



Finanzas Descentralizadas (DeFi)

B.A, LL.M, Leonardo F. Brum Ramírez

I. Origen y fundamentos de los contratos inteligentes

En 2013, un programador ruso de diecinueve años, Vitalik Buterin propuso el concepto de Ethereum. Buterin comenzó a trabajar con Gavin Wood (creador de Polkadot¹) y con otros científicos de datos y desarrolladores muy respetados como Charles Hoskinson (creador de Cardano²), para amplificar los casos de uso y las capacidades de la tecnología blockchain. En los primeros años de la cadena de bloques de Bitcoin, se consideraba una maravilla tecnológica. Con el tiempo, los desarrolladores que operaban la red comenzaron a darse cuenta de que blockchain podría admitir características adicionales construidas sobre ella y esto llevó a la creación de una nueva cadena de bloques llamada Ethereum³.

Ethereum utiliza la plataforma informática distribuida basada en blockchain Ethereum Virtual Machine (EVM)⁴ de código abierto. El objetivo principal del EVM es mantener un registro distribuido de las transacciones realizadas utilizando la moneda digital Ethereum (ETH). Ésta nueva manera de programar generalmente se escribe en un lenguaje llamado "Solidity", que da vida a un nuevo tipo de software denominado "Contrato inteligente" creado por el Dr. Gavin Wood como un lenguaje explícitamente para escribir contratos de mercado con características para apoyar directamente la ejecución del mismo en el ecosistema descentralizado de Ethereum.

Los contratos inteligentes son programas informáticos o software que pueden llevar a cabo los términos de los acuerdos entre

las partes sin necesidad de coordinación o intervención humana y puede automatizar procesos previamente programados. Estos acuerdos se pueden registrar y validar en una cadena de bloques que luego puede ejecutar y hacer cumplir automáticamente el contrato, generalmente bajo instrucciones "si-entonces". Estas acciones podrían incluir, por ejemplo, liberar fondos de la cuenta bancaria de una de las partes del contrato cuando se reciba el producto o servicio, registrar un vehículo o emitir una factura, solo por mencionar algunas ideas. Una vez que se cumplen las condiciones, los contratos inteligentes se ejecutan inmediatamente y la cadena de bloques se actualiza, manteniendo el registro de acciones que podrían incluir transacciones monetarias como se ejemplifica.



¹ Polkadot es una plataforma blockchain interoperable y de múltiples cadenas que permite la transferencia de datos y activos entre diferentes redes. Fue fundada en 2016 por el co-fundador de Ethereum, Gavin Wood, y utiliza un sistema de consenso de prueba de participación nominada (NPoS) para validar transacciones y asegurar la red. Polkadot tiene como objetivo facilitar la creación y conexión de cadenas de bloques especializadas para una mayor eficiencia y escalabilidad.

² Cardano es una plataforma blockchain de tercera generación que utiliza el algoritmo de consenso Ouroboros para validar transacciones y generar nuevos bloques. Fue fundada en 2015 por el co-fundador de Ethereum, Charles Hoskinson, y tiene como objetivo proporcionar una plataforma segura y escalable para la construcción de aplicaciones descentralizadas.

³ Lorne Lantz y Daniel Cawrey, "Dominar blockchain: desbloquear el poder de las criptomonedas, los contratos inteligentes y las aplicaciones descentralizadas", La evolución a Ethereum, Capítulo 4, O'Reilly, noviembre de 2020, pp 79

⁴ El EVM es una plataforma donde viven los datos de Ethereum y los contratos inteligentes (similar a los sites, pero basados en infraestructura de blockchain).