

# Minicorso su Blockchain

Struttura del corso (24h - 2CFU)

- Prof. Roberto Segala 4h
- Prof. Fausto Spoto 2h
- Dr.ssa Avv. Maddalena Castellani 6h
- Dr. Matteo Cristani 4-5h
- Dr. Marco Pighin ([synclab.it](http://synclab.it)) 2h
- Prof Fausto Spoto 4h

Contenuti:

Elementi di crittografia, blockchain, stato, Merkle tree e consenso. Programmazione e principi di implementazione di una blockchain. Teoria dei contratti in generale e specificatamente sui contratti tipici e atipici dell'informatica (licenza, sviluppo, outsourcing, services etc.). Diritto della blockchain e le implicazioni giuridiche a seconda che si tratti di blockchain aperta o chiusa. Carrellata relativa ai contratti che possono essere stipulati nell'applicazione di progetti block differenti (per esempio: progetto supply chain; progetto retail logistica / contratti di locazione). Smart contract. Trasposizione del contratto tradizionale in smart contract. Aspetti logico formali nella trasposizione in smart contracts e viceversa. Compliance dei processi. Semantica ed ermeneutica degli smart contracts. Descrizione del funzionamento della catena Ethereum (GAS, deploy ed esecuzione smartcontract ecc.), fondamentali del linguaggio solidity e dei tool per lo sviluppo di smart contract su Ethereum (principalmente Remix, Ganache, MetaMask) ed esempi ed **hands-on** di blockchain con [synclab.it](http://synclab.it). Implementazione di una piattaforma di votazione mediante l'utilizzo di SmartContract su catena Ethereum (linguaggio Solidity). Problemi di sicurezza in codice Solidity.

Calendario (dal 1 Giugno 2020):

- 1 giugno (2h) 14:00-16:00 - Roberto Segala  
Introduzione alla crittografia, sicurezza crittografica, crittografia simmetrica e asimmetrica, codifiche a blocchi, semplici protocolli
- 3 giugno (2h) 16:00-18:00 - Roberto Segala  
Firma digitale, funzioni hash collision resistant, autenticazione, cenni alla crittografia ellittica
- 4 giugno 9:00-11:00 (2h) - Fausto Spoto  
introduzione alle blockchain, blocchi, stato, proof of work, proof of stake, consenso, il caso di Bitcoin ed Ethereum, wallet, Infura, web3j, indirizzi Ethereum, transazioni, nonce, transazioni con Infura e web3j
- Giorno 4 (2h) - 08/06/2020 - Maddalena Castellani  
Introduzione generale ai contratti - contratti tipici / atipici ; trattative precontrattuali ; la tutela del sw ; i contratti di informatica (licenza; sviluppo; manutenzione; outsourcing; services ( cloud - SAAS); condizioni generali - condizioni speciali )

- Giorno 5 (2h) - 09/06/2020 - Maddalena Castellani - riprendo contratti di informatica; blockchain in generale (con permesso senza permesso esempio vendita immobiliare) ; esempi di clienti tipo ( certificazione bio - retail e logistica - gestione dati disorganizzati - cliente che vuole stipulare un contratto tra due o più parti collegamento con smart contract)
- Giorno 6 (2h) - 10/06/2020 - Maddalena Castellani - smart contract e collegamento con lezione prof. Cristani sulla trasposizione del contratto naturale in smart contract.
- Giorno 7 (2h) Natural language processing: tecniche di traduzione di contratti in sistemi logici, proprietà dei contratti. Negoziato digitale
- Giorno 8 (2h) Trattamento dell'automazione della correttezza di contratti rispetto allo sfondo normativo con tecniche logico-formali.
- Giorno 9 (2h) 05/06/2020 (14-16) Sync Lab  
Catena Ethereum (funzionamento generale, GAS, deploy ed esecuzione Smart Contract), introduzione al linguaggio Solidity ed ai tool di sviluppo (principalmente Remix, Ganache, MetaMask)
- Giorno 10 (2h) 05/06/2020 (16-18) Sync Lab  
Hands-on con implementazione di una piattaforma di votazione su Ethereum
- 6 giugno 9:00-11:00 (2h) - Fausto Spoto  
Esempi di smart contract Solidity per schemi Ponzi ed aste
- 6 giugno 11:00 - 13:00 (2h) - Fausto Spoto  
Problemi di sicurezza del codice Solidity: reentrancy, over/underflows, entropy illusion, front running (ed altri)

Luogo: ZOOM.