

KATALOG ZNANJA

1. IME PREDMETA IZ ODPRTEGA KURIKULA

TEMELJI TEHNOLOGIJE VERIŽENJA BLOKOV

2. CILJI PREDMETA

Splošni cilji predmeta so:

- razviti navade za sprotno spremljanje novosti na strokovnem področju;
- ozavestiti pomen nenehnega izpopolnjevanja svojega znanja in veščin;
- razviti sposobnost samostojnega reševanja strokovnih vprašanj in načrtovanja, organizacije dela ter sodelovanja v timu;
- razviti veščine za kritično, analitično in sintetično razmišljanje.

Specifično strokovno usmerjeni cilji so:

- razumeti temeljne koncepte porazdeljenih knjig (distributed ledger) in vlogo tehnologije veriženja blokov v sodobnih informacijskih sistemih;
- razviti sposobnost kritičnega vrednotenja različnih verig blokov, njihovih modelov soglasja (konsenza) in ustreznosti za specifične primere uporabe;
- spodbujati uporabo kriptografskih pristopov za zagotavljanje integritete, avtentičnosti in nepreklicnosti podatkov;
- krepiti spretnosti praktičnega eksperimentiranja z zasebnimi verigami blokov ter izvajanjem osnovnih pametnih pogodb;
- ozavestiti varnostna, energetska in etična vprašanja, povezana z uporabo tehnologije veriženja blokov.

3. PREDMETNO SPECIFIČNE KOMPETENCE

Pri predmetu si študenti poleg generičnih pridobijo naslednje kompetence:

- razumevanje strukture bloka in delovanja verige blokov ter transakcijskega modela;
- uporaba osnovnih kriptografskih mehanizmov (hash funkcije, digitalni podpisi, Merklava drevesa) v kontekstu verig blokov;
- razlikovanje in primerjava konsenznih algoritmov (Proof-of-Work, Proof-of-Stake, BFT-družina);
- vzpostavitev in konfiguracija zasebnega testnega omrežja (npr. Ethereum lokalna veriga, Hyperledger Fabric test-net);
- načrtovanje, implementacija in testiranje enostavnih pametnih pogodb (npr. v Solidity) in interakcija z njimi prek denarnic / odjemalcev;
- sposobnost analize varnostnih tveganj (51-odstotni napad, Sybil, vrednostne manipulacije) in potenciala za energetske optimizacije;
- razumevanje regulativnih okvirjev ter implikacij varovanja osebnih podatkov v verigah blokov.

4. OPERATIVNI CILJI

INFORMATIVNI CILJI	FORMATIVNI CILJI
Študent:	Študent:
1. Uvod v veriženje blokov	
- definira pojme blok, veriga blokov, porazdeljena knjiga; - navede ključne dogodke v razvoju (Bitcoin, Ethereum); - pojasni razliko med centraliziranimi in decentraliziranimi sistemi; - prepozna akterje (vozlišče, rudar/validator, odjemalec).	analizira primer verige blokov (npr. javni explorer).
2. Kriptografske osnove	
- razloži funkcije zgoščanja in lastnosti (pre-slika, trk); - opiše digitalne podpise (ECDSA) in Merklova drevesa; - definira pojem „dokaz o delu“; - zgradi Merklovo drevo in preveri dokaz o vključenosti (Merkle proof).	izračuna hash niza podatkov (npr. SHA-256) in preveri podpis.
3. Struktura bloka in transakcije	
- opiše polja glave bloka (timestamp, nonce, hash prejšnjega bloka); - razloži potek transakcije od ustvarjanja do potrditve; - našteje mehanizme pristojbin; - ustvari in pošlje testno transakcijo na zasebnem omrežju.	razčleni blok iz javne verige (JSON-izpis).
4. Mehanizmi konsenza in algoritmi	
- analizira dejavnike varnosti in skalabilnosti; - poveže koncept finalnosti s konsenzom; - meri čas potrditve in porabo virov pri različnih nastavitvah.	konfigurira testno omrežje z alternativnim konsenzom.
5. Pametne pogodbe	
- definira pojem smart contract in vlogo virtualnega stroja (EVM); - razloži osnovne tipe podatkov in dogodke v Solidity; - navaja varnostne ranljivosti (reentrancy, integer overflow); - izvede testne klice funkcij prek tržnice tržnih enot (remix, Hardhat, MetaMask).	napiše in razhrošči preprosto pogodbo (npr. števec, token ERC-20).

6. Varnost in regulativa	
• navede glavne napade (51 %, Sybil, BGP hijack); • opiše vpliv GDPR na shranjevanje osebnih podatkov; • razloži koncept nezamenljivosti in pravico do pozabe; • argumentira skladnost svojega projekta z relevantnimi predpisi.	• izvede preprost varnostni pregled pogodbe z orodjem Mythril ali Slither.
7. Skalabilnost in layer 2	
• definira pojme sidechain, rollup, state channel; • primerja trilemo decentralizacija-varnost-skalabilnost; • opiše pristop „sharding“; • analizira učinek na stroške in hitrost transakcij.	• simulira prenos sredstev prek testnega rollupa.
8. Integrirani projekt	
• navaja faze razvoja DApp (analiza, načrt, implementacija, testiranje, vzdrževanje).	• samostojno (ali v paru) razvije delujoč prototip (npr. glasovalni sistem, enostavna NFT-tržnica, sledljivostni sistem dobavne verige) in pripravi tehnično dokumentacijo z diagrami ter navodili za uporabo.

5. OBVEZNOSTI ŠTUDENTOV IN POSEBNOSTI V IZVEDBI

Število kontaktnih ur: 66 ur (33 ur predavanj, 33 ur vaj).

Število ur samostojnega dela: 79 ur (20 ur študij literature, 30 ur vaj, 29 ur projektna naloga,).

Skupaj 145 ur dela študenta (5 KT).

Obveznosti za pristop k izpitu

- aktivna prisotnost na vajah (min. 80 %);
- sprotna oddaja laboratorijskih poročil;
- izdelava in predstavitev projektne naloge;
- končni pisni izpit iz teorije in prakse.

Načini preverjanja in ocenjevanja:

- laboratorijske naloge 25 %;
- projekt 35 %;
- sprotni kvizi 10 %;
- končni izpit 30 %.

1. KADROVSKI POGOJI

Izvajalec	Znanje s področja
Predavatelj	visokošolskega izobraževanja računalništva, informatike, elektrotehnike, matematike, fizike, strojništva, mehatronike, menedžmenta, gospodarskega inženirstva, biosistemskega inženirstva, podatkovnih ved, statistike, bioinformatike ali telekomunikacij
Inštruktor	visokošolskega izobraževanja računalništva, informatike, elektrotehnike, matematike, fizike, strojništva, mehatronike, menedžmenta, gospodarskega inženirstva, biosistemskega inženirstva, podatkovnih ved, statistike, bioinformatike ali telekomunikacij