**Workshop: introduction to Blockchain**

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

*Grupo MAD -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.