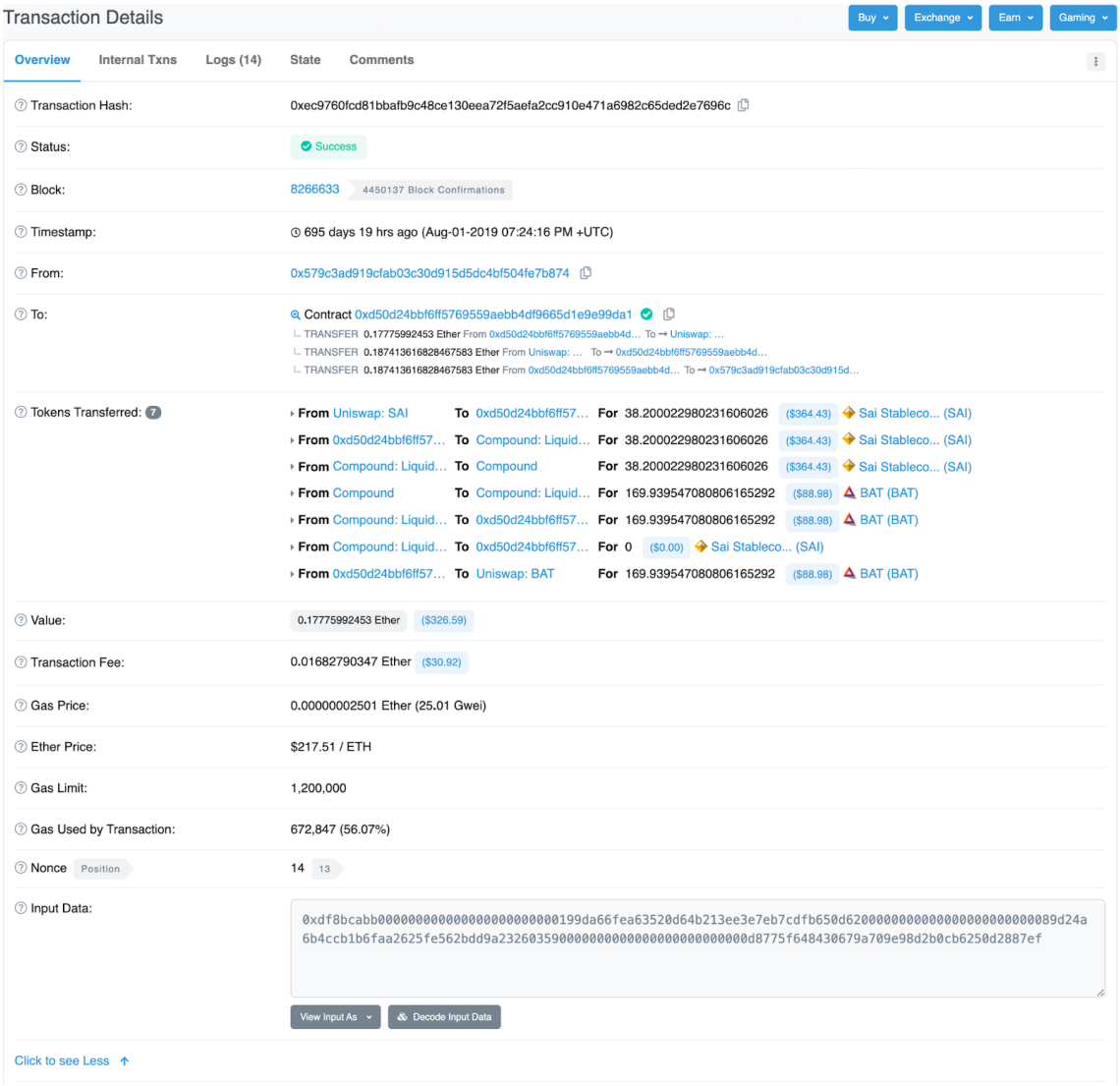

Ilustración 44. Ejemplo de un contrato inteligente programado por un usuario ejecutando liquidaciones con el fin de llevarse beneficios. Fuente: https://etherscan.io/tx/0xec9760fcd81bbafb9c48ce130eea72f5aefa2cc910e471a6982c65ded2e7696c

Este contrato inteligente automatiza todo el proceso de liquidación en Compound: el liquidador envía ETH a un contrato inteligente, el contrato inteligente intercambia ETH a SAI (usando Uniswap), luego el contrato inteligente usa el SAI obtenido para pagar el préstamo y liquidación de la garantía en BAT, y finalmente intercambia BAT de nuevo a ETH (usando Uniswap) y lo devuelve al usuario para obtener una ganancia fácil de ~ 6%. Además de ser una forma elegante de obtener ganancias, realmente muestra el poder de DeFi al poder mezclar y combinar libremente servicios (en este caso, Compound y Uniswap) para crear nuevas oportunidades de ganancias.

Otra ventaja es que un contrato inteligente tiene éxito y su usuario recupera más ETH de lo que comenzó o falla por completo. Si este proceso no se implementó como un contrato inteligente, en el caso de que algo salga mal durante el proceso de liquidación, el usuario podría haberse quedado con algunos resultados intermedios no

deseados; poseer SAI o BAT. Porque el contrato inteligente o se ejecuta por completo o no se ejecuta.

Uso de la plataforma Compound Finance: Guía paso a paso

En esta parte vamos a explicar cómo utilizar Compound Finance paso a paso, con breves explicaciones de cómo utilizar sus herramientas fundamentales. Vamos a explicar cómo suministrar fondos a una piscina de liquidez de un mercado concreto y cómo pedir prestado del protocolo.

Suministrar fondos a la piscina de liquidez

Paso 1:

- Dirigirse a la aplicación Compound: https://app.compound.finance/
- Conectar nuestra billetera, como ya hemos realizado en repetidas ocasiones, tendremos que autorizar a la plataforma para que podamos usar nuestra billetera
- Depositar criptomonedas en la piscina de liquidez (cualquiera de las que hay), cada una tendrá un APY diferente

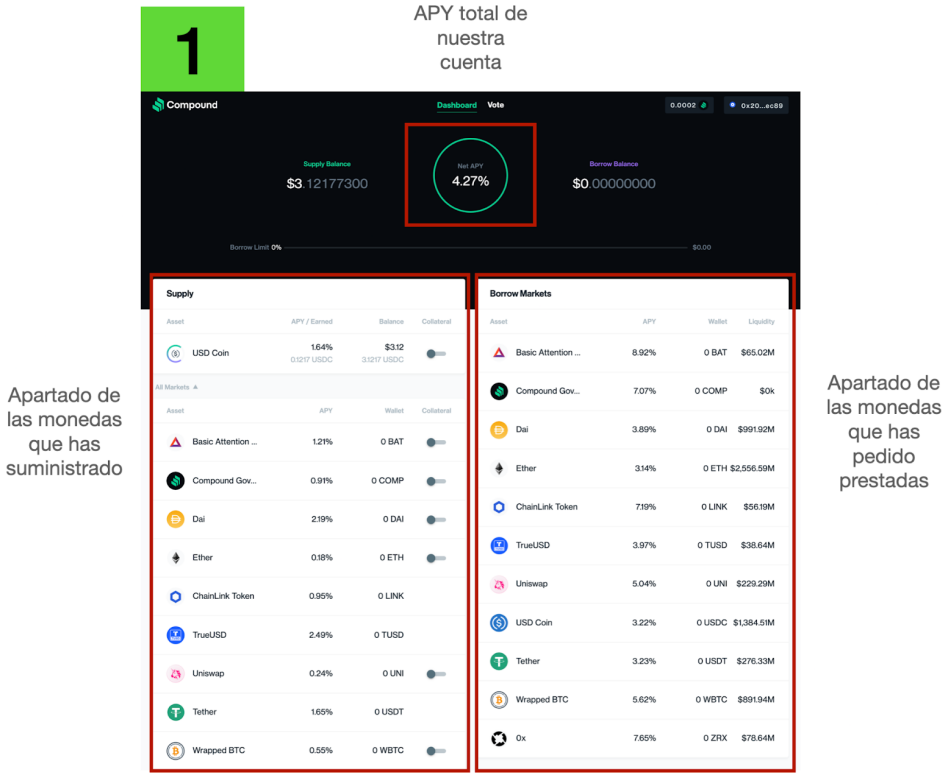

Ilustración 45. (2021). Página principal de la aplicación Compound.

Paso 2:

- En el apartado de Supply tenemos para suministrar dentro del protocolo todas esas criptomonedas.
- Si queremos suministrar la moneda 0x y es la primera vez que queremos realizar esta operación, deberemos pagar una pequeña tarifa como se indica en la Ilustración 46.
- Cuando suministremos cualquier criptomoneda, nos aparecerá como el USD Coin en la ilustración 45, el total del Supply Balance aumentará y estaremos ganando un APY por proveer liquidez al mercado. Es decir, cuando insertemos criptomonedas en el mercado el protocolo nos dará el equivalente, pero en cTokens, que representa el tipo y la cantidad de activos que hemos suministrado.

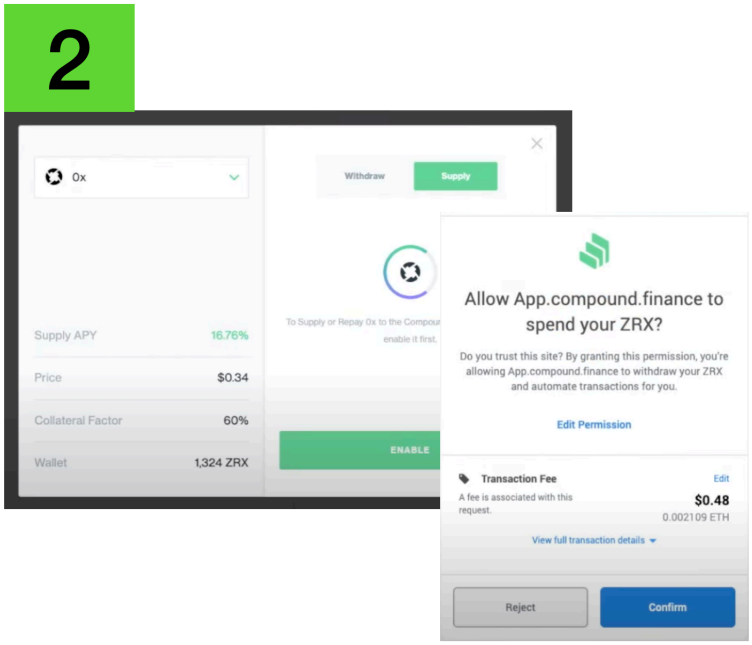

Ilustración 46. (2021). Transacciones que aceptar si usamos por primera vez el protocolo.

