<table>
<tr><td>NAZIV PREDMETA</td><td colspan="5">Kriptovalute</td></tr>
<tr><td>Kod</td><td>DIT045</td><td>Godina studija</td><td colspan="3">2.</td></tr>
<tr><td>Nositelj/i predmeta</td><td>Nikola Grgić, dipl. ing., predavač</td><td>Bodovna vrijednost (ECTS)</td><td colspan="3">6</td></tr>
<tr><td rowspan="2">Suradnici</td><td rowspan="2">-</td><td rowspan="2">Način izvođenja nastave (broj sati u semestru)</td><td>P</td><td>S</td><td>V</td><td>T</td></tr>
<tr><td>30</td><td>15</td><td>15</td><td></td></tr>
<tr><td>Status predmeta</td><td>Izborni</td><td>Postotak primjene e-učenja</td><td colspan="3">50%</td></tr>
<tr><td colspan="6">OPIS PREDMETA</td></tr>
<tr><td>Ciljevi predmeta</td><td colspan="5">• upoznavanje studenata s načinom na koji funkcioniraju kriptovalute
• prepoznavanje sigurnosnih rizika kod korištenja i razvoja aplikacija vezanih za kriptovalute
• teorijska i praktična priprema studenta za razvoj aplikacija za rad s kriptovalutama
• shvaćanje društvenih i ekonomskih aspekata razvoja i šireg prihvaćanja kriptovaluta</td></tr>
<tr><td>Uvjeti za upis predmeta i ulazne kompetencije potrebne za predmet</td><td colspan="5">• znanje programiranja u nekom od programskih jezika (Python, Java, C#, PHP, ili sl.)</td></tr>
<tr><td>Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)</td><td colspan="5">1. definirati karakteristike i opisati specifičnosti važnijih kriptovaluta
2. razumjeti rad protokola Bitcoin
3. analizirati podatke s liste zapisa blockchain
4. napraviti transakciju na mreži Bitcoin i potpisati poruku privatnim ključem
5. izraditi aplikaciju koja koristi blockchain i komunicira s poslužiteljem Bitcoin Core</td></tr>
<tr><td>Sadržaj predmeta detaljno razrađen prema satnici nastave</td><td colspan="5">
<table>
<tr><th>Tjedan</th><th>Sati</th><th>Oblik nastave</th><th>Tema</th></tr>
<tr><td rowspan="2">1.</td><td>2</td><td>predavanja</td><td>Povijest novca. Razvoj kriptovaluta. Problem bizantskog generala. Dokaz rada. Lanac zapisa blockchain. Prvi blok (Genesis block).</td></tr>
<tr><td>2</td><td>vježbe</td><td>Analiziranje podataka na lancu zapisa blockchain.</td></tr>
</table>
</td></tr>
</table>

	2.	2	predavanja	Protokol Bitcoin: hash funkcije, Merkle tree, potpisi. Struktura poruke i tipovi poruka.
		1	seminar	Podjela tema seminarskih radova i projektnih zadataka.
		2	vježbe	Bitcoin privatni i javni ključ. Adrese. Program vanitygen.
	3.	2	predavanja	Standardna implementacija protokola Bitcoin (Bitcoin Core). Parametri standardne implementacije.
		1	seminar	Predstavljanje tema seminarskih radova. Diskusija.
		2	vježbe	Rad u naredbenom retku programa Bitcoin Core.
	4.	2	predavanja	API sučelje na poslužitelju Bitcoin Core. RPC pozivi.
		2	vježbe	Pokretanje programa Bitcoin Core u poslužiteljskom načinu rada. Bitcoin Core API. Programiranje RPC poziva prema sučelju Bitcoin Core poslužitelja.
	5.	2	predavanja	Bitcoin transakcije. Cijena transakcije i red čekanja (mempool). Natjecanje za prostor u bloku i troškovi rada mreže.
		2	seminar	Analiza projektnih zadatka.
	6.	2	predavanja	Kriptografski algoritmi u protokolu Bitcoin. Kriptografija javnog ključa. Potpisivanje poruka privatnim ključem. Provjera poruke i potpisa.
		2	seminar	Planiranje i oblikovanje projekata.
	7.	2	predavanja	Rudarenje. Algoritmi za prilagođavanje težine rudarenja. Rudarenje na GPU jedinicama. ASIC uređaji.
		2	seminar	Odabir i analiza API poziva potrebnih za izradu projekata.
	8.	2	predavanja	Sigurnosni model Bitcoina.
		2	vježbe	Priprema i slanje transakcije na mrežu Bitcoin. Analiza iznosa naknade potrebne za uspješno

