<table>
<tr><th>NAZIV PREDMETA</th><th colspan="5">Kriptovalute</th></tr>
<tr><td>Kod</td><td>DPR013</td><td>Godina studija</td><td colspan="3">2.</td></tr>
<tr><td>Nositelj/i predmeta</td><td>Nikola Grgić,
viši 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>LV</td></tr>
<tr><td>24</td><td>16</td><td>20</td></tr>
<tr><td>Status predmeta</td><td>Obavezni</td><td>Postotak primjene e-učenja</td><td colspan="3">25%</td></tr>
<tr><th colspan="6">OPIS PREDMETA</th></tr>
<tr><td>Ciljevi predmeta</td><td colspan="5">usvajanje i primjena teorijskih znanja vezanih za kriptovalute i tehnologiju blockchain
teorijska i praktična priprema studenta za razvoj programskih rješenja zasnovanih na tehnologijama kriptovaluta
usvajanje metoda za dohvat, analizu i obradu podataka s blockchaina
prepoznavanje sigurnosnih rizika kod korištenja kriptovaluta
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 i izrade mobilnih ili web aplikacija</td></tr>
<tr><td>Očekivani ishodi učenja na razini predmeta (4-10 ishoda učenja)</td><td colspan="5">Usporediti specifičnosti i karakteristike važnijih kriptovaluta.
Objasniti osnovne pojmove vezane za kriptovalute zasnovane na tehnologiji blockchain.
Primijeniti teoretska znanja vezana za rad protokola Bitcoin u interpretaciji događaja na mreži i u razvoju vlastitih programskih rješenja.
Utvrditi vezu između različitih događaja na blockchainu i objasniti njihov odnos.
Izdvojiti povezane podatke iz blockchaina i prikazati rezultate na jasan i pregledan način.
Razviti aplikaciju i postaviti sustav za pristup Bitcoin blockchainu neovisan o trećoj strani.</td></tr>
</table>

	Sati	Oblik nastave	Tema
Sadržaj predmeta detaljno razrađen prema satnici nastave	2	predavanja	Povijest novca. Razvoj kriptovaluta. Bitcoin *whitepaper*. Pregled osnovnih pojmova vezanih za kriptovalute i Bitcoin.
	2	predavanja	Novčanici (engl. *wallet*). Vrste novčanika. Preporuke za odabir softverskog novčanika. Generiranje privatnog ključa. Standardni i deterministički novčanici.
	2	predavanja	Standardna implementacija protokola Bitcoin. Funkcionalnosti standardne implementacije. Puni čvor (engl. *full node*). Podatkovni direktorij klijenta Bitcoin Core.
	2	predavanja	Pokretanje programa Bitcoin Core u poslužiteljskom načinu rada. Programsko sučelje poslužitelja. RPC pozivi. Mreža Bitcoin testnet.
	2	predavanja	Transakcije. Ulazi i izlazi. Transakcijska naknada i red čekanja (engl. *mempool*). Nepotrošeni izlazi transakcije.
	2	predavanja	Elementi transakcije. Transakcijske skripte i skriptni jezik. Svojstva skriptnog jezika u Bitcoinu. Postupak provjere valjanosti transakcije.
	2	predavanja	Ključevi i adrese. Kriptografija javnog ključa. Kodiranje Base58 i Base58Check. Oblici zapisa ključeva. P2PKH, P2SH, Bech32 i Multisig adrese.
	2	predavanja	Arhitektura mreže Bitcoin. Vrste čvorova i njihova uloga na mreži. Lagani Bitcoin klijenti.
	2	predavanja	Blockchain. Zaglavlje i struktura bloka. Merkle tree. Rudarenje. Dokaz rada. Konsenzus. Prilagođavanje težine rudarenja.
	2	predavanja	Natjecanje za prostor u bloku i troškovi rada mreže. Podjele mreže (engl. *forks*). Problem skalabilnosti i protokoli drugog sloja. Mreža Lightning.
	2	predavanja	Društveni i ekonomski aspekti razvoja i prihvaćanja kriptovaluta. Pravni status kriptovaluta. Trgovanje kriptovalutama i porezna regulativa.
	2	predavanja	Prijedlozi za unaprjeđenje protokola Bitcoin (BIP). Ostale kriptovalute (engl. *altcoins*). Specifičnosti i karakteristike važnijih predstavnika ostalih kriptovaluta.