Paso 3:

- Una vez depositamos y adquirimos esos cTokens, empezaremos a ganar automáticamente unos intereses, como muestra la Ilustración 47. Con el tiempo, el interés se acumula y cada cTokens se puede convertir en un mayor valor de los activos subyacentes. Podemos canjear los cTokens en cualquier momento y recibiremos los activos en nuestra billetera al instante.

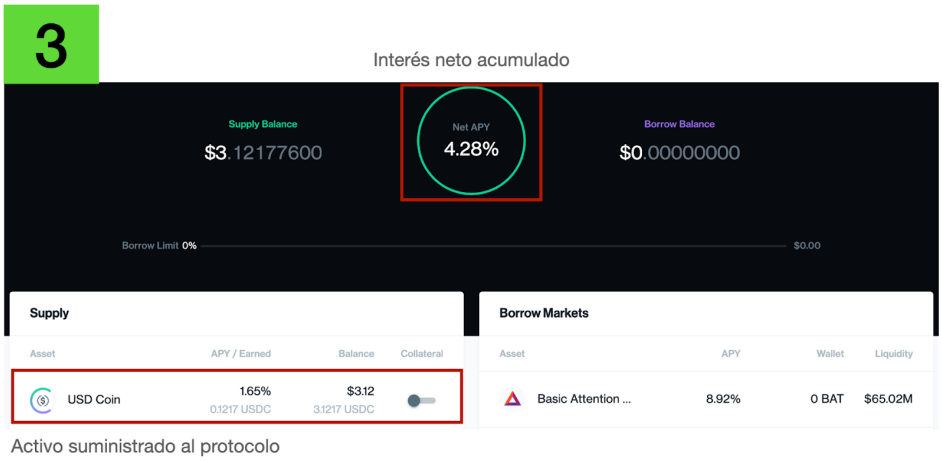

Ilustración 47. (2021). Ejemplo del suministro de USDC al protocolo.

Pedir prestado del protocolo

Paso 1:

- Deberemos ir a la página principal de Compound: https://app.compound.finance/
- Los Borrow Markets son los mercados de los que nosotros podemos pedir prestado. Podemos elegir cualquiera de los disponibles. En la Ilustración 48 se muestran todos los disponibles.

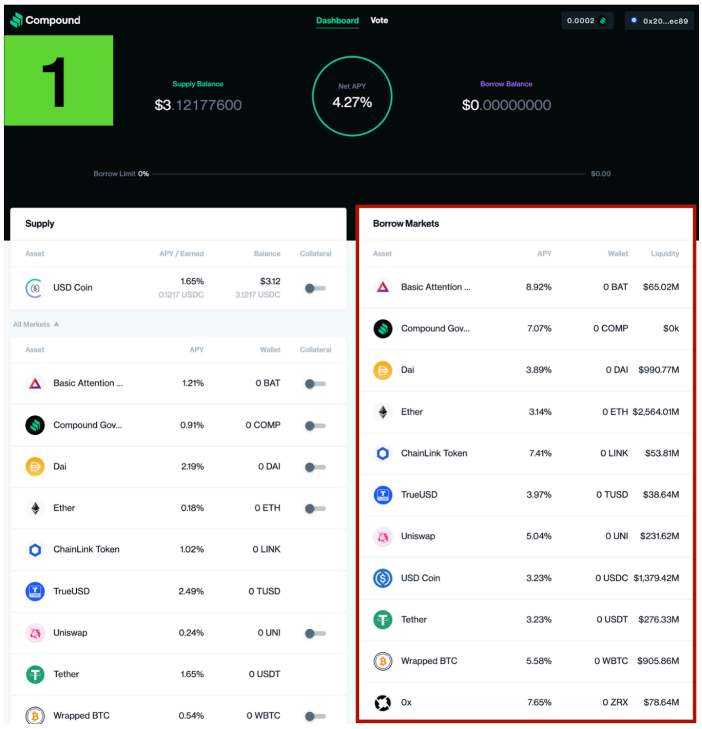

Ilustración 48. (2021). Mercados de los que podemos pedir prestado.

Paso 2:

- Hemos hecho clic en la moneda Ether y la cantidad que queremos pedir prestado en este caso es de 7.73 Ether, para ello le damos al botón Borrow y aceptamos los permisos que nos pida nuestra billetera; esto se observa Ilustración 49.

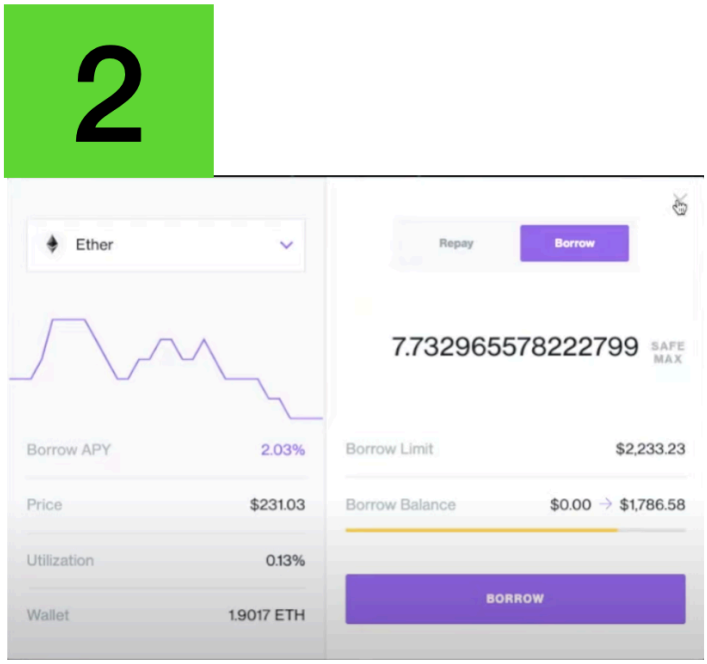

Ilustración 49. (2021). Ejemplo ilustrativo de cómo pedir prestado en Compound.

Paso 3:

- Después de ello nuestro Borrow Balance habrá aumentado el Ethereum que hayamos pedido prestado, pero en dólares. Y en la página principal se podrá observar cuánto hemos suministrado y cuanto hemos pedido prestado, con su respectivo APY, que puede ser negativo si el APY del apartado Borrow es mayor que el de Supply.

7. Ethereum 2.0

En este último apartado se va a introducir Ethereum 2.0, el futuro de la blockchain Ethereum. Esta transición va a suponer un cambio en cómo se conoce Ethereum hoy en día, va a cambiar su funcionamiento, arquitectura, disposición, implementación etc., pero siempre conservando sus principios y su ética. Para ello, se explicarán sus diferentes componentes y características, sin la presencia de un caso práctico, debido a que aún están en pleno desarrollo y transición y a lo único que se puede optar es a ser un validador en la nueva red. El objetivo principal de Ethereum 2.0 es reducir drásticamente los problemas que tiene su predecesor, acercándolo cada vez más a las características que tienen las mejores plataformas de internet, pero todo ello en la blockchain.

7.1 Introducción

Ethereum 1.0 tiene hoy en día un problema principal, el cual es la escalabilidad. El uso de su red implica a veces pagar unas tarifas desorbitadas, 1000$ por una transacción de 100$, no tiene ningún sentido pagar más por el medio por el que se envía que lo que se va a enviar. Esto sucedía en 2017 cada vez que había una ICO acompañada del ya congestionado mercado por las altas rentabilidades que ofrecía. Hoy en día es un problema que sigue estando en boca de todos los amantes de las criptomonedas, porque continúa sucediendo, debido a la popularidad de DeFi y del *Yield Farming* [136].

En la tecnología blockchain, hay dos formas de hacer mejorar la escalabilidad de la red, aplicando modificaciones a la capa 1, la capa base, o escalar la red mediante la descarga de trabajo en otra capa, capa 2, esta es básicamente un protocolo o framework secundario [137]. La capa 1 es la base de nuestra red, donde todas las transacciones se llevan a cabo. Llegados a este punto, hay que destacar varias características importantes, la capa 2 puede ser construida encima de la capa 1, sin que esta primera se vea afectada, utilizando los elementos ya creados de la capa 1, como, por ejemplo, los contratos inteligentes. Por otra parte, la capa 2 también aprovecha la seguridad de la capa 1 al anclar su estado en la capa 1. Esto podría llevar a ethereum a aumentar su capacidad de 15 TPS a ~100k TPS en la fase 1 de Ethereum 2.0 [138]. Pero mientras tanto, los rollups serán el paradigma de escalabilidad dominante por los primeros 2 años y utilizando ethereum 1.0 como la capa de datos principal.

Desde otro punto de vista, los protocolos de la capa 2 crean un framework secundario, donde la transacciones y los procesos pueden ser llevados a cabo de forma independiente respecto a la capa 1. Por esta razón, estas técnicas se conocen como soluciones de escalabilidad “off-chain” [139].
Una ventaja de las soluciones off-chain, es que no será necesario modificar la main chain, porque la capa 2 es añadida como una capa extra que mejora el rendimiento. Por lo tanto, la capa 2 tiene el potencial para conseguir un buen rendimiento y no sacrificar la seguridad. En otras palabras, una gran parte del trabajo que es realizada hoy en día por la capa 1, será movida a la capa 2, de esta forma, la capa 1 será la

encargada de proveer seguridad, mientras que la capa 2 se encargará de la productividad, siendo capaz de llevar la velocidad de las transacciones a otro nivel. Un ejemplo de solución para la capa 1 de ethereum es el sharding [140], que resuelve el problema de cuello de botella que tiene cuando hay un número elevado de transacciones. Actualmente, cada nodo tiene que procesar cada transacción de forma secuencial, limitando el rendimiento de las transacciones de la red al máximo que puede procesar cada nodo. Dividiendo la red en 'shards' este límite se elimina y así cada nodo puede procesar diferentes transacciones en paralelo.

La interoperabilidad es una de las soluciones para mejorar la escalabilidad. La red Polkadot proporciona escalabilidad transaccional mediante la distribución de transacciones a través de múltiples blockchains paralelas, conocidas como *parachains* [141].
Los cambios en la capa base de una blockchain pueden ser increíblemente difíciles de ejecutar, ya que la integridad y la seguridad del protocolo son fundamentales para su éxito. Debido a este problema, también se están desarrollando soluciones de capa 2 que complementarán los métodos de capa 1 para proporcionar una blockchain escalable y eficiente.

