

Denominazione	Diritto delle blockchain e cybersecurity
Moduli componenti	
Settore scientifico-disciplinare	GIUR-03/A
Anno di corso e semestre di erogazione	2° Anno, 1° Semestre
Lingua di insegnamento	Italiano
Carico didattico in crediti formativi universitari	6
Numero di ore di attività didattica assistita complessive e ripartite tra DE e DI	Didattica Erogativa: 36 Didattica Interattiva: 6
Docente	Fulvio Sarzana di S. Ippolito
Risultati di apprendimento specifici	Al termine del percorso di studio lo studente avrà le conoscenze di base relative al contesto normativo valutario nazionale e internazionale delle blockchain; avrà pertanto la capacità di comprendere, analizzare ed interpretare le dinamiche giuridiche e regolamentari delle cd. tecnologie emergenti in ambito nazionale ed europeo. Lo studente acquisirà altresì le conoscenze relative alle caratteristiche delle criptovalute e degli strumenti e prodotti finanziari associati alla tokenizzazione, al fine di comprendere fattispecie come i cripto-assets e gli smart contracts. Infine, lo studente acquisirà le conoscenze relative ai profili normativi nazionali e internazionali della cyber security al fine di comprendere e analizzare le problematiche giuridiche di quest'ultima attraverso una comparazione con gli istituti in ambito nazionale e sovranazionale. Attraverso le nozioni acquisite lo studente sarà in grado di: redigere uno smart contract attraverso la blockchain; lanciare un progetto di finanziamento attraverso la tokenizzazione e le initial coin offerings (ICO); identificare i requisiti regolamentari per gli intermediari di criptovalute; valutare e comprendere i perimetri di rischio di cybersicurezza delle infrastrutture nazionali, analizzare le diverse giurisdizioni sui registri distribuiti e le blockchain. Lo studente avrà così acquisito la capacità di valutare autonomamente da un punto di vista regolamentare le diverse categorie di blockchain e i profili di rischio di un sistema informatico complesso. Sarà altresì in grado di esprimere in modo efficace le conoscenze acquisite e descrivere, con linguaggio tecnico-normativo, le caratteristiche dei registri elettronici distribuiti e delle blockchain, i processi di valutazione degli strumenti finanziari associati alle tecnologie emergenti, le caratteristiche di un sistema protetto dai rischi della cyber security.
Programma	La struttura del Corso si articola in tre parti. Nella prima parte sono illustrate le caratteristiche di base delle blockchain e sono descritte le caratteristiche istituzionali ed organizzative. • La nascita delle criptovalute • Da bitcoin alle blockchain • I registri elettronici distribuiti • Le diverse forme di blockchain • Gli smart contracts • La validazione temporale elettronica La seconda parte è dedicata allo studio delle caratteristiche tecnico-giuridiche delle blockchain e degli strumenti e prodotti finanziari e le responsabilità e i doveri degli intermediari della blockchain, con particolare riferimento a: • Le norme valutarie nazionali ed internazionali • L'applicazione della disciplina antiriciclaggio • I diversi tipi di token associati ad un progetto blockchain • Le initial coin offerings (ICO) • I progetti finanziari nelle diverse filiere produttive: dal made in Italy al settore agro-alimentare alla difesa della proprietà intellettuale ed industriale Nella terza parte sono analizzati i principali problemi associati alla cybersecurity ed in particolare • Il perimetro di rischio della cybersecurity • Le norme nazionali ed internazionali sulla cybersecurity • Il cd golden power.
Tipologie di attività	L'insegnamento è strutturato in lezioni, che si svolgono in modo frontale, incoraggiando l'interazione

didattiche previste e relative modalità di svolgimento	e la partecipazione attiva degli studenti, ed esercitazioni, integrate con le lezioni, che si svolgono in aula. Sono previste lezioni e seminari tenuti da operatori ed esperti del settore, con analisi di casi pratici, al fine di consentire un pieno contatto con la concreta operatività di quanto insegnato a lezione.
Metodi e criteri di valutazione dell'apprendimento	L'esame è svolto in forma orale, prevede almeno quattro domande e dura almeno 40 minuti. Le domande sono finalizzate a verificare: l'acquisizione, da parte degli studenti, della conoscenza e della comprensione delle caratteristiche giuridiche della blockchain e dei diversi profili associati alla cyber security, nonché la capacità di applicare le conoscenze apprese, operando e scelte corrette in relazione alla complessità ed alla peculiarità del caso oggetto del singolo esercizio e dimostrando quindi discernimento ed autonomia di giudizio. Viene altresì valutata l'abilità comunicativa e di esposizione dello studente utilizzando il linguaggio tecnico adeguato, in particolare con riferimento alle caratteristiche istituzionali, normative e organizzative delle blockchain nonché della cybersecurity.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	La valutazione dell'apprendimento prevede l'attribuzione di un voto finale espresso in trentesimi. Il voto finale deriva dalla valutazione complessiva della prova e risulta dalla verifica del livello di raggiungimento dei risultati di apprendimento stabiliti. Ai fini del voto finale, in particolare, • le domande a carattere teorico hanno un indicativamente peso pari al 50%; ai fini della valutazione si considera sia l'evidenza della conoscenza acquisita, sia la proprietà ed articolazione con cui essa è illustrata; • le domande volte ad accertare le conoscenze pratiche hanno un peso indicativamente pari al 50%; si tiene in considerazione nella valutazione sia la capacità di individuare il corretto procedimento, sia la corretta esecuzione del medesimo.
Propedeuticità	Conoscenze necessarie per seguire il corso con profitto: nozioni di base di diritto.
Materiale didattico utilizzato e materiale didattico consigliato	<u>Materiale didattico di supporto all'apprendimento</u> Dispense e slide del docente. <u>Testo di consultazione</u> Fulvio SARZANA DI S.IPPOLITO-Massimiliano NICOTRA, Diritto della blockchain, intelligenza artificiale ed IoT, IPSOA-Wolters Kluwer, 2018.