

The background features a complex network of gold-colored lines and dots. Some lines are horizontal, some vertical, and some form right-angled paths. Scattered throughout are small currency symbols: the Euro (€), the Dollar (\$), and the Pound (£). The overall aesthetic is clean, modern, and financial.

# FINANZAS DESCENTRALIZADAS: LA NUEVA Y DEFINITIVA LIBERTAD ECONÓMICA

DESCUBRE POR QUÉ LAS FINANZAS  
DESCENTRALIZADAS (DEFI) REPRESENTAN  
LA MAYOR REVOLUCIÓN FINANCIERA DE LA  
HISTORIA Y CÓMO PUEDEN PERMITIRTE  
HACER CRECER TU DINERO

PEPE  
DÍAZ

DEUSTO

# **Finanzas descentralizadas: la nueva y definitiva libertad económica**

Descubre por qué las finanzas descentralizadas (DeFi) representan la mayor revolución financiera de la historia y cómo pueden permitirte hacer crecer tu dinero

**PEPE DÍAZ**



EDICIONES DEUSTO

© Pepe Díaz, 2023

© Prólogo de Isra Bravo

© Centro de Libros PAFP, SLU., 2023

Deusto es un sello editorial de Centro de Libros PAFP, SLU.

Av. Diagonal, 662-664

08034 Barcelona

[www.planetadelibros.com](http://www.planetadelibros.com)

Primera edición: enero de 2023

Depósito legal: B. 22.090-2022

ISBN: 978-84-234-3404-6

Preimpresión: Realización Planeta

Impreso por Huertas Industrias Gráficas, S. A.

Impreso en España - *Printed in Spain*

El papel utilizado para la impresión de este libro está calificado como papel ecológico y procede de bosques gestionados de manera sostenible.

La lectura abre horizontes, iguala oportunidades y construye una sociedad mejor.

La propiedad intelectual es clave en la creación de contenidos culturales porque sostiene el ecosistema de quienes escriben y de nuestras librerías.

Al comprar este libro estarás contribuyendo a mantener dicho ecosistema vivo y en crecimiento.

En Grupo Planeta agradecemos que nos ayudes a apoyar así la autonomía creativa de autoras y autores para que puedan seguir desempeñando su labor.

Dirígete a CEDRO (Centro Español de Derechos Reprográficos) si necesitas fotocopiar o escanear algún fragmento de esta obra. Puedes contactar con CEDRO a través de la web [www.conlicencia.com](http://www.conlicencia.com) o por teléfono en el 91 702 19 70 / 93 272 04 47.

# Sumario

---

Prólogo .....	9
Introducción .....	11
Regalo inesperado.....	17

## PARTE I

### Lo que no quieren que sepas

1. Blockchain y el negocio de la confianza .....	21
2. Cómo funciona una blockchain .....	27
3. La paradoja de la descentralización financiera .....	35
4. ¿Qué son las finanzas descentralizadas (DeFi)? .....	39
5. Las capas de DeFi .....	45
6. El trilema blockchain.....	49
7. Las estacas del abuelo Andrés.....	53
8. La importancia de los tokenomics en los proyectos cripto .	59
9. Banca sin bancos.....	67
10. <i>Stablecoins</i> : las responsables de la explosión de crecimiento de DeFi .....	75
11. Préstamos descentralizados .....	85
12. ¿Qué es un DEX y cómo puedes sacarle partido? .....	91
13. Liquidez: la gasolina necesaria para que el motor DeFi funcione .....	101

14. La capa de agregadores (o cómo ofrecer valor añadido al usuario) .....	105
15. Derivados financieros descentralizados .....	109
16. Diseña tu propio fondo indexado cripto .....	113
17. «Tokenizando», que es gerundio .....	115
18. ¿Qué es una DAO? .....	123
19. Los riesgos de las finanzas descentralizadas (DeFi) .....	129
20. Un pequeño alto en el camino .....	145

## PARTE 2

### Paso a paso

21. Kit de iniciación DeFi: las herramientas básicas que necesitarás .....	151
22. Claves privadas y claves públicas .....	153
23. Tipos de wallets .....	157
24. Tu primera compra de tokens cripto .....	163
25. La importancia de los tokens envueltos .....	169
26. Interoperabilidad entre blockchains .....	173
27. Ideas para crear tus propias estrategias DeFi .....	177
28. Diseñando tu primera cartera estratégica en DeFi .....	191

## PARTE 3

### Reflexiones

29. «DeFinitivamente», tu dinero merece (mucho) más .....	201
30. Probablemente pierdas todo tu dinero .....	203
31. Seguramente, tú elegirías también esa opción .....	209
32. Esto jamás me volverá a pasar .....	213
33. Punto y final .....	217

## **Blockchain y el negocio de la confianza**

Las instituciones financieras de las que hablábamos anteriormente se han beneficiado desde hace décadas de la obligación de hacer uso de terceros de confianza para llevar a cabo transacciones financieras de toda índole. Veamos con un ejemplo en qué consiste este negocio al que muchos llaman el «negocio de la confianza».

Imagina que quieres darle 1.000 euros a tu amigo Aitor. Si vives cerca, puedes quedar con él y entregarle los 1.000 euros en mano. Todo sencillo, anónimo y sin que nadie más que tú y tu amigo tenga que intervenir en la transmisión de valor. No hay terceros entremedias.

Pero los humanos tenemos la costumbre de no vivir siempre cerca de nuestros amigos. Quizá tú vives en Cuenca y tu amigo Aitor, en Bilbao; o, peor aún, tú vives en España y tu amigo, en el extranjero. La cosa se complica.

Para ayudarnos con esas complicaciones, en nuestro sistema financiero aparecen los llamados «terceros de confianza», que pueden ser bancos u otro tipo de entidades que facilitan que tú puedas hacerle llegar los 1.000 euros a tu amigo. A cambio, el intermediario se lleva una comisión..., y algo más: se lleva parte de tu libertad económica.

Es posible que ni te hayas dado cuenta, pero, para poder en-

viar ese dinero a tu amigo Aitor, has tenido que dar algunos pasos que han hecho que seas algo más preso del sistema. Y, efectivamente, cuanto más preso eres, menos libertad tienes.

Quizá te preguntes por qué eres menos libre al necesitar de los terceros de confianza en el sistema financiero tradicional. Te lo explico rápidamente. Lo primero de todo es que, para poder enviarle el dinero a tu amigo Aitor, tuviste que abrir cuenta en un banco. Pongamos que elegiste el Banco A. Para abrirte una cuenta, el Banco A te dijo que quería conocerte algo más —es el protocolo KYC del que hablábamos antes—. Necesitarás presentar algún documento oficial que te identifique, tu vida laboral para justificar el origen de tus fondos (y, de paso, cumplir con el otro protocolo del que hablamos antes, el de antiblanqueo de capitales, o AML), tu alta censal si le has dicho que trabajas por cuenta propia y, en definitiva, toda una serie de documentos que hacen que tu vida privada sea un poquito menos privada desde el momento en el que los terceros de confianza se cruzan en tu vida.

El caso es que ya tienes tu cuenta bancaria abierta. Depositas tus 1.000 euros y te preparas para enviarle el dinero a tu amigo. Pero surge otro problema... Tu amigo Aitor tendrá que seguir los mismos pasos que tú y abrirse también una cuenta bancaria a su nombre; si no lo hace, no podrás hacerle llegar los 1.000 euros. En su caso, Aitor elige el Banco B. Y ello conllevó las mismas preguntas que a ti te hicieron y la misma pérdida parcial de libertad.

Superado el escollo, ya podrás llevar a cabo el intercambio de valor. Aitor te envía su número de cuenta y empieza a oler de cerca los 1.000 euros. Tú te identificas en la web de tu banco. Éste confirma con sus servidores centrales que, efectivamente, ese usuario y contraseña corresponden a un cliente de la entidad. Acto seguido, indicas que quieres llevar a cabo una transferencia bancaria. Tu banco te pedirá datos: importe, beneficiario, número de cuenta de éste, concepto de la transferencia, etcétera. Después, comprobará en sus registros que tienes suficiente saldo para poder hacer el envío. Y comprobará que la estructura de la cuenta bancaria de tu amigo es correcta, aunque no sabrá si realmente existe o no, porque no tiene ninguna información al respecto, al

tratarse de una entidad bancaria distinta a la tuya, y finalmente te pedirá una confirmación extra sobre tu solicitud de transferencia (para cumplir con otra regulación adicional, la PSD2, que persigue mejorar la seguridad de los pagos online) y te indicará que la transferencia ha sido realizada con éxito.

Ahora, a ti y a tu amigo Aitor sólo os queda confiar en que sea así. Confiar en que el Banco A transfiera el dinero al Banco B. Y confiar en que el Banco B, una vez recibidos los fondos por parte del Banco A, apunte ese importe en la cuenta de tu amigo Aitor.