7.2 Ethereum 2.0

Desde que nació Ethereum, lo que se ha querido hacer es construir un protocolo de consenso en blockchain más eficiente que el "Proof of Work" y para conseguir que la blockchain sea más escalable de lo que son hoy en día, utilizando el "Proof of Stake" y sharding [142].

La demanda de Ethereum, cada vez más alta, hace que las tarifas por cada transacción sean a su vez cada vez más altas, haciendo insostenible el realizar transacciones pequeñas, debido a que el coste de hacerla es mayor que la transacción en sí. Con ello, el almacenamiento de disco necesario para ejecutar un cliente en Ethereum está creciendo a un ritmo vertiginoso, además de el gran impacto energético y ambiental que tiene el mecanismo de consenso actual en Ethereum, el Proof of Work. Para solucionar todos estos problemas y más, llega Ethereum 2.0.

Lo que comúnmente se conoce como Ethereum 2.0 es el conjunto de actualizaciones que abordan estos problemas y más. Este conjunto de actualizaciones ha sido un área que han estado investigando a fondo y desarrollando desde 2014. Ethereum 2.0 es básicamente la conexión de un conjunto de actualizaciones que cooperan entre sí, para hacer que la escalabilidad, la seguridad y la sostenibilidad de Ethereum mejore.

Esto significa que Ethereum no será una actualización que se lance un día y todo el mundo empiece a usarla. Las mejoras serán llevadas a cabo y lanzadas de forma gradual.

ARQUITECTURA

En el centro del sistema Ethereum 2.0 se encontrará la “Beacon Chain” y el propósito de la Beacon Chain es básicamente gestionar el consenso. La Beacon Chain almacena la información sobre las validaciones de los nodos de la red, qué mensajes reciben y envían en la red.... En su esencia, actúa como una red central a la que los shards envían datos. La Beacon Chain tiene una conexión con Eth 1.0, por lo tanto, es una cadena nueva, pero esto no significa que sea un ecosistema separado del inicial, sino que colaboran entre ellos. El puente entre ellos permite enviar los Ether y activos que se tuvieran dentro del existente Ethereum 1.0 y que sea más sencillo migrarlos a la Beacon Chain y con ello a los shards de Ethereum 2.0 [143].

Beacon Chain [144]

Responsabilidad de la Beacon Chain:

- Gestión de validadores y sus intereses.
- Nominar al proponente de bloque elegido para cada shard en cada paso.
- Organizar validadores en comités para votar sobre los bloques propuestos.
- Aplicar las reglas de consenso.
- Aplicar recompensas y sanciones a los validadores.
- Funcionar como un punto de anclaje en el que los shards registren sus estados para facilitar las transacciones entre shards.
- Disposición de aleatoriedad: para mantener la seguridad al realizar un sharding en una blockchain, la Beacon chain realiza una reorganización aleatoria de un comité de validadores que se asignará a cada bloque del shard. Este proceso evita que el sistema sea atacado o controlado por un solo actor malo.

¿Qué hace Eth2 especial?

- Un protocolo nuevo y mejorado con años de dedicación, investigación y experiencia en Ethereum 1.0
- Nuevas tecnologías: BLS aggregation, PoC, Casper FFG, optimización en los Merkle proofs, disponibilidad de los datos, Casper CBC…
- Misma criptomoneda (ETH), mismo ecosistema, puente entre proyectos para su migración
- Énfasis en la simplicidad, escalabilidad y seguridad
- Focalización en una verdadera descentralización

Fases Ethereum 2.0 [145]

- **Fase 0**: Esta fase conlleva la adopción de Proof of Stake, es decir, que puedes depositar ETH y empezar a hacer staking. Esta fase no conlleva mucha más funcionalidad, se despliega para que los usuarios se puedan ir familiarizando con esta nueva forma de validación y que empiecen a iniciar sus nodos y a operar con ellos. La Beacon Chain es el núcleo de la cadena del sistema Ethereum 2.0. Es responsable de administrar el algoritmo de consenso, es decir, el protocolo de PoS de Casper para sí mismo y para todos los shards. La red estará dirigida por un grupo de validadores. Para convertirse en un validador, el nodo envía su participación al contrato inteligente en la actual

blockchain Ethereum. A continuación, el monto de Ether se bloqueará y después de la verificación de validez, se generará un recibo que contiene una identificación que indica el shard al que se asignará el validador.

- **Fase 1 (Data sharding)**: Esto significa que la “shard chain” empieza a funcionar, pero aún no están verificando transacciones, no están ejecutando contratos inteligentes, lo único que hacen es verificar la disponibilidad de los datos.
- **Fase 2**: Estado y ejecución de las cuentas, contratos inteligentes, disponibilidad en los shards, diferentes funcionalidades…
- **Fase 3 y posteriores**: Son mejoras técnicas en el protocolo. Ejemplo: Consensos, escalabilidad etc

7.3 Componentes de Ethereum 2.0

Hay muchas partes importantes en Ethereum 2.0 y más que se van a ir introduciendo con el paso del tiempo, pero para entender Ethereum 2.0, se tienen que explicar los conceptos que se listan a continuación, el Proof of Stake y las partes implicadas y el Sharding. Estas son las partes más importantes del corazón de Ethereum 2.0.

7.3.1 Proof of Stake

Ethereum se está moviendo hacia un mecanismo de consenso llamado prueba de participación o *Proof of Stake* (PoS) desde Proof of Work o prueba de trabajo (PoW). Este fue siempre el plan, ya que es una parte clave en la estrategia de la comunidad para escalar Ethereum a través de las actualizaciones de Ethereum 2.0.

La razón por la que se necesita una prueba de cualquier cosa es por una idea básica. Se tiene una red y se poseen muchas computadoras que están de acuerdo en qué bloque aceptar y, a veces, se obtienen dos bloques que se publican al mismo tiempo y sólo se tiene que acordar una orden para ejecutar, por lo que tiene que haber una especie de juego de votación. Pero entonces la pregunta es, en este juego de votación, quién obtiene el voto. No se puede decir una persona, un voto. La razón por la que no se puede decir que una persona un voto es porque necesitas algún tipo de autoridad o mecanismo para decir quiénes son los humanos y si no tienes eso, entonces un usuario malicioso podría entrar con una máquina virtual o con una computadora que tiene en ella 10 mil millones de máquinas virtuales que tienen 10 mil millones de nodos virtuales y luego simplemente dice "obtengo el poder del 99% de la red, debería controlar todo", así que para evitar esto, lo que hacen PoW (Proof of Work) y PoS (Proof of Stake) es básicamente, medir el peso del voto, cuánta influencia tienen los votos en el consenso y esto es proporcional a la cantidad de recursos económicos que se aportan

Mecanismos de consenso [146]

Los mecanismos de consenso (también conocidos como protocolos de consenso o algoritmos de consenso) permiten que los sistemas distribuidos (redes de computadoras) trabajen juntos y se mantengan seguros.

Durante décadas, estos mecanismos se han utilizado para establecer un consenso entre los nodos de la base de datos, los servidores de aplicaciones y otras infraestructuras empresariales. En los últimos años, se han inventado nuevos protocolos de consenso para permitir que los sistemas *cryptoeconomic*, cómo Ethereum, se pongan de acuerdo sobre el estado de la red.

Un mecanismo de consenso en un sistema *cryptoeconomic* también ayuda a prevenir ciertos tipos de ataques económicos. En teoría, un atacante puede comprometer el consenso controlando el 51% de la red. Los mecanismos de consenso están diseñados para hacer inviable este "ataque del 51%". Para ello, se diseñan diferentes mecanismos para resolver este problema de seguridad de manera diferente.

¿Qué es el Proof of Stake? [147]

La prueba de participación es un tipo de mecanismo de consenso utilizado por las redes blockchain para lograr un consenso distribuido.

Requiere que los usuarios apuesten su ETH para convertirse en un validador en la red. Los validadores son responsables de lo mismo que los mineros en PoW: ordenar transacciones y crear nuevos bloques para que todos los nodos puedan ponerse de acuerdo sobre el estado de la red.

La prueba de participación viene con una serie de mejoras en el sistema de prueba de trabajo:

- Mejor eficiencia energética: no necesita usar muchos bloques de minería de energía,

- Barreras de entrada más bajas, requisitos de hardware reducidos.

- Mayor inmunidad a la centralización: la prueba de participación debería conducir a más nodos en la red

- Mayor soporte al *sharding*: una actualización clave para escalar la red Ethereum

La prueba de participación es el mecanismo que activa validadores una vez recibe la suficiente participación, a través de la tenencia de Ether. Para Ethereum, los usuarios deberán bloquear 32 ETH para convertirse en validador. Los validadores se eligen al azar para crear bloques y son responsables de verificar y confirmar los bloques que ellos no crean. La participación de un usuario también se utiliza como una forma de incentivar el buen comportamiento del validador. Por ejemplo, un usuario puede perder una parte de su participación por cosas como desconectarse (no validar) o toda su participación por actuar de forma malintencionada.

¿Cómo funciona el Proof of Stake en Ethereum? [148]

A diferencia de la prueba de trabajo, los validadores no necesitan usar cantidades significativas de poder computacional porque se seleccionan al azar y no compiten entre ellos, como se hacía en PoW. No necesitan extraer bloques; solo necesitan crear bloques cuando son elegidos y validar los bloques propuestos cuando no lo son. Esta validación se conoce como *attesting*. Se puede pensar como si se dijera "este bloque me parece bien". Los validadores obtienen recompensas por proponer nuevos bloques y dar fe de los que han visto. Eso sí, si se da fe de bloques maliciosos, pierde todo su monto bloqueado.

Beacon Chain [149]: Cuando Ethereum reemplace la prueba de trabajo por la prueba de participación, habrá una complejidad adicional debido al sharding. Estas son blockchains separadas que necesitarán validadores para procesar transacciones y crear nuevos bloques. El plan es tener 64 blockchains, cada una con una comprensión compartida del estado de la red. Como resultado, es necesaria una coordinación adicional y será realizada por la Beacon Chain.
La Beacon chain recibe información del estado de los *shards* y la pone a disposición de otros *shards*, lo que permite que la red se mantenga sincronizada. La Beacon Chain también gestionará a los validadores desde el registro de sus depósitos de participación hasta la emisión de sus recompensas y sanciones.

Cómo funciona la validación [150]

Cuando se envía una transacción en un fragmento, un validador será responsable de agregar su transacción a un bloque del shard. Los validadores son elegidos algorítmicamente por la Beacon Chain para proponer nuevos bloques.

