**Taller introducción Blockchain**

José Manuel Calabuig - <https://jmcalabu.blogs.upv.es/> -

*Grupo MAD*$φ$ *-MATHEMATICS AND APPLICATIONS TO DATA AND PHYSICS-*

<https://www.madphy.webs.upv.es/>

Instituto Universitario de Matemática Pura y Aplicada

Universitat Politècnica de València

La tecnología Blockchain (cadena de bloques) fue introducida en el año 2008 por Satoshi Nakamoto (pseudónimo con el que se conoce a la persona o grupo de personas creadores que son, a día de hoy, todavía desconocidos). En el artículo se describía el funcionamiento de un sistema de dinero electrónico P2P (del inglés *Peer to peer,* es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos). Un año después se creó el software *Bitcoin* (así como la red del mismo nombre) y las primeras unidades de moneda, los conocidos *bitcoins*. Surge así la primera criptomoneda. De una manera muy simplificada Blockchain de Bitcoin no es más que una base de datos, descentralizada, distribuida y abierta, que registra todas las transacciones de bitcoins. Más concretamente la cadena de bloques de Bitcoin se caracteriza por:

1. Es **descentralizada**, eliminando la necesidad de una entidad central de confianza (como un banco central). En este sentido todos los nodos que componen la red son iguales no habiendo así un poder central sobre ella.
2. Es **distribuida**: todos y cada uno de los nodos de la red tienen una copia exacta y actualizada de la cadena de bloques.
3. Es **consensuada**: hay unas reglas claras que marcan un consenso en torno a qué transacciones son válidas y cuál es el estado actual de la cadena.
4. Es **abierta**, en el sentido de que cualquiera puede participar (sólo se necesita descargarse el programa) permitiendo a cualquier persona no solamente enviar transacciones sino también acceder a la información registrada en la cadena de bloques.
5. Es **segura,** existiendo no sólo una verificación criptográfica sino también una serie de incentivos económicos sobre los que se asienta parte de la seguridad de la cadena.

Su éxito ha ido despertando cada vez un mayor interés en diferentes ámbitos lo que ha hecho que la tecnología haya ido avanzando en distintas direcciones con aplicaciones en muchos casos alejadas del mundo de las criptomonedas. En este sentido cabe destacar la introducción de los conocidos como *Smart Contracts* (contratos inteligentes) que son programas informáticos que se ejecutan automáticamente cuando se asegura el cumplimiento de las condiciones marcadas en dicho contrato. Si bien a nivel teórico dicho término fue acuñado por el informático Nick Szabo (alrededor del año 1993) antes de la aparición de la Blockchain no existía ninguna plataforma capaz de hacer realidad los contratos inteligentes. Cabe aquí mencionar a la cadena de bloques *Ethereum* que además de tener su criptomoneda (llamada *ether*) permite, mediante un lenguaje propio (*Solidity*), la redacción y ejecución de contratos inteligentes.

Este taller tendrá dos partes un primera de carácter introductorio en el que se explicarán los conceptos más usuales en este ámbito (Blockchain, contratos inteligentes, ICOs, Gemelos digitales,…). Contaremos también algunas iniciativas recientes tanto de aplicación en el sector público como en el privado. En la segunda parte, de carácter práctico, se construirá un ejemplo de un contrato inteligente que desplegaremos y ejecutaremos en un simulador de Blockchain local formado por diez nodos.

Taller introducció Blockchain
José Manuel Calabuig - https://jmcalabu.blogs.upv.es/ -
Grup MADφ -MATHEMATICS AND APPLICATIONSTO DATA AND PHYSICS-
https://www.madphy.webs.upv.es/
Institut Universitari de Matemàtica Pura i Aplicada
Universitat Politècnica de València

La tecnologia Blockchain (cadena de blocs) va ser introduïda l'any 2008 per Satoshi Nakamoto pseudònim amb el qual es coneix a la persona o grup de persones creadors que són, hui dia, encara desconeguts). En l'article es descrivia el funcionament d'un sistema de diners electrònics P2P (de l'anglés Peer to peer, és una xarxa d'ordinadors en la qual tots o alguns aspectes funcionen sense clients ni servidors fixos). Un any després es va crear el programari Bitcoin (així com la xarxa del mateix nom) i les primeres unitats de moneda, els coneguts bitcoins. Sorgeix així la primera criptomoneda. D'una manera molt simplificada Blockchain de Bitcoin no és més que una base de dades, descentralitzada, distribuïda i oberta, que registra totes les transaccions de bitcoins. Més concretament la cadena de blocs de Bitcoin es caracteritza per:

