Raspodijeljene glavne knjige i kriptovalute
Međuispit – 29. studeni 2018.

1. **(8 bodova)** Razmatramo Bitcoin sustav:

a) **(2 boda)** Koliko je dogovoreno očekivano vrijeme između blokova?

b) **(3 boda)** Čemu služi težina rudarenja (eng. *difficulty*)?

c) **(3 boda)** Do kojih bi problema došlo u mreži da je očekivano vrijeme rudarenja bloka 1 sekunda?

2. **(8 bodova)** Rudarite blokove kriptovalute koja koristi *proof-of-work* sustav. Hashrate vaše opreme je 1 Ghash/s, a čitava mreža svih rudara ima hashrate 6 Thash/s.

a) **(1 bod)** Ukoliko je vrijeme između blokova 1 min, koliko vremena vam u očekivanju treba da izrudarite 1 blok?

b) **(3 boda)** Što su bazeni rudara, tko njima upravlja te zašto biste se vi kao individualni rudar priključili bazenu rudara?

c) **(2 boda)** Kako rudari u bazenu dokazuju svoj udio računalne snage uložene u rudarenje?

d) **(2 boda)** Zašto rudar u bazenu, ukoliko pronađe *nonce* koji daje hash odgovarajuće vrijednosti, ne bi jednostavno promijenio adresu u *coinbase* transakciji i sam sebi uplatio čitavu nagradu za blok?

3. **(8 bodova)** Niste zadovoljni činjenicom da *proof-of-work* sustavi troše jako puno energije i razmatrate alternativne pristupe rudarenju:

a) **(3 boda)** Objasnite ukratko principe virtualnog rudarenja. Zašto bi sustavi virtualnog rudarenja bili otporni na rudarenje pomoću ASIC-a?

b) **(3 boda)** Što je *coin-age* i na koji način Peercoin implementira *proof-of-stake* principe?

c) **(2 boda)** Zašto je kod *proof-of-stake* sustava rudarima u interesu uvijek pokušavati stvoriti fork (tzv. "nothing at stake" problem)?

4. **(8 bodova)** Baka je unuku Josipu odlučila ostaviti svoju imovinu, no htjela se pobrinuti da Josip ne dobije nasljeđe prije nego odraste. Budući da je (kao svaka moderna baka) upoznata s Bitcoinom, napisat će *locking* (*scriptPubKey*) skriptu koju će Josip moći otključati tek kada postane punoljetan, svojim potpisom i potpisom jednog od svoja dva roditelja. Josip će postati punoljetan otprilike kada će biti izrudaren blok 600.000.

a) **(3 boda)** Napišite opisanu *locking* (*scriptPubKey*) skriptu.

b) **(3 boda)** Napišite *unlocking* (*scriptSig*) skriput koja će otključati skriptu iz a) zadatka.

c) **(2 boda)** Ukoliko bi baka htjela "spaliti" novce, odnosno napisati ispravnu skriptu čija sredstva nije moguće potrošiti, kako bi takva *locking* (*scriptPubKey*) skripta izgledala?

5. **(8 bodova)** Bitcoin Improvement Proposal (BIP) je dokument kojim se predlažu promjene Bitcoin standarda. BIP 34 je dodao sljedeće pravilo (malo pojednostavljeno): prvi element *scriptSig* polja svake *coinbase* transakcije mora biti visina bloka koji sadrži tu transakciju. Ova promjena je predložena kako ne bi bilo više moguće da dvije transakcije imaju isti identifikator. Recimo da se ova promjena počela primjenjivati počevši od bloka 200.000.

a) **(1 bod)** Što je indentifikator Bitcoin transakcije i kako se računa?

b) **(2 boda)** Zašto je bitno da svaka transakcija ima jedinstven identifikator? Opišite problem do kojeg dolazi ako dvije transakcije u lancu imaju isti identifikator.

c) **(2 boda)** Je li moguće da dvije *coinbase* transakcije u istom lancu u blokovima nastalima nakon bloka 200.000 imaju isti identifkator? Obrazložite odgovor.

d) **(2 boda)** Ako se BIP 34 primjenjuje od početka lanca, je li moguće da dvije obične (ne *coinbase*) transakcije u istom lancu imaju isti identifikator? Ako je moguće konstruirajte primjer, ako nije moguće detaljno obrazložite zašto.

e) **(1 bod)** Spada li BIP 34 u hard fork ili soft fork promjenu pravila? Obrazložite odgovor.