Attestation

Si no se elige un validador para proponer un nuevo bloque del shard, tendrá que dar fe de la propuesta de otro validador y confirmar que todo se ve como debería. Es la *attestation* la que se registra en la Beacon Chain en lugar de la transacción en sí.

Se requieren al menos 128 validadores para dar fe de cada bloque de los shards; esto se conoce como un "comité".

El comité tiene un marco de tiempo para proponer y validar un bloque de fragmentos. Esto se conoce como "slot". Solo se crea un bloque válido por slot y hay 32 slots en una "epoch". Después de cada epoch, el comité se disuelve y se reforma con diferentes participantes aleatorios. Esto ayuda a mantener los shards a salvo de los comités constituidos por actores con malas intenciones.

Crosslinks

Una vez que una nueva propuesta de bloque de fragmentos tiene suficientes certificaciones, se crea un "crosslink" que confirma la inclusión del bloque y su transacción en la Beacon Chain.

Una vez que hay un crosslink, el validador que propuso el bloque obtiene su recompensa.

Finalidad

En las redes distribuidas, una transacción tiene una "finalidad" cuando es parte de un bloque que no puede ser cambiado.

Para hacer esto en la prueba de participación, Casper, un protocolo de finalidad, hace que los validadores acuerden el estado de un bloque en ciertos puntos de control. Siempre que 2/3 de los validadores estén de acuerdo, el bloque está finalizado. Los validadores perderán toda su participación si intentan revertir esto más adelante mediante un ataque del 51%. Esto es como un minero que participa en un ataque del 51%, lo que hace que su hardware de minería se queme de inmediato.

7.3.2 Sharding

Sharding es el futuro de la escalabilidad de Ethereum, y será clave para ayudar al ecosistema a soportar miles de transacciones por segundo y permitir que grandes porciones del mundo usen la plataforma regularmente a un coste asequible. Sin embargo, también es uno de los conceptos más incomprendidos en el ecosistema Ethereum y en los ecosistemas blockchain en general. Se refiere a un conjunto muy específico de ideas con propiedades muy específicas, pero a menudo se combina con técnicas que tienen propiedades de seguridad muy diferentes y, a menudo, mucho más débiles. El propósito de este apartado será explicar exactamente qué propiedades específicas proporciona el sharding.

“The scalability trilemma”

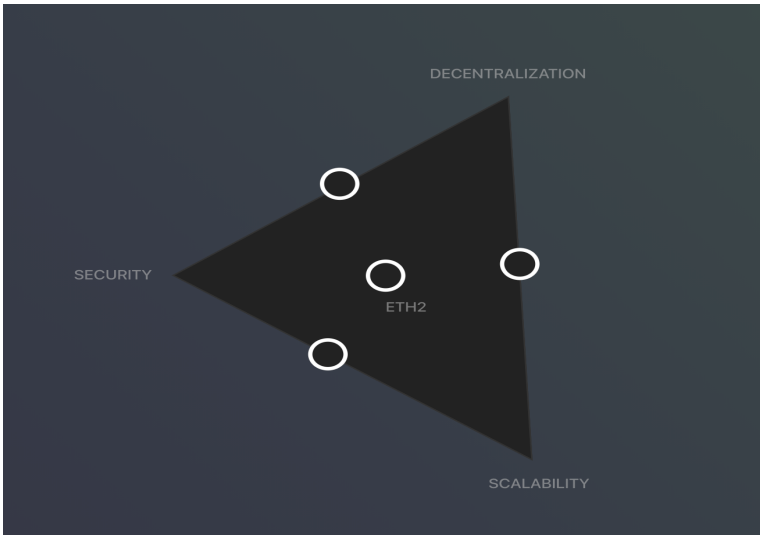

Ilustración 50. (2021). El reto de la escalabilidad descentralizada. Fuente: https://ethereum.org/en/eth2/vision/

The scalability trilemma [151], Ilustración 50, dice que hay tres propiedades que una blockchain intenta tener, y que, si te ciñes a técnicas "simples", solo puedes obtener dos de esas tres. Las tres propiedades son:

- **Escalabilidad**: la cadena puede procesar más transacciones de las que un solo nodo normal (piense: una computadora portátil de consumo) puede verificar.
- **Descentralización**: la cadena puede funcionar sin ninguna dependencia de confianza en un pequeño grupo de grandes actores centralizados. Por lo general, esto se interpreta en el sentido de que no debe haber ninguna confianza (o incluso suposición de mayoría honesta) de un conjunto de nodos a los que no puede unirse sólo con una computadora portátil normal.
- **Seguridad**: la cadena puede resistir un gran porcentaje de nodos participantes que intentan atacarla (idealmente el 50%; cualquier valor por encima del 25% está bien, el 5% definitivamente no está bien).

Ahora podemos ver las tres clases de "soluciones fáciles" que solo obtienen dos de las tres:

- **Blockchains tradicionales**, que incluyen Bitcoin, Ethereum 1.0, Litecoin y otras cadenas similares. Estos dependen de que cada participante ejecute un nodo completo que verifique cada transacción, por lo que tienen descentralización y seguridad, pero no escalabilidad.
- **Cadenas de alto TPS**, incluida la familia DPoS, pero también muchas otras. Estos se basan en una pequeña cantidad de nodos (a menudo de 10 a 100) que mantienen el consenso entre ellos, y los usuarios tienen que confiar en la mayoría de estos nodos. Esto es escalable y seguro (usando las definiciones anteriores), pero no está descentralizado.
- **Ecosistemas multi-chain**: esto se refiere al concepto general de "escalado horizontal" al tener diferentes aplicaciones viviendo en diferentes cadenas y

utilizando protocolos de comunicación entre cadenas para hablar entre ellas. Esto es descentralizado y escalable, pero no es seguro, porque un atacante sólo necesita obtener una mayoría de nodo de consenso en una de las muchas cadenas (a menudo <1% de todo el ecosistema) para romper esa cadena y posiblemente causar efectos dominó que causan gran daño a aplicaciones en otras cadenas.

Sharding es una técnica que te permite usar las tres. Una *sharded blockchain* es [152]:

- **Escalable**: puede procesar muchas más transacciones que un solo nodo
- **Descentralizada**: puede sobrevivir por completo en los ordenadores portátiles de los usuarios, sin depender de "supernodos" en absoluto
- **Seguro**: un atacante no puede apuntar a una pequeña parte del sistema con una pequeña cantidad de recursos; solo pueden intentar dominar y atacar todo el conjunto.

El resto del texto describirá cómo las sharded blockchains logran hacer esto [154].
La versión más fácil de comprender el sharding es mediante el sharding de muestreo aleatorio. El sharding mediante muestreo aleatorio tiene propiedades de confianza más débiles que las formas de sharding que se estan desarrollando en el ecosistema Ethereum, pero utiliza una tecnología más simple.
La idea central es la siguiente. Suponga que tiene una cadena PoS con un gran número (por ejemplo, 10000) validadores y tiene un gran número (por ejemplo, 100) bloques que deben verificarse. Ningún ordenador es lo suficientemente poderoso para validar *todos* estos bloques antes de que entre el siguiente conjunto de bloques.
Por lo tanto, lo que hacemos es dividir aleatoriamente el trabajo de hacer la verificación. Mezclamos aleatoriamente la lista de validadores, y asignamos a los primeros 100 validadores en la lista mezclada la tarea de verificar el primer bloque, los segundos 100 validadores en la lista mezclada verificar el segundo bloque, etc. Un grupo de validadores seleccionados al azar que le asigna verificar un bloque (o realizar alguna otra tarea) se llama comité [154], un ejemplo ilustrativo perfecto sería el de la Ilustración 51.

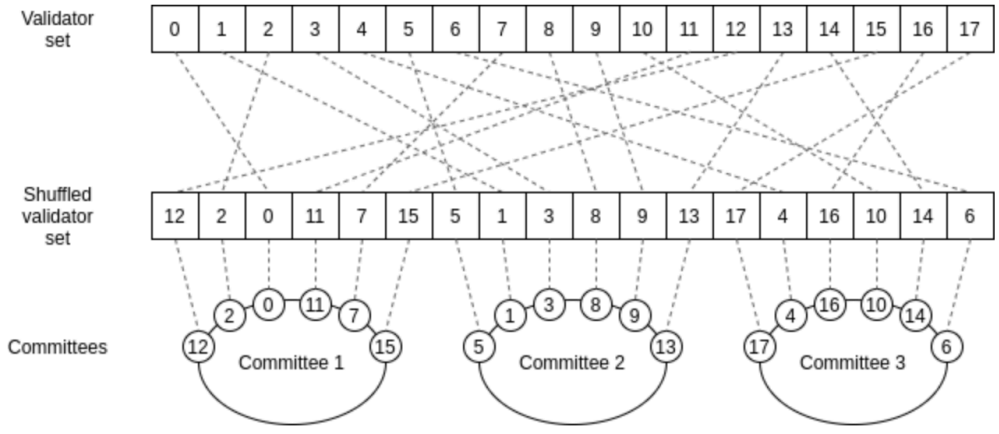

Ilustración 51. (2021). ELI5: randomly sampled committes. Fuente: hackmd.io/@vbuterin/sharding_proposal

Cuando un validador verifica un bloque, publica una firma que da fe de que lo hizo. Todos los demás, en lugar de verificar 100 bloques completos, ahora solo verifican 10000 firmas, una cantidad de trabajo mucho menor, especialmente con la agregación de firmas BLS. En lugar de que cada bloque se transmita a través de la misma red P2P, cada bloque se transmite en una subred diferente, y los nodos solo necesitan unirse a las subredes correspondientes a los bloques de los que son responsables (o están interesados por otras razones) [155].

Considere lo que sucede si la potencia de cálculo de cada nodo aumenta en 2x. Debido a que cada nodo ahora puede validar de manera segura 2 veces más firmas, puede reducir el tamaño mínimo del depósito de *staking* para admitir 2 veces más validadores, y por lo tanto puede crear 200 comités en lugar de 100. Por lo tanto, puede verificar 200 bloques en lugar de 100. Además, cada bloque individual podría ser 2 veces más grande. Por lo tanto, tiene 2 veces más bloques de 2 veces el tamaño o 4 veces más capacidad de cadena en total.

