

# Raspodijeljene glavne knjige i kriptovalute

## Prva laboratorijska vježba: Bitcoin transakcije

Listopad 2022.

### Priprema okruženja

Laboratorijsku vježbu možete pisati u bilo kojem programskom jeziku, ali ćete podršku od asistenata imati samo za programski jezik Java. Ako se ipak odlučite za rad u nekom drugom programskom jeziku koji nije kompatibilan s Javom (poput Kotlin-a i Scala-e) morat ćete se sami pobrinuti da pronađete sve potrebne biblioteke te ćete morati napisati ekvivalentne testove kao one dane u početnom kodu.

Preporuča se korištenje razvojnog okruženja *IntelliJ IDEA*. Kao studenti imate pravo na korