

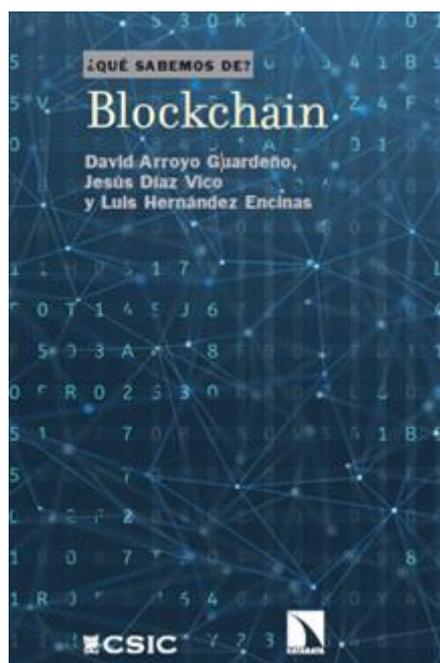
Madrid, lunes 20 de mayo de 2019

Del dinero virtual a la web 3.0: las claves de *blockchain* en un libro de divulgación

- Investigadores del CSIC y BBVA explican cómo surge *blockchain* a partir del bitcoin, la criptomoneda propuesta como alternativa al sistema financiero de bancos centrales
- Los autores detallan las aplicaciones de esta tecnología utilizada para realizar transacciones financieras y que puede ser la base de nuevos modelos de negocio
- La obra también analiza las limitaciones de *blockchain*, como su gobernanza y sostenibilidad, su escasa escalabilidad o su posible uso para actividades delictivas

En 2008 alguien que firmaba bajo el seudónimo de Sataoshi Nakamoto creó el bitcoin. La famosa moneda virtual ha sido la punta de lanza de un fenómeno más amplio: la criptoconomía. Este concepto se refiere a toda la actividad financiera basada en el uso de criptomonedas y tecnología *blockchain*. Para acercarnos a este nuevo ámbito tecnológico, los investigadores del Consejo Superior de Investigaciones Científicas (CSIC) **David Arroyo** y **Luis Hernández**, y el ingeniero **Jesús Díaz**, acaban de publicar el libro *Blockchain* (Editorial CSIC-Los libros de la Catarata), donde explican el significado y alcance de este término. Así, a lo largo del texto narran cómo funciona y para qué sirve una tecnología que será clave para transitar a una nueva economía digital y a la denominada web 3.0.

Como explican los autores, la *blockchain* o cadena de bloques es un sistema descentralizado de recolección de datos en el que la información se agrupa en bloques, de forma que, con la ayuda de herramientas



criptográficas, se garantiza la detección de cualquier cambio en los datos ya escritos en la cadena. Esta particular estructura hace que pueda ser utilizada, por ejemplo, para la creación de sistemas financieros alternativos que eluden el control de los bancos centrales. Muestras de ello son **las plataformas Bitcoin y Ethereum, que posibilitan el registro de transacciones sin intermediarios con sus respectivas monedas virtuales, el bitcoin y el ether.**

Los investigadores relatan cómo la utilización de este dinero virtual y la tecnología en la que se basa –*blockchain*– ha pasado de cierto rechazo institucional, e incluso mala fama, a representar una oportunidad para nuevos modelos de negocio y de actividad financiera, en medio de una ola de entusiasmo hacia la denominada criptoconomía. El potencial de *blockchain* es diverso, y pasa por la construcción de sistemas de protección de derechos de autor; la configuración de organizaciones autónomas basadas en ‘contratos inteligentes’ o la gestión del Internet de las cosas, entre otras aplicaciones.

Pero junto a sus múltiples oportunidades, esta tecnología también tiene puntos débiles al considerar tipos concretos de *blockchain* y contextos específicos de aplicación: por ejemplo, la dificultad asociada a la trazabilidad de las criptomonedas y que obstaculiza la persecución del lavado de dinero; las limitaciones en la gestión de la identidad y privacidad de los usuarios en el caso de *blockchains* públicas como las de Bitcoin y Ethereum; las fluctuaciones en la cotización de monedas virtuales; la gran cantidad de energía que requiere la escritura de nuevos bloques en *blockchains* basadas en la prueba de trabajo, característica que limita la escalabilidad; o ciertos incidentes de seguridad. “En los últimos años podemos hallar errores en la implementación de protocolos criptográficos, robos de credenciales en plataformas digitales, incluso fallas graves de seguridad en dispositivos *hardware* resistentes a la manipulación”, señalan los autores del libro.

Con todo, la obra incide en que *blockchain* va mucho más allá de posibilitar meros intercambios financieros. En definitiva, se trata de una herramienta para desarrollar nuevos protocolos que permitan la gestión de todo tipo de datos en la sociedad de la información.

Integrado en la colección de divulgación [¿Qué sabemos de?](#), el libro *Blockchain* puede adquirirse tanto en librerías como en las páginas web de la [Editorial CSIC](#) y [Los Libros de la Catarata](#). Con esta obra, la colección suma ya 103 títulos que acercan la actualidad científica y tecnológica al conjunto de la sociedad.

Para solicitar entrevistas con los autores o más información, se debe contactar con: divulga@csic.es (teléfono 915680043).

Sobre los autores

David Arroyo es ingeniero y doctor en Telecomunicación y científico titular en el Instituto de Tecnologías Físicas y de la Información Leonardo Torres Quevedo (ITEFI) del CSIC. Su actividad investigadora se centra en el análisis, diseño y evaluación de sistemas para la protección de la seguridad y de la privacidad de la información.

Luis Hernández es licenciado y doctor en Matemáticas, e investigador del Departamento TIC en el ITEFI (CSIC). Su investigación incluye la criptografía de clave pública, esquemas de firma digital, autenticación, identificación y compartición de secretos, *blockchain* y criptobiometría, entre otros.

Jesús Díaz es ingeniero, doctor en Informática y *research scientist* en BBVA Next Technologies. Entre sus campos de investigación destacan la criptografía aplicada a la privacidad, el análisis de seguridad de protocolos de comunicaciones y los sistemas distribuidos.

CSIC Comunicación