Se puede introducir un poco de notación matemática para hablar sobre lo que está sucediendo. Usando la notación Big O, usamos "O (B)" para referirnos a la capacidad computacional de un solo nodo. Una blockchain tradicional puede procesar bloques de tamaño O (B). Un *sharded chain* como se describe anteriormente puede procesar bloques O (B) en paralelo (recuerde, el costo para cada nodo para verificar cada bloque indirectamente es O (1) porque cada nodo sólo necesita verificar un número fijo de firmas), y cada bloque tiene capacidad O (B), por lo que la capacidad total de la *sharded chain* es O (B^2). Es por eso por lo que llamamos a este tipo de sharding, sharding cuadrático [156], y este efecto es una razón clave por el que se piensa que, a largo plazo, el sharding es la mejor manera de escalar una cadena de bloques.

Idealmente, se quiere tener una forma de sharding que evite las suposiciones de validez del 51% y preserve el poderoso baluarte de seguridad que las blockchains tradicionales obtienen de la verificación completa. Y esto es exactamente de lo que se ha tratado gran parte de la investigación de la organización Ethereum durante los últimos años.

7.4 Características Ethereum 2.0

Ethereum 2.0 deberá de cumplir ciertos parámetros que vayan acorde con los objetivos principales del proyecto. Esta serie de características que va a tener este protocolo se expondrán a continuación [157], para ello se explicará el motivo de su relevancia cuando todos estos atributos estén interconectados entre sí, haciendo de Ethereum 2.0, por mucho, el cambio más ambicioso y radical que se implementará en la red y con el requerimiento de varios años para implementarlo por completo.

Ethereum 2.0 deberá ser:

Escalable

Ethereum necesita poder hacer frente a más transacciones por segundo sin incrementar el tamaño de los nodos en la red. Los nodos son los participantes imprescindibles de la red que almacenan y ejecutan la blockchain. Aumentar el tamaño del nodo no es práctico porque sólo aquellos con ordenadores potentes y costosos podrían hacerlo. Para escalar, Ethereum necesita más transacciones por segundo, junto con más nodos, porque más nodos significa más seguridad.
Los shards permitirán que se distribuya la carga de la red entre 64 nuevas cadenas. Esto permitirá a Ethereum ganar espacio para reducir la congestión y mejorar las velocidades más allá del límite actual entre 15-20.
Y aunque habrá más cadenas, esto en realidad requerirá menos trabajo de los validadores, los que se encargan de mantener la red. Los validadores solo necesitarán 'ejecutar' su shard y no toda la cadena de Ethereum. Esto hace que los nodos sean más livianos, lo que permite que Ethereum escale y permanezca descentralizado.

Seguro

Las actualizaciones de Eth2 mejoran la seguridad de Ethereum contra ataques coordinados, como el ataque del 51%. Este es un tipo de ataque en el que, si alguien controla la mayor parte de la red, puede forzar cambios fraudulentos.
La transición a la prueba de participación (proof of stake) significa que el protocolo Ethereum tiene ciertos desincentivos contra los ataques. Esto se debe a que, en Proof of Stake, los validadores que aseguran la red deben apostar cantidades significativas de ETH en el protocolo. Si intentan atacar la red, el protocolo puede destruir automáticamente sus Ether.
Esto no es posible en la prueba de trabajo (Proof of Work), donde lo mejor que puede hacer un protocolo es obligar a las entidades que aseguran la red (los mineros) a perder las recompensas mineras que de otro modo habrían ganado. Para lograr el efecto equivalente en la PoW, el protocolo tendría que poder destruir todo el equipo de un minero si intentan hacer trampa.
El modelo de seguridad de Ethereum también debe cambiar debido a la introducción de los shards. Beacon Chain asignará validadores aleatoriamente a los diferentes shards; esto hace que sea prácticamente imposible que los validadores se unan para atacar a un shard específico. El sharding no es tan seguro en una blockchain de PoW, porque los mineros no pueden ser controlados por el protocolo de esta manera.
Staking también implica que no sea necesario invertir en hardware costoso para 'ejecutar' un nodo Ethereum. Esto debería alentar a las personas que cumplan unos requisitos mínimos a convertirse en validadores, aumentando la descentralización de la red y disminuyendo el área de superficie de ataque.
Un usuario puede convertirse en validador bloqueando sus Ether en un contrato inteligente. Más adelante se explicará cómo.

Sostenible

Ethereum necesita colaborar más con el medio ambiente
No es ninguna novedad que estas redes blockchain consuman grandes cantidades de energía debido a la minería que conlleva la PoW. Para conseguir dicho objetivo se ha escogido el algoritmo de prueba de participación (proof of stake).

El staking fue introducido en Ethereum por la Beacon Chain. La red Ethereum que usamos hoy se ejecutará en paralelo durante un período de tiempo, antes de que se 'fusione' o se 'acople' con las actualizaciones de Eth2. Este nuevo sistema estará asegurado por ETH, el otro por poder de cómputo. Esto se debe a que, al principio, los shards no podrán manejar cosas como las cuentas o dapps. Así que no se podrá olvidar la minería y la red principal.
Una vez que la Beacon Chain y las actualizaciones los shards estén en funcionamiento, se comenzará a trabajar para acoplar la red principal con el nuevo sistema. Esto convertirá la red principal en un shard que esté protegido por ETH y requiera mucha menos energía.

Se han estipulado 5 características que deberá alcanzar Ethereum 2.0 cuando finalice todas sus fases:

- **Descentralización**: Permitir que un ordenador portátil de consumo típico con recursos limitados procese / valide shards (incluida cualquier validación a nivel del sistema, como la Beacon Chain).
- **Resiliencia**: Permanecer activo a través de las principales particiones de red y cuando una gran parte de los nodos se desconectan.
- **Seguridad**: Utilizar técnicas criptográficas y de diseño que permitan una gran participación de validadores en total por unidad de tiempo.
- **Sencillez**: Minimizar la complejidad, incluso a costa de algunas pérdidas de eficiencia.
- **Longevidad**: Seleccionar todos los componentes de manera que sean seguros cuánticamente o puedan intercambiarse fácilmente por contrapartes de seguridad cuántica cuando estén disponibles y que se pueda realizar actualizaciones con más facilidad.

8. Conclusión

En este último apartado queremos desarrollar la conclusión personal de este trabajo y de que forma vemos el pasado, presente y el futuro que van a tener que afrontar los proyectos de DeFi, además de exponer las percepciones que como usuarios e inversores hemos abstraído al cabo de los años. Para empezar, nos gustaría aclarar que con la evidencia que se ha presentado anteriormente, la blockchain puede ayudar a conseguir la privacidad que no se tiene en la sociedad actual y la privacidad es uno de los fundamentos de una sociedad libre. Este activo puede ser creado bajo el control de los ciudadanos y donde pueden gestionar nuestra identidad de forma responsable.

En este trabajo se han explicado las raíces del mundo DeFi y el suelo en el que está construido (Ethereum). Los primeros proyectos en atraer a todos los usuarios fueron los que se han nombrado en este trabajo, Uniswap, Compound y Maker, que hoy en día siguen siendo las plataformas más utilizadas. Además, se ha explicado los principios y los principales conceptos de Ethereum y su predecesor, Ethereum 2.0. Se ha pensado, que no se podían explicar los proyectos sin hablar sobre el entorno en el que están ejecutados y el futuro de este. Porque si Ethereum se termina, DeFi probablemente también.

En este proyecto hemos conseguido concentrar una gran cantidad de información para que los lectores puedan acercarse al innovador mundo de la blockchain y de las criptomonedas. Este sector está en constante crecimiento, por lo que la información básica poco a poco se está quedando atrás debido a la cantidad de proyectos nuevos que salen día tras día. Además, hemos intentado traer información abstraída de la experiencia y de referencias de elevada calidad académica, para que cualquier detalle que se hable en este documento esté justificado por personas de elevada influencia en este sector. En este trabajo se descubrirá: qué es DeFi y sus diferencias con las finanzas tradicionales, qué es Ethereum y su función en DeFi, casos de uso de la vida real de DeFi y cómo también puede sacar provecho de las oportunidades dentro del espacio. Con estas explicaciones y guías concisas, pensamos que en muy pocas ocasiones ha sido más fácil para el lector comprender y comenzar con las diversas aplicaciones DeFi.
Trabajos como este son de vital importancia para las criptomonedas y para la blockchain, porque muchas personas son reticentes al riesgo que han escuchado que estas conllevan, pero la blockchain y sus aplicaciones van mucho más allá de eso. Con este documento, se busca que las personas vayan entrando en contacto con lo que posiblemente sea el futuro de diversas aplicaciones y rompan esa barrera de únicamente utilizar las finanzas tradicionales; que apoyen a la innovación tecnológica porque para lo único que ha venido es para mejorarnos las vidas. La captación de nuevos usuarios y futuros desarrolladores puede resultar en nuevos y apasionantes proyectos que mejoren la vida de muchas personas.

Hemos aplicado una gran cantidad de conceptos que sin la formación universitaria no hubiera sido posible. Gracias a la gran visión tecnológica que nos ha aportado estos 4 años de grado, hemos sido capaces de sintetizar y abstraer numerosa información de otros importantes trabajos con ideas especialmente técnicas y de gran complejidad.

Problemas de optimización aplicados al aumento de retornos sobre el capital, lectura de código, entendimiento de las funciones programadas de los contratos inteligentes y de la tecnología en la cual estos contratos están basados, poder tener una conversación sobre informática avanzada con desarrolladores de la blockchain, lectura de documentos complejos de alta repercusión en el sector etc. Se nos ocurren inumerables aplicaciones que debido al grado cursado hemos sido capaces de llevar a cabo, por no hablar de la gran cantidad de veces que gracias a la lectura del código de las aplicaciones y de sus funciones programadas, nos hemos salvado de que programadores con malas intenciones nos roben nuestros fondos, no solo a nosotros, sino a otros usuarios. Las bases sobre los conocimientos que se puedan adquirir posteriormente sobre DeFi ya estarán asentadas después de leer esto. Por ello, este trabajo puede ser una gran inspiración a trabajos futuros sobre este tema, porque como las bases ya estarán explicadas, podrán adentrarse en temas más específicos que sean de su interés. Porque en verdad, por cada plataforma que se ha explicado aquí, se podría hacer un trabajo de fin de grado, ya que, por ejemplo, cada Exchange descentralizado es diferente entre sí y cada uno tiene una serie de normas diferentes y características distintas; por lo tanto, este trabajo se ha visto limitado por la longitud de este documento y su posterior exposición.

El principal objetivo de este trabajo era reducir toda la información que hemos adquirido y que se presenta en internet, comprimirla de la forma mas sencilla posible y transmitirla a otras personas, para que de esta forma puedan saber las bases en las que se sustentan las Finanzas Descentralizadas. Porque, aunque no se haya hablado de todos los aspectos que conllevan estos proyectos ni de todos los proyectos que hay en el panorama, se han explicado los cimientos, los inicios y principios; entendiendo esto, se puede empezar a indagar en todos los demás proyectos adquiriendo cada vez más conocimientos sobre el tema. Pero, nos gustaría finalizar con la siguiente reflexión.