	2	seminar	Predstavljanje tema seminarskih radova. Definiranje projektnih zadataka.
	2	seminar	Analiza projektnih zadataka. Planiranje i oblikovanje rješenja.
	2	seminar	Rad na projektnom zadatku. Odabir i analiza API poziva potrebnih za izradu projektnog zadatka.
	5	seminar	Predstavljanje i obrane seminarskih radova. Diskusija.
	5	seminar	Predstavljanje i obrane projektnih zadataka.
	2	laboratorijske vježbe	Softverski novčanici. Generiranje privatnog ključa i adresa. Priprema, potpisivanje i odašiljanje transakcije.
	2	laboratorijske vježbe	Analiza podataka s blockchaina. Transakcijske naknade. Mempool.
	2	laboratorijske vježbe	Bitcoin Core: podatkovni direktorij, sinkronizacija s mrežom. Transakcije. Mreža Bitcoin testnet.
	2	laboratorijske vježbe	Rad u naredbenom retku programa Bitcoin Core. Upravljanje bitcoinima (engl. *coin control*).
	2	laboratorijske vježbe	Pokretanje programa Bitcoin Core u poslužiteljskom načinu rada. Konfiguracijska datoteka i parametri.
	2	laboratorijske vježbe	Bitcoin Core API. Generiranje jednostavnih RPC poziva prema poslužitelju Bitcoin Core.
	2	laboratorijske vježbe	Postavljanje razvojnog okruženja za pristup programskom sučelju poslužitelja Bitcoin Core.
	2	laboratorijske vježbe	Rad s programskim sučeljem poslužitelja Bitcoin Core. Priprema za obranu vježbi.
	4	laboratorijske vježbe	Obrana vježbi i nadoknade.

Vrste izvođenja nastave:	☒ predavanja ☒ seminari ☒ laboratorijske vježbe ☒ mješovito e-učenje	☒ samostalni zadaci ☐ multimedija ☒ mentorski rad

<table>
<tr><td>Obveze studenata</td><td colspan="6">obavljanje i obrana svih propisanih laboratorijskih vježbi
uspješna izrada i obrana seminarskog rada
uspješna izrada i obrana projektnog zadatka
nazočnost na predavanjima u iznosu od najmanje 70% predviđene satnice (za izvanredne studente 50%)</td></tr>
<tr><td rowspan="5">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>0,4</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>1,6</td></tr>
<tr><td>Projektni zadatak</td><td>1,6</td><td>Seminarski rad</td><td>0,3</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 colspan="6"></td></tr>
<tr><td>Ocjenjivanje i vrjednovanje rada studenata tijekom nastave i na završnom ispitu</td><td colspan="6"><table>
<tr><th colspan="3">KONTINUIRANA PROCJENA</th></tr>
<tr><th>Pokazatelji kontinuirane provjere</th><th>Uspješnost A_i (%)</th><th>Udjel u ocjeni k_i (%)</th></tr>
<tr><td>Seminarski rad</td><td>10 – 100</td><td>100</td></tr>
<tr><td>Nazočnost i aktivnost na predavanjima</td><td>70 – 100</td><td>0</td></tr>
<tr><td>Nazočnost i aktivnost na laboratorijskim vježbama</td><td>100</td><td>0</td></tr>
<tr><td>Laboratorijske vježbe (završna provjera usvojenih znanja i vještina)</td><td>100</td><td>0</td></tr>
</table></td></tr>
</table>

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

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 60%	*zadovoljava minimalne kriterije*	dovoljan (2)
od 61% do 74%	*prosječan uspjeh s primjetnim nedostatcima*	dobar (3)
od 75% do 89%	*iznadprosječan uspjeh s ponekom greškom*	vrlo dobar (4)
od 90% do 100%	*izniman uspjeh*	izvrstan (5)

<table>
<tr><td rowspan="4">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>Antonopoulos, A. M., „Mastering Bitcoin: Programming the Open Blockchain“, O'Reilly Media, 2017.</td><td>3</td><td>Elektroničko izdanje na webu pod licencom Creative Commons Attribution-ShareAlike 4.0 (CC BY-SA 4.0)</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"></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 (hrvatska i engleska inačica) su u cilju informiranja javnosti izravno dostupni na web stranicama Odjela.</td></tr>
</table>