El Banco A y el Banco B son terceros de confianza y están en el lucrativo negocio de la confianza. En el sistema financiero tradicional, los terceros de confianza son necesarios para transmitir valor entre personas que no estaban físicamente en el mismo lugar. La pregunta que cabe hacerse es si es posible prescindir de esos terceros de confianza. O bien, dicho de un modo algo más coloquial, la pregunta sería: ¿es posible no tener que confiar en los bancos?

Probablemente ésa fue una de las preguntas que se hizo Satoshi Nakamoto, el seudónimo con el que se firmó el libro blanco titulado originalmente «Bitcoin: A Peer-to-Peer Electronic Cash System»<sup>1</sup> (traducido al castellano como «Bitcoin: un sistema de pago electrónico de persona a persona»). La respuesta de Satoshi fue que sí que era posible. Y para demostrarlo creó el protocolo Bitcoin basado en una novedosa tecnología a la que bautizó con el nombre de *blockchain*. La blockchain, o cadena de bloques, no es más que una enorme base de datos donde se llevan a cabo registros de transacciones. Estos registros de transacciones se incluyen en bloques de información secuenciales, que van encadenados entre sí mediante el uso de mecanismos de encriptación criptográfica, de ahí el nombre de «cadena de bloques».

Al igual que tu banco (el Banco A) registró en su base de datos una salida de 1.000 euros que tú enviabas a la cuenta de tu amigo Aitor, reduciendo esa cantidad del saldo de tu cuenta, y al

1. Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System». Disponible en <<https://bitcoin.org/bitcoin.pdf>>. [Consulta: 13/09/2022]

igual que el banco de Aitor (el Banco B) registró en su base de datos una entrada de 1.000 euros que vinculó a la cuenta bancaria de Aitor, haciendo que el saldo de la cuenta de Aitor se incrementara en esa cantidad, en una blockchain se registran transacciones cuando se transmite valor de persona a persona y también se actualizan los saldos de cada persona que ha participado en la transacción.

Éste era uno de los objetivos del protocolo Bitcoin. El otro era poder hacer esta transmisión de valor digital sin la intervención de terceros de confianza. Es decir, sin intermediarios. Sin Banco A ni Banco B.

El Banco A tiene su propia base de datos, donde registra a sus clientes, los números de cuenta asociados a estos clientes, las transacciones que se llevan a cabo en esos números de cuenta, etcétera. Esta base de datos es centralizada, pues está controlada por el Banco A y solamente se puede acceder a ella si dicho banco lo autoriza (o si un juez obliga al banco a facilitar esa información).

En el Banco B ocurre lo mismo. Sus bases de datos también son centralizadas, y sus datos son controlados por el Banco B, no pudiendo conocer el resto de los bancos del sistema ni los movimientos ni los saldos que los clientes del Banco B tengan en sus cuentas.

Sin embargo, la cosa cambia con la tecnología blockchain. Para empezar, la base de datos que registra todas las transacciones es pública, y no se utilizan bases de datos centralizadas, sino «distribuidas», lo que implica que cualquier persona que quiera puede tener una copia de esa base de datos para su consulta, construyéndose de esta manera una red de ordenadores distribuidos por todo el mundo, los cuales, de manera voluntaria, han decidido participar de la supervisión y monitorización de los registros de información de la blockchain y, además, han podido hacerlo sin necesidad de pedir permiso a nadie. Es por eso que se dice que la blockchain es una «base de datos distribuida», ya que la información no está controlada por un único punto de acceso centralizado.

Ahora bien, en el sistema financiero tradicional, nos fiamos

del Banco A y del Banco B. El Banco A garantiza que puedes enviar 1.000 euros porque tienes ese saldo en tu cuenta. El Banco B garantiza que la cuenta de Aitor existe y que anotará el ingreso de 1.000 euros en su cuenta cuando reciba los fondos por parte del Banco B.

En la blockchain, todo este proceso de confianza que permite la transmisión de valor se consigue de manera descentralizada. Nadie tiene que fiarse de nadie en particular, ya que el diseño y las características de la tecnología blockchain hace que todos se puedan fiar de todos, sin depender de terceros de confianza.

Esto ha permitido un cambio de rumbo en el negocio de la confianza que está evolucionando desde el conocido modelo del sistema financiero tradicional, en el que unas pocas entidades centralizadas tienen todo el control sobre los usuarios y sus movimientos financieros y se aprovechan económicamente de ello, hacia una situación en la que cualquiera puede ser parte activa de una blockchain y participar del rendimiento económico que ésta genere, haciendo que el valor económico no vaya a manos de terceros de confianza, sino que se reparta de manera equitativa entre los partícipes de la blockchain.