Consideramos que muchos proyectos DeFi se sustentan debido a que los usuarios bloquean, intercambian y prestan stablecoins entre ellos. Esto sucede porque en este punto los proyectos reparten incentivos por agregar liquidez a sus proyectos. Este pago proviene de los tokens de gobernanza. Son regalados a los usuarios de la plataforma por apoyarla y de un día para otro tendrán grandes valoraciones de mercado. Pero no se puede gastar valoraciones, por lo que realmente el dinero proviene de la gente que compra los tokens de gobernanza de ese proyecto y el motivo por el que lo compran es porque su TVL es alto. Así es el ciclo, Incentivos por liquidez -> TVL alto -> Valoraciones altas -> Grandes incentivos -> TVL sube más.
Es un ciclo de feedback positivo, empezando de no tener nada, llegar a crear billones de dólares en volumen, activos bloqueados y gran valuación del proyecto.
El problema es que este proceso no está creando ningún tipo de ganancia o valor para los usuarios (independientemente del precio pagado por los tokens de gobernanza). Pero esto puede acabar bien o mal, porque no sabemos si es un plan de marketing sublime con un crecimiento brillante o es humo y espejos

En el mundo de las criptomonedas ha habido proyectos que han tenido precios desorbitados, billones de dólares al día, incentivos gratis… Pero cuando todo se viene abajo, todos los malos aspectos del proyecto salen a la luz y los usuarios se quedan

sin nada, en realidad, menos que nada. 0 valor, volumen falso y activos por valor ridículo. Ha habido proyectos que hacían esto y de un día para otro dejaron de hacerlo, aunque su precio cayera, sabían que el precio que iban a tener iba a ser real. Después de todo esto, estos proyectos empezaron a construir, lanzaron más funcionalidades, mejoraron su tecnología y colaboraron con más proyectos para aportar valor. Sucedió lo evidente, mucha gente empezó a querer trabajar con ellos, es lo que sucede cuando escoges a buenos equipos para trabajar. El proyecto A se transformó en el proyecto B, empezaron desde el mismo sitio, uno no existe y el otro está en constante crecimiento.
DeFi está enfrentándose a este tipo de situaciones, el crecimiento ha sido debido al marketing y a humo. Si se termina con este tipo de situaciones desfavorables se podrá empezar el camino hacia las finanzas descentralizadas, para llegar allí, es esencial construir buenos productos y tener una actitud muy positiva hacia ellos.
Con todo esto se quiere expresar que porque una persona haya hecho un buen marketing no significa que haya sustancia más allá de eso.

El corazón de DeFi es ser descentralizado y *trustless*. Pero la centralización es normalmente más eficiente y para muchos proyectos DeFi el coste de la descentralización ha sido un mal producto para vender. Pero, por ejemplo, los Atomic Swaps (ambas partes depositan fondos en un smart contract y una vez depositado y que ambas partes hayan aceptado el intercambio, se envía automáticamente lo que hayan comprado), ha sido una de las mejores cosas que se han implementado en la blockchain que favorezca a las DeFi. Se puede hacer esto a través de smart contracts preprogramados para que hagan lo que necesites sin intermediarios que puedan suponer una molestia. Compound y Aave, entre otras, funcionan a la perfección y son muy buenos productos para el ecosistema DeFi.
Pero, las stablecoins en DeFi son una idea incompleta. El problema en realidad es que esa stablecoin funciona como un dólar y los dólares no están en la blockchain, en cambio, están centralizados en los bancos. Es decir, que, si solo tuviéramos la blockchain, no podríamos tener 1$.

El problema que DeFi está intentando resolver es este. Diferentes proyectos están intentando crear modelos híbridos, intercambios de stablecoin:stablecoin, sin tarifas y sin límites. Pero todo requiere a los bancos, si no se permitieran los elementos centralizados se estaría únicamente con intercambios de por ejemplo USDT y USDC, que de todos modos necesitan de mecanismos externos para mantenerlos en línea y para proveer liquidez.
Al final terminamos hablando de DAI, que su funcionalidad es clara y dudosa al mismo tiempo. El DAI no está respaldado por los dólares, de hecho, no lo puedes crear, solo lo puedes pedir prestado. Entonces su vinculación al dólar es muy débil, porque está respaldado por los préstamos y el apalancamiento, por lo tanto, si el mercado se mueve pueden terminar los titulares de estas monedas liquidados.
Las stablecoins son sólo un ejemplo, los problemas de la centralización y la usabilidad están por todo el sector.
Muchos proyectos DeFi necesitan el feedback de los precios del mercado, por eso usan oracles, es decir, que no es extremadamente descentralizado, es propenso a tener fallos centralizados o problemas respecto a las API. Pero, incidiendo más en la

blockchain, una de las formas para hacer la red más rápida y barata es haciéndola centralizada, pero esto se termina en las DeFi.

Para terminar, creemos que las soluciones para esto no son obvias, pero eso no significa que no haya y que no vayan a haber. Hay poderosos procesos para crear una solución y redes que ganan velocidad sin sacrificar la velocidad. Y hay formas de acercarse a las monedas estables que, aunque no son perfectas, al menos hacer algo mejor que DAI y menos centralizado que USDC. Para que DeFi crezca, tendrá que presentar un caso convincente de que la falta de trustless justifique la molestia que causa debido a los problemas que presenta. Eso significa encontrar la eficiencia de pareto, hacer las mejores compensaciones posibles y continuar encontrando formas de desarrollar el poder del ecosistema DeFi sin sacrificar sus principios básicos.
En gran medida, este es el precio que se paga por la descentralización. Si no se desea que un solo país controle una base de datos, al menos se debe esperar a que la luz viaje entre los nodos. Los exchanges descentralizados son importantes, pero en comparación con un exchange centralizado, son torpes, lentos y costosos, porque en comparación con un servidor de Microsoft, la blockchain Ethereum es torpe, lenta y costosa, pero descentralizada. A medida que se le presta más atención a DeFi, se ha utilizado más, pero ha tenido problemas con su escalabilidad.
Esto realmente limita el crecimiento. Pero hay noticias buenas, proyectos como Polkadot y Kusama, Ethereum 2.0, Solana, Cosmos etc., van a terminar con estos problemas.

Bibliografía

[1] Companiesmarketcap. (2020). *Largest banks by market cap*. Companies ranked by Market Cap: https://companiesmarketcap.com/banks/largest-banks-by-market-cap/

[2] CoinMarketCap. (2021). *Global Cryptocurrency Charts*. CoinMarketCap: https://coinmarketcap.com/charts/

[3] Companiesmarketcap. (2020). *Largest banks by market cap*. Companies ranked by Market Cap: https://companiesmarketcap.com/banks/largest-banks-by-market-cap/

[4] Stevens, R. (2017). *¿Qué son y a qué se dedican los bancos?* Rankia: https://www.rankia.co/blog/mejores-cdts/3699075-que-son-dedican-bancos

[5] Dalio, R. (2012). How the economic machine works. Economic Principles: https://economicprinciples.org/downloads/ray_dalio__how_the_economic_machine_works__leveragings_and_deleveragings.pdf

[6] Murphy, A. (2008). An analysis of the financial crisis of 2008: causes and solutions. *An Analysis of the Financial Crisis of 2008*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1295344

[7] Boehlke, J. (2017). *How Long Does It Take to Have a Payment Post Online to Your*. GOBankingRates: https://www.gobankingrates.com/banking/checking-account/how-long-payment-posted-online-account/

[8] Facilities, S. & VGNG. (2020). *SolanaBeach*. Solana: https://solana.com/

[9] World Bank Group. (2017). *The unbanked*. The World Bank: https://globalfindex.worldbank.org/chapters/unbanked

[10] Cornish, L. (2018). *Insights from the World Bank's 2017 Global Findex database*. Obtenido de Devex: https://www.devex.com/news/insights-from-the-world-bank-s-2017-global-findex-database-92589

[11] Office of the Comptroller of Currency. (2008). *Washington Mutual Acquired by JPMorgan Chase*. Office of the Comptroller of Currency: https://occ.gov/static/ots/press-releases/ots-pr-2008-46.pdf

[12] Yale School of Management. (2014). *The Lehman Brothers Bankruptcy A: Overview.* Yale School of Management: http://som.yale.edu/sites/default/files/files/001-2014-3A-V1-LehmanBrothers-A-REVA.pdf

[13] Corporation, F. D. (2000). *Failed Bank List*. FDIC: https://www.fdic.gov/resources/resolutions/bank-failures/failed-bank-list/

[14] Financial Crisis Inquiry Commission. (2011). *The financial crisis inquiry report: The final report of the National Commission on the causes of the financial and economic crisis in the United States including dissenting views*. Cosimo, Inc.: https://www.govinfo.gov/content/pkg/GPO-FCIC/pdf/GPO-FCIC.pdf

[15] Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*, *58*(4), 102584: https://www.sciencedirect.com/science/article/pii/S0306457321000844

[16] Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance (DeFi). *IIEL Issue Brief*, *2*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=%203539194

[17] Metcalfe, W. (2020). Ethereum, Smart Contracts, DApps. In *Blockchain and Crypt Currency* (pp. 77-93). Springer, Singapore: https://library.oapen.org/bitstream/handle/20.500.12657/37713/2020_Book_BlockchainAndCryptCurrency.pdf?sequence=1#page=88

[18] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf

[19] Antonopoulos, A. M., & Wood, G. (2018). *Mastering ethereum: building smart contracts and dapps*. O'reilly Media: https://books.google.es/books?hl=en&lr=&id=nJJ5DwAAQBAJ&oi=fnd&pg=PR4&dq=mart+contracts+ethereum&ots=uBIKanKXxM&sig=K_GnJlpdjxIlGfxjyH_YoY95Zis&redi_esc=y#v=onepage&q=smart%20contracts%20ethereum&f=false

[20] CoinMarketCap. (2020). *What Is Total Value Locked (TVL)?*. CoinMarketCap: https://coinmarketcap.com/alexandria/glossary/total-value-locked-tvl

[21] Defipulse. (s.f.). *Total Value Locked in DeFi*. DEFI PULSE: https://defipulse.com/

[22] Kistner, J. *How Decentralized is DeFi? A Framework for Classifying Lending Protocols* [en línea]. Hackernoon: https://hackernoon.com/how-decentralized-is-defi-a-framework-for-classifying-lending-protocols-90981f2c007f