				izvršavanje transakcije. Potpisivanje poruke privatnim ključem.
	9.	2	predavanja	Bitcoin čvorovi s cjelovitom povijesti transakcija (full nodes). Slabosti laganih Bitcoin klijenata.
		2	vježbe	Lagani klijenti. Odabir klijenta prema zadanim razinama sigurnosti.
	10.	2	predavanja	Novčanik s privatnim ključevima: standardni i deterministički novčanik. Papirnati i hardverski novčanik. Čuvanje novčanika. Potpisivanje transakcija u sigurnom okruženju.
		2	vježbe	Deterministički novčanik. BIP 39 seed generator. Sigurnosna pohrana i povrat novčanika.
	11.	2	predavanja	Ostale kriptovalute (altcoini). Važniji predstavnici ostalih kriptovaluta. Proof of stake (POS) algoritmi.
		1	vježbe	Instalacija i korištenje softverskih klijenata drugih kriptovaluta.
		1	seminar	Obrane seminarskih radova. Diskusija.
	12.	2	predavanja	Mikroplaćanje na internetu. Prijedlozi za promjenu veličine bloka u mreži Bitcoin. Protokoli drugog sloja. Segwit, Lightning network. Dijeljenja mreže (forks).
		1	seminar	Obrane seminarskih radova. Diskusija.
	13.	2	predavanja	Prijedlozi za unaprjeđenje protokola Bitcoin (BIP).
		1	seminar	Obrane seminarskih radova. Diskusija.
	14.	2	predavanja	Alternativni načini korištenja lanca zapisa blockchain: pametni ugovori, obojane transakcije.
		2	seminar	Predstavljanje i obrana projekata.
	15.	2	predavanja	Društveni i ekonomski i aspekti razvoja i prihvaćanja kriptovaluta.
		2	seminar	Predstavljanje i obrana projekata.
	☒ predavanja			☐ samostalni zadaci

<table>
<tr><td>Vrste izvođenja nastave:</td><td>☒ seminari i radionice
☒ vježbe
☐ on line u cijelosti
☒ mješovito e-učenje</td><td>☐ multimedija
☒ laboratorij
☐ mentorski rad
☒ projekt</td></tr>
<tr><td>Obveze studenata</td><td colspan="2">• obavljanje svih propisanih laboratorijskih vježbi
• uspješna izrada i obrana seminarskog rada
• uspješna izrada i obrana projekta
• nazočnost na predavanjima u iznosu od najmanje 70% predviđene satnice (za izvanredne studente 50%)</td></tr>
</table>

<table>
<tr><td rowspan="6">Praćenje rada studenata (upisati udio u ECTS bodovima za svaku aktivnost tako da ukupni broj ECTS bodova odgovara bodovnoj vrijednosti predmeta):</td><td>Pohađanje nastave</td><td>2</td><td>Istraživanje</td><td>0,5</td><td>Konzultacije i završni ispit</td><td>0,1</td></tr>
<tr><td>Eksperimentalni rad</td><td></td><td>Referat</td><td></td><td>Samostalno učenje</td><td>0,5</td></tr>
<tr><td>Projekt</td><td>2,4</td><td>Seminarski rad</td><td>0,5</td><td></td><td></td></tr>
<tr><td>Kolokviji</td><td></td><td>Usmeni ispit</td><td></td><td></td><td></td></tr>
<tr><td>Pismeni ispit</td><td></td><td>Praktični rad</td><td></td><td></td><td></td></tr>
</table>