1. És **descentralitzada,** eliminant la necessitat d'una entitat central de confiança (com un banc central). En aquest sentit tots els nodes que componen la xarxa són iguals no havent-hi així un poder central sobre ella.
2. És **distribuïda**: tots i cadascun dels nodes de la xarxa tenen una còpia exacta i actualitzada de la cadena de blocs.
3. És **consensuada**: hi ha unes regles clares que marquen un consens entorn de quines transaccions són vàlides i quin és l'estat actual de la cadena.
4. És **oberta,** en el sentit que qualsevol pot participar (només es necessita descarregar-se el programa) permetent a qualsevol persona no solament enviar transaccions sinó també accedir a la informació registrada en la cadena de blocs.
5. És **segura**, existint no solament una verificació criptogràfica sinó també una sèrie d'incentius econòmics sobre els quals s'assentisca part de la seguretat de la cadena.

El seu èxit ha anat despertant cada vegada un major interés en diferents àmbits, el que ha fet que la tecnologia haja anat avançant en diferents direccions amb aplicacions en molts casos allunyades del món de les criptomonedas. En aquest sentit cal destacar la introducció dels coneguts com Smart Contracts(contractes intel·ligents) que són programes informàtics que s'executen automàticament quan s'assegura el compliment de les condicions marcades en aquest contracte. Si bé a nivell teòric aquest terme va ser encunyat per l'informàtic Nick Szabo (al voltant de l'any 1993) abans de l'aparició de la Blockchain no existia cap plataforma capaç de fer realitat els contractes intel·ligents. Cal esmentar a la cadena de blocs Ethereum que a més de tindre la seua criptomoneda (cridada ether) permet, mitjançant un llenguatge propi (Solidity), la redacció i execució de contractes intel·ligents.

Aquest taller tindrà dues parts, una primera de caràcter introductori en la qual s'explicaran els conceptes més usuals (Blockchain, contractes intel·ligents, ICOs, Bessons digitals,…). Comptarem també algunes iniciatives recents tant d'aplicació en el sector públic com en el privat. En la segona part, de caràcter pràctic, es construirà un exemple d'un contracte intel·ligent que desplegarem i executarem en un simulador de Blockchain local format per deu nodes.

**Workshop: introduction to Blockchain**

José Manuel Calabuig - <https://jmcalabu.blogs.upv.es/> -

*Grupo MAD*$φ$ *-MATHEMATICS AND APPLICATIONS TO DATA AND PHYSICS-*

<https://www.madphy.webs.upv.es/>

Instituto Universitario de Matemática Pura y Aplicada

Universitat Politècnica de València

Blockchain technology was introduced in 2008 by Satoshi Nakamoto (actually a pseudonym with which the individual or group of individuals that created blockchain is known). This pioneering article described the functioning of a P2P electronic money system. A year later, bitcoin software was created, together with the network of the same name and the first currency units (bitcoins). This is how the first cryptocurrency came about. In a very simplified way, bitcoin's blockchain is only a decentralized, distributed and open database that stores all bitcoin transactions. More specifically, the bitcoin blockchain is characterized by:

1. It is **decentralized**, eliminating the need for a central trust institution (such as a central bank). In this sense, all nodes making up the network are equal, and there is no central power over it.
2. It is **distributed**: each and every node of the network has an exact and updated copy of the blockchain.
3. It is **consensual**: there are clear rules for a consensus around which transactions are valid and what is the current status of the chain.
4. It is **open**, in the sense that anyone can participate (you only need to download the program), allowing any person not only to make transactions but also to access the information registered in the blockchain.
5. It is **safe**, there being not only a cryptographic verification but also a series of economic incentives on which the security of the chain is partly based.

Its success has been arousing increasing interest from different fields. This has made the technology to move in different directions with applications in many cases away from the world of cryptocurrencies. In this regard, it is worth highlighting the introduction of the so-called smart contracts, i.e. computer programs that are automatically executed when the legal requirements established in the contract are met. Although, from a theoretical perspective, the term was coined by computer scientist Nick Szabo (around 1993), prior to blockchain there was no platform capable of making smart contracts a reality. It is worth mentioning, however, that Ethereum blockchain not only has its specific cryptocurrency (ether) but also allows, through its language Solidity, writing and performing smart contracts.

This workshop will consist of two parts. The first one will be introductory and devoted to explaining the most popular concepts in this field (Blockchain, smart contracts, ICOs, Digital Twins, among others), as well as recent initiatives in the area (both in the public and private sectors). In the second part, more focused on practical aspects, an example of a smart contract will be first created and then tested in a local blockchain simulator made up by ten nodes.