[23] Redman, J. (2018). *The Difference Between Custodial and Noncustodial Cryptocurrency Services*. Obtenido de Bitcoin.com: https://news.bitcoin.com/the-difference-between-custodial-and-noncustodial-cryptocurrency-services/

[24] Kiziryan, M. (2018). *Tipo de Interés*. Obtenido de Economipedia: https://economipedia.com/definiciones/tipo-de-interes.html

[25] Chohan, U. W. (2019). Are stable coins stable?. *Notes on the 21st Century (CBRi)*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326823

[26] Lipton, A., Sardon, A., Schär, F., & Schüpbach, C. (2020). 11. Stablecoins, Digital Currency, and the Future of Money. In *Building the New Economy*. PubPub: https://wip.mitpress.mit.edu/pub/17h9tjq7/release/4

[27] Bbva. (2021). *Tipos de préstamos, cuáles son sus características*. Obtenido de Bbva: https://www.bbva.es/finanzas-vistazo/ef/prestamos/tipos-de-prestamos.html

[28] Bartoletti, M., Chiang, J. H. Y., & Lluch-Lafuente, A. (2020). SoK: Lending Pools in Decentralized Finance. *arXiv preprint arXiv:2012.13230*: https://arxiv.org/abs/2012.13230

[29] Institute, C. F. (2020). *Cryptocurrencies Exchanges*. Obtenido de Corporate Finance Institute: https://corporatefinanceinstitute.com/resources/knowledge/other/cryptocurrency-exchanges/

[30] Stulz, R. M. (2005). Financial derivatives. *The Milken Institute Review*, 20-31: https://cpb-us-w2.wpmucdn.com/u.osu.edu/dist/0/30211/files/2019/07/Demystifying-Financial-Derivatives.pdf

[31] Chohan, U. W. (2017). The double spending problem and cryptocurrencies. *Available at SSRN 3090174*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

[32] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260: https://bitcoin.org/bitcoin.pdf

[33] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32: https://ethereum.github.io/yellowpaper/paper.pdf

[34] Buterin, V. (2016). Ethereum: Platform Review. *Opportunities and Challenges for Private and Consortium Blockchains*: http://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-and-Challenges-for-Private-and-Consortium-Blockchains.pdf

[35] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37): https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[36] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32: https://ethereum.github.io/yellowpaper/paper.pdf

[37] Cohen, D. (2018). Merkle trees and blockchains: https://www.cs.tau.ac.il/~msagiv/courses/blockchain/merkel.pdf

[38] Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*: https://arxiv.org/abs/1710.06372

[39] Ethereum. (2016). *Account Types, Gas and Transactions. Ethereum Homestead* Documentation: https://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#eoa-vs-contract-accounts

[40] Wesley. (2016). *Introduction to Smart Contracts*. Ethereum: https://ethereum.org/en/developers/docs/smart-contracts/

[41] Bins, W. (2018). *Smart Contracts and Solidity*. Obtenido de Github: https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc#evm_chapter

[42] Chriseth. (2016). Introduction to Smart Contracts. Solidity: https://docs.soliditylang.org/en/v0.4.21/introduction-to-smart-contracts.html

[43] Solidity. (2016). *Contracts*. Solidity: https://docs.soliditylang.org/en/v0.5.3/contracts.html

[44] Ethereum. (2018). What is Ether?. Ethereum: https://ethereum.org/en/eth/

[45] Ziechmann, K. (2012). *Ethereum Virtual Machine (EVM)*. Ethereum: https://ethereum.org/es/developers/docs/evm/

[46] Takenobu T. (2018). Ethereum EVM illustrated. Github: https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf

[47] LOOPA. (2016). Paradigmas de programación: Programación imperativa y programación declarativa. Medium: https://medium.com/@Loopa/paradigmas-de-programaci%C3%B3n-programaci%C3%B3n-imperativa-y-programaci%C3%B3n-declarativa-4c4a4182fd87

[48] Dannen, C. (2019). Introducing Ethereum and Solidity: https://books.google.es/books?hl=en&lr=&id=H99YDwAAQBAJ&oi=fnd&pg=PP1&dq=solidity+ethereum&ots=nKt9f4UH4D&sig=fHcJ8ZypcJAiazyv0iWwZE7ntH4&redir_esc=y#v=onepage&q=solidity%20ethereum&f=false

[49] TxStreet Ethereum. (2016). *Ethereum Gas Fees*. TxStreet: https://txstreet.com/v/eth

[50] Rosic, A. (2020). *What is Ethereum Gas?* Blockgeeks: https://blockgeeks.com/guides/ethereum-gas/

[51] Ethereum. (2016). *Account Types, Gas and Transactions. Ethereum Homestead* Documentation: https://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#eoa-vs-contract-accounts

[52] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37): https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[53] Chohan, U. W. (2017). The decentralized autonomous organization and governance issues. *Available at SSRN 3082055*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055

[54] CoinMarketCap. (2018). *Top Stablecoin Tokens by Market Capitalization*. CoinMarketCap: https://coinmarketcap.com/view/stablecoin/

[55] ConsenSys. (2019). The State of Stablecoin 2019. ConsenSys: https://consensys.net/blog/news/the-state-of-stablecoins-2019/

[56] Zhao, W., Li, H., & Yuan, Y. (2021). Understand Volatility of Algorithmic Stablecoin: Modeling, Verification and Empirical Analysis. *arXiv preprint arXiv:2101.08423*: https://arxiv.org/abs/2101.08423

[57] Tether. (2021). Digital money for a digital age. Tether: https://tether.to/

[58] Circle. (2018). USDC: The world's leading digital dollar stablecoin. Circle: https://www.circle.com/en/usdc

[59] Berentsen, A., & Schär, F. (2019). Stablecoins: The quest for a low-volatility cryptocurrency. *Fatas A.(a cura di), Economics of Fintech and Digital Currencies*, 65-71: https://www.researchgate.net/publication/332464789_Stablecoins_The_quest_for_a_low-_volatility_cryptocurrency

[60] Maker. (2016). MakerDAO Documentation. Maker: https://docs.makerdao.com/

[61] Maker. (2016). MakerDAO Documentation. Maker: https://docs.makerdao.com/

[62] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/whitepaper/White%20Paper%20-The%20Maker%20Protocol_%20MakerDAO%E2%80%99s%20Multi-Collateral%20Dai%20(MCD)%20System-FINAL-%20021720.pdf

[63] Maker. (2016). Smart Contract Modules. Maker: https://docs.makerdao.com/

[64] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/whitepaper/White%20Paper%20-The%20Maker%20Protocol_%20MakerDAO%E2%80%99s%20Multi-Collateral%20Dai%20(MCD)%20System-FINAL-%20021720.pdf

[65] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/whitepaper/White%20Paper%20-The%20Maker%20Protocol_%20MakerDAO%E2%80%99s%20Multi-Collateral%20Dai%20(MCD)%20System-FINAL-%20021720.pdf

[66] MakerDAO. (2021). Dai Savings Rate. MakerDAO: https://community-development.makerdao.com/en/learn/Dai/dsr

[67] MakerDAO. (2021). Vaults. MakerDAO: https://community-development.makerdao.com/en/learn/vaults

[68] MakerDAO. (2021). Vaults. MakerDAO: https://community-development.makerdao.com/en/learn/vaults

[69] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/en/whitepaper#abstract

[70] MakerDAO. (2021). Keepers. MakerDAO: https://docs.makerdao.com/keepers/auction-keepers

[71] MakerDAO. (2021). Liquidation. MakerDAO: https://community-development.makerdao.com/en/learn/vaults/liquidation/

[72] MakerDAO. (2021). Liquidation. MakerDAO: https://community-development.makerdao.com/en/learn/vaults/liquidation/

[73] MakerDAO. (2021). Dai Savings Rate. MakerDAO: https://community-development.makerdao.com/en/learn/Dai/dsr

[74] MakerDAO. (2021). Governance. MakerDAO: https://community-development.makerdao.com/en/learn/governance

[75] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/en/whitepaper#abstract

[76] MakerDAO. (2021). Governance. MakerDAO: https://community-development.makerdao.com/en/learn/governance

[77] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/en/whitepaper#abstract

[78] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/en/whitepaper#abstract

[79] MakerDAO. (2021). Governance. MakerDAO: https://community-development.makerdao.com/en/learn/governance

[80] MakerDAO. (2014). The Maker Protocol: MakerDAO's Multi-collateral Dai (MCD) System. Maker: https://makerdao.com/en/whitepaper#abstract

[81] Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. *arXiv preprint arXiv:2106.06389*: https://arxiv.org/pdf/2106.06389.pdf

[82] Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. *arXiv preprint arXiv:2106.06389*: https://arxiv.org/pdf/2106.06389.pdf

[83] Qin, K., Zhou, L., Gamito, P., Jovanovic, P., & Gervais, A. (2021). An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. *arXiv preprint arXiv:2106.06389*: https://arxiv.org/pdf/2106.06389.pdf

[84] Thompson, P. (2020). *Most Significant Hacks of 2019 – New Record of Twelve in One Year*. Cointelegraph: https://cointelegraph.com/news/most-significant-hacks-of-2019-new-record-of-twelve-in-one-year

[85] Young, J. E. (2020). On Equivalence of Automated Market Maker and Limit Order Book Systems: https://professorjey.com/assets/papers/AMM_Order_Book_Equivalence_DRAFT_2020_10_16.pdf

[86] Binance Academy. (2020). What are Liquidity Pools in DeFi and How Do They Work. Binance: https://academy.binance.com/en/articles/what-are-liquidity-pools-in-defi

[87] Lo, Y. C., & Medda, F. (2020). Uniswap and the rise of the decentralized exchange. *Available at SSRN 3715398*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3715398

[88] Wang, Y. (2020). Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*: https://arxiv.org/pdf/2009.01676.pdf

[89] Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2020). *Uniswap v2 core*. Tech. rep., Uniswap: https://uniswap.org/whitepaper.pdf

[90] Uniswap. (2020). Pools. Uniswap Docs: https://uniswap.org/docs/v2/core-concepts/pools/

[91] Uniswap. (2020). Fees. Uniswap Docs: https://uniswap.org/docs/v2/advanced-topics/fees

[92] Pourpouneh, M., Nielsen, K., & Ross, O. (2020). *Automated Market Makers* (No. 2020/08). IFRO Working Paper: https://www.econstor.eu/bitstream/10419/222424/1/IFRO_WP_2020_08.pdf

[93] Wang, Y. (2020). Automated market makers for decentralized finance (defi). *arXiv preprint arXiv:2009.01676*: https://arxiv.org/pdf/2009.01676.pdf

[94] Di Maggio, M. (2019). Survey of Automated Market Making Algorithms. Medium: https://medium.com/terra-money/survey-of-automated-market-making-algorithms-951f91ce727a

[95] Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2020). *Uniswap v2 core*. Tech. rep., Uniswap: https://uniswap.org/whitepaper.pdf

[96] Adams, H., Zinsmeister, N., Salem, M., Keefer, R., & Robinson, D. (2021). *Uniswap v3 core*. Tech. rep., Uniswap: https://uniswap.org/whitepaper-v3.pdf

[97] Dexe.network. (2020). What is Slipage and why does it matter? (Uniswap example). Medium: https://dexenetwork.medium.com/what-is-slippage-and-why-does-it-matter-uniswap-example-43e32d712651#:~:text=With%20Slippage%20Tolerance%2C%20you%20can,it%20to%20any%20%25%20you%20want.

