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.