

OPĆE INFORMACIJE		
Nositelj kolegija	Nikola Grgić, viši predavač	
Naziv kolegija	Kriptovalute	
Studijski program	Stručni diplomski studij Primijenjeno računarstvo	
Status kolegija	obavezni	
Godina studija	2.	
Semestar	3.	
Bodovna vrijednost i način izvođenja nastave	ECTS koeficijent opterećenja studenata	6
	Broj sati (P+LV+S)	24+20+16
OPIS KOLEGIJA		
Ciljevi kolegija		
• 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 blockchaine • prepoznavanje sigurnosnih rizika kod korištenja kriptovaluta • shvaćanje društvenih i ekonomskih aspekata razvoja i šireg prihvaćanja kriptovaluta		
Uvjeti za upis kolegija		
• znanje programiranja i izrade mobilnih ili web aplikacija		
Očekivani ishodi učenja za kolegij		
1. Usporediti specifičnosti i karakteristike važnijih kriptovaluta. 2. Objasniti osnovne pojmove vezane za kriptovalute zasnovane na tehnologiji blockchain. 3. Primijeniti teoretska znanja vezana za rad protokola Bitcoin u interpretaciji događaja na mreži i u razvoju vlastitih programskih rješenja. 4. Utvrditi vezu između različitih događaja na blockchainu i objasniti njihov odnos. 5. Izdvojiti povezane podatke iz blockchaine i prikazati rezultate na jasan i pregledan način. 6. Razviti aplikaciju i postaviti sustav za pristup Bitcoin blockchainu neovisan o trećoj strani.		
Sadržaj kolegija		
Povijest novca. Razvoj kriptovaluta. Bitcoin whitepaper. Pregled osnovnih pojmova vezanih za kriptovalute i Bitcoin. Novčanici (engl. wallet). Vrste novčanika. Preporuke za odabir softverskog novčanika. Generiranje privatnog ključa. Standardni i deterministički novčanici. Standardna implementacija protokola Bitcoin. Funkcionalnosti standardne implementacije. Puni čvor (engl. full node). Podatkovni direktorij čvora Bitcoin Core. Programsko sučelje poslužitelja Bitcoin Core. Pokretanje programa Bitcoin Core u poslužiteljskom načinu rada. RPC pozivi. Mreža Bitcoin testnet. Transakcije. Ulazi i izlazi. Transakcijska naknada i red čekanja (engl. mempool). Nepotrošeni izlazi transakcije. Elementi transakcije. Transakcijske skripte i skriptni jezik. Svojstva skriptnog jezika u Bitcoinu. Postupak provjere valjanosti transakcije. Ključevi i adrese. Kriptografija javnog ključa. Kodiranje Base58. Tehnologije za		

generiranje i pohranu ključeva. Vrste čvorova i njihove uloge u mreži. Bitcoin čvorovi s cjelovitom povijesti transakcija (engl. full nodes). Lagani Bitcoin klijenti. Blockchain. Zaglavlje i struktura bloka. Merkle tree. Rudarenje. Dokaz rada. Konsenzus. Prilagođavanje težine rudarenja. Natjecanje za prostor u bloku i troškovi rada mreže. Podjela mreže (engl. fork). Segwit, Lightning network. Društveni i ekonomski aspekti razvoja i prihvatanja kriptovaluta. Prijedlozi za unaprjeđenje protokola Bitcoin (BIP). Ostale kriptovalute (engl. altcoins). Specifičnosti i karakteristike važnijih predstavnika ostalih kriptovaluta.

Vrste izvođenja nastave (staviti X)	☒ predavanja ☒ seminari i radionice ☐ vježbe ☐ obrazovanje na daljinu ☐ terenska nastava	☒ samostalni zadaci ☐ multimedija i mreža ☒ laboratorijske vježbe ☒ mentorski rad ☐ ostalo _____
-------------------------------------	---	---

Obveze studenata

- **obavljanje i obrana svih propisanih laboratorijskih vježbi**
- **uspješna izrada i obrana seminarskog rada**
- **uspješna izrada i obrana projektnog zadatka**
- **nazočnost na nastavi sukladno Pravilniku o studijima i sustavu studiranja na Odjelu**

Praćenje rada studenata (dodati X uz odgovarajući oblik praćenja)

Pohađanje nastave	x	Aktivnost u nastavi		Seminarski rad	x	Eksperimentalni rad	
Pismeni ispit		Usmeni ispit		Esej		Istraživanje	x
Projektni zadatak	x	Kolokviji		Referat		Praktični rad	
Portfolio		Samostalno učenje	x	Konzultacije i završni ispit	x		

Ocjenjivanje i vrednovanje rada studenata tijekom nastave i na završnom ispitu / Način provjere stečenih ishoda učenja za svaku studentsku obvezu

KONTINUIRANA PROCJENA		
Pokazatelji kontinuirane provjere	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
Seminarski rad	20 – 100	10
Projektni zadatak	20 – 100	20
Laboratorijske vježbe (završna provjera usvojenih znanja i vještina)	50 – 100	10

ZAVRŠNA PROCJENA		
Pokazatelji provjere - završni ispit (prvi i drugi ispitni termin)	Uspješnost A_i (%)	Udjel u ocjeni k_i (%)
<i>Ispit</i>	<i>40 – 100</i>	<i>60</i>
<i>Seminarski rad (iz k.p.)</i>		<i>10</i>
<i>Projektni zadatak (iz k.p.)</i>		<i>20</i>
<i>Laboratorijske vježbe (iz k.p.)</i>		<i>10</i>

Ocjena se 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 62%	<i>zadovoljava minimalne kriterije</i>	dovoljan (2)
od 63% do 74%	<i>prosječan uspjeh s primjetnim nedostacima</i>	dobar (3)
od 75% do 87%	<i>iznadprosječan uspjeh s ponekom greškom</i>	vrlo dobar (4)
od 88% do 100%	<i>izniman uspjeh</i>	izvrstan (5)

Obvezna literatura i broj primjeraka u odnosu na broj studenata koji trenutačno pohađaju nastavu na kolegiju

Naslov	Broj primjeraka	Broj studenata
<i>Antonopoulos, A. M., „Mastering Bitcoin: Programming the Open Blockchain“, O'Reilly Media, 2017.</i>	<i>3</i>	
<i>Nakamoto, S.: „A Peer-to-Peer Electronic Cash System“, 2008.</i>		
<i>Nastavni materijali s predavanja</i>		

<i>Dopunska literatura</i>
<i>Načini praćenja kvalitete koji osiguravaju stjecanje izlaznih znanja, vještina i kompetencija</i>
• <i>evidencija pohađanja nastave i uspješnosti izvršenja ostalih obveza studenata (nastavnik).</i> • <i>ažuriranje detaljnih izvedbenih planova nastave - DIP (nastavnik).</i> • <i>nadzor izvođenja nastave (zamjenik pročelnika Odjela za nastavu, pročelnici odsjeka).</i> • <i>kontinuirana provjera kvalitete svih parametara nastavnog procesa u skladu s Akcijskim planovima (pomoćnik pročelnika Odjela za kvalitetu).</i> • <i>semestralno provođenje studentske ankete</i>