[98] Torres, C. F., Camino, R., & State, R. (2021). Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain. *arXiv preprint arXiv:2102.03347*: https://arxiv.org/pdf/2102.03347.pdf

[99] Wang, Y., Chen, Y., Deng, S., & Wattenhofer, R. (2021). Cyclic Arbitrage in Decentralized Exchange Markets. *Available at SSRN 3834535*: https://arxiv.org/pdf/2105.02784.pdf

[100] Uniswap. (2020). Pools. Uniswap Docs: https://uniswap.org/docs/v2/core-concepts/pools/

[101] Uniswap. (2020). Fees. Uniswap Docs: https://uniswap.org/docs/v2/advanced-topics/fees

[102] Uniswap. (2020). Pools. Uniswap Docs: https://uniswap.org/docs/v2/core-concepts/pools/

[103] Maldonado, J. (2020). ¿Qué es una pérdida impermanente o impermanent loss?. Cointelegraph: https://es.cointelegraph.com/explained/what-is-an-impermanent-loss

[104] Chen, J. (2021). Know Your Client (KYC). Investopedia: https://www.investopedia.com/terms/k/knowyourclient.asp

[105] Leshner, R., & Hayes, G. (2019). Compound: The money market protocol. *White Paper*: https://compound.finance/documents/Compound.Whitepaper.pdf

[106] Leshner, R., & Hayes, G. (2019). Compound: The money market protocol. *White Paper*: https://compound.finance/documents/Compound.Whitepaper.pdf

[107] Ramos, D., & Zanko, G. (2020). A Review of the Current State of Decentralized Finance as a Subsector of the Cryptocurrency Market. *MobileyourLife. Available at https://www. mobileyourlife. com/research*: https://static1.squarespace.com/static/553d790de4b08ceb08ab88fd/t/5f5c2a4d381d4c58ce97cde2/1599875662625/DeFi_P2_SciPaper_3.pdf

[108] Compound. (2021). cTokens. Compound Docs: https://compound.finance/docs/ctokens

[109] Compound. (2021). cTokens. Compound Docs: https://compound.finance/docs/ctokens

[110] Leshner, R., & Hayes, G. (2019). Compound: The money market protocol. *White Paper*: https://compound.finance/documents/Compound.Whitepaper.pdf

[111] Compound. (2021). API. Compound Docs: https://compound.finance/docs/api

[112] Compound. (2021). API. Compound Docs: https://compound.finance/docs/api

[113] Compound. (2021). cTokens. Compound Docs: https://compound.finance/docs/ctokens

[114] Bavosa, A. (2020). Supplying Assets to the Compound Protocol. Medium: https://medium.com/compound-finance/supplying-assets-to-the-compound-protocol-ec2cf5df5aa

[115] Bavosa, A. (2020). Borrowing Assets from the Compound Protocol. Medium: https://medium.com/compound-finance/borrowing-assets-from-compound-quick-start-guide-f5e69af4b8f4

[116] Compound. (2021). cTokens. Compound Docs: https://compound.finance/docs/ctokens

[117] Compound. (2021). Open Price Feeds. Compound Docs: https://compound.finance/docs/prices

[118] Compound. (2021). Comptroller. Compound Docs: https://compound.finance/docs/comptroller

[119] Compound. (2021). Security. Compound Docs: https://compound.finance/docs/security

[120] Gauntlet. (2020). Market Risk Assessment. Compound: https://gauntlet.network/reports/compound

[121] Compound. (2021). Security. Compound Docs: https://compound.finance/docs/security

[122] Compound. (2021). Governance. Compound Docs: https://compound.finance/docs/governance

[123] Compound. (2021). Governance. Compound Docs: https://compound.finance/docs/governance

[124] Riady, Y. (2018). Signing and Verifying Ethereum Signatures. Yos Riady: https://yos.io/2018/11/16/ethereum-signatures/

[125] Yao, A. C. (1982). Theory and application of trapdoor functions. In *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)* (pp. 80-91). IEEE: https://ieeexplore.ieee.org/abstract/document/4568378

[126] Sullivan, N. (2013). A (Relatively Easy to Understand) Primer on Elliptic Curve Cryptography. Cloudflare: https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

[127] Dinur, I., Dunkelman, O., & Shamir, A. (2012). New attacks on Keccak-224 and Keccak-256. In *International Workshop on Fast Software Encryption* (pp. 442-461). Springer, Berlin, Heidelberg: https://link.springer.com/content/pdf/10.1007/978-3-642-34047-5_25.pdf

[128] Zuidhoorn, M. (2020). The Magic of Digital Signatures on Ethereum. Medium: https://medium.com/mycrypto/the-magic-of-digital-signatures-on-ethereum-98fe184dc9c7

[129] Zuidhoorn, M. (2020). The Magic of Digital Signatures on Ethereum. Medium: https://medium.com/mycrypto/the-magic-of-digital-signatures-on-ethereum-98fe184dc9c7

[130] Zuidhoorn, M. (2020). The Magic of Digital Signatures on Ethereum. Medium: https://medium.com/mycrypto/the-magic-of-digital-signatures-on-ethereum-98fe184dc9c7

[131] Remco, B., Logvinov, L., & Evans, J. (2017). EIP-712: Ethereum typed structured data hashing and signing. Ethereum Improvement Proposals: https://eips.ethereum.org/EIPS/eip-712

[132] Remco, B., Logvinov, L., & Evans, J. (2017). EIP-712: Ethereum typed structured data hashing and signing. Ethereum Improvement Proposals: https://eips.ethereum.org/EIPS/eip-712

[133] Compound. (2021). Governance. Compound Docs: https://compound.finance/docs/governance

[134] Compound. (2021). API. Compound Docs: https://compound.finance/docs/api

[135] Compound. (2021). API. Compound Docs: https://compound.finance/docs/api

[136] Chohan, U. W. (2021). Decentralized Finance (DeFi): An Emergent Alternative Financial Architecture. *Critical Blockchain Research Initiative (CBRI) Working Papers*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3791921

[137] Lichtigsteign, A. (2018). Web 3.0 Will Be Powered by Blockchain Technology Stack. Hackernoon: https://hackernoon.com/web-3-0-will-be-powered-by-blockchain-technology-stack-626ce3f828c7

[138] Kim, C. (2020). Confessions of a Sharding Skeptic. Coindesk: https://www.coindesk.com/sharding-eth-2-podcast

[139] Wackerow, P. (2021). Layer 2 Rollups. Ethereum: https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/

[140] Buterin, V. (2021). Shard chains. Ethereum: https://ethereum.org/en/eth2/shard-chains/

[141] Polkadot. (2021). Technology. Polkadot: https://polkadot.network/technology/

[142] Ethereum. (2021). The Eth2 Upgrades. Ethereum: https://ethereum.org/en/eth2/

[143] Prysmatic Labs. (2021). Architecture Overview. Prysm Eth2 Docs: https://docs.prylabs.network/docs/how-prysm-works/architecture-overview/#:~:text=As%20described%20in%20this%20section,known%20as%20a%20beacon%20chain.&text=Ethereum%202.0%20provides%20a%20massive,of%20the%20existing%20ETH1%20blockchain.

[144] Butta. (2021). Ethereum 2.0 Knowledge Base. Beaconcha: https://kb.beaconcha.in/glossary

[145] EthHub. (2019). Ethereum 2.0 Phases. EthHub: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-phases/

[146] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, *7*, 22328-22370: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8629877

[147] Moindrot, O., & Bournhonesque, C. (2017). Proof of stake made simple with casper. *ICME, Stanford University*: https://www.scs.stanford.edu/17au-cs244b/labs/projects/moindrot_bournhonesque.pdf

[148] Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*: https://arxiv.org/pdf/1710.09437.pdf?source=post_elevate_sequence_page----------

[149] Butta. (2021). Ethereum 2.0 Knowledge Base. Beaconcha: https://kb.beaconcha.in/glossary

[150] ETHOS.DEV. (2020). The Beacon Chain Ethereum 2.0 explainer you need to read first. Ethos.dev: https://ethos.dev/beacon-chain/

[151] Altarawneh, A., Herschberg, T., Medury, S., Kandah, F., & Skjellum, A. (2020, January). Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0727-0736). IEEE: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9031204

[152] Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (2018, July). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 122-128). IEEE: https://www.researchgate.net/profile/Tejinder-Singh-

Mor/publication/327000219_Blockchain_and_Scalability/links/5d414891a6fdcc370a6f1067/Blockchain-and-Scalability.pdf

[153] Buterin, V. (2020). An explanation of the sharding + DAS proposal. Hackmd: https://hackmd.io/@vbuterin/sharding_proposal

[154] Buterin, V. (2020). An explanation of the sharding + DAS proposal. Hackmd: https://hackmd.io/@vbuterin/sharding_proposal

[155] Buterin, V. (2020). An explanation of the sharding + DAS proposal. Hackmd: https://hackmd.io/@vbuterin/sharding_proposal

[156] Skidanov, A. (2018). The authoritative guide to Blockchain Sharding, part 1. Near: https://near.org/blog/the-authoritative-guide-to-blockchain-sharding-part-1/#:~:text=the%20quadratic%20sharding.-,Quadratic%20sharding,participating%20in%20the%20network%20operation.&text=The%20throughput%20across%20the%20system,thus%20the%20name%20quadratic%20sharding.

[157] Kim, C. (2020). Ethereum 2.0: HOW IT WORKS AND WHY IT MATTERS. Coindesk: https://www.coindesk.com/wp-content/uploads/2020/07/ETH-2.0-072120.pdf