Ocjenjivanje i vrjednovanje rada studenata tijekom nastave i na završnom ispitu

KONTINUIRANA PROCJENA		
Pokazatelji kontinuirane provjere	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Seminarski rad	*10 – 100*	*100*
Nazočnost i aktivnost na predavanjima	*70 – 100*	*0*
Nazočnost i aktivnost na laboratorijskim vježbama	*70 – 100*	*0*

ZAVRŠNA PROCJENA		
Pokazatelji provjere - završni ispit (prvi i drugi ispitni termin)	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Projekt	*20 – 100*	*50*
Ispit (na računalu ili pisano)	*40 – 100*	*30*
Ispit (usmeni)	*100*	*0*
Prethodne aktivnosti (uključuju sve pokazatelje kontinuirane provjere)	*10 – 100*	*20*
Pokazatelji provjere - popravni ispit (treći i četvrti ispitni termin)	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Projekt	*20 – 100*	*50*
Ispit (na računalu ili pisano)	*45 – 100*	*30*
Ispit (usmeni)	*100*	*0*
Prethodne aktivnosti (uključuju sve pokazatelje kontinuirane provjere)	*10 – 100*	*20*

Općenito se ocjena na završnom i popravnom ispitu (u postotcima) formira temeljem svih pokazatelja koji opisuju razinu studentskih aktivnosti prema relaciji:

$$Ocjena\ (\%) = \sum_{i=1}^{N} k_i A_i$$

k_i - težinski koeficijent za pojedinu aktivnost,
A_i - postotni uspjeh postignut za pojedinu aktivnost,
N - ukupan broj aktivnosti.

ODNOS POLUČENOG USPJEHA I PRIPADNE OCJENE		
Postotak	Kriterij	Ocjena
od 50% do 61%	*zadovoljava minimalne kriterije*	dovoljan (2)
od 62% do 74%	*prosječan uspjeh s primjetnim nedostatcima*	dobar (3)
od 75% do 87%	*iznadprosječan uspjeh s ponekom greškom*	vrlo dobar (4)
od 88% do 100%	*izniman uspjeh*	izvrstan (5)

<table>
<tr><td rowspan="3">Obvezna literatura (dostupna u knjižnici i putem ostalih medija)</td><td>Naslov</td><td>Broj primjeraka u knjižnici</td><td>Dostupnost putem ostalih medija</td></tr>
<tr><td>Nakamoto, S.: „A Peer-to-Peer Electronic Cash System“, 2008.</td><td></td><td>www.bitcoin.org</td></tr>
<tr><td>Nastavni materijali s predavanja</td><td></td><td>Moodle</td></tr>
<tr><td>Dopunska literatura</td><td colspan="3">Antonopoulos, A. M., „Mastering Bitcoin: Programming the Open Blockchain“, O'Reilly Media, 2014.</td></tr>
<tr><td>Načini praćenja kvalitete koji osiguravaju stjecanje utvrđenih ishoda učenja</td><td colspan="3">- evidencija pohađanja nastave i uspješnosti izvršenja ostalih obveza studenata (nastavnik).
- ažuriranje detaljnih izvedbenih planova nastave - DIP (nastavnik).
- nadzor izvođenja nastave (zamjenik pročelnika Odjela za nastavu, pročelnici odsjeka).
- kontinuirana provjera kvalitete svih parametara nastavnog procesa u skladu s akcijskim planovima (pomoćnik pročelnika Odjela za kvalitetu).
- semestralno provođenje studentske ankete sukladno „Pravilniku o postupku studentskog vrednovanja nastavnog rada na sveučilištu u Splitu“ (UNIST, Centar za unaprjeđenje kvalitete).</td></tr>
<tr><td>Ostalo (prema mišljenju predlagatelja)</td><td colspan="3">DIP-ovi predmeta nalaze se unutar sustava za podršku nastavi (Moodle) i dostupni su studentima i nastavnicima Odjela. Skraćeni izvedbeni programi - IP (hrvatska i engleska inačica) su u cilju javnosti informiranja izravno dostupni na web stranicama Odjela.</td></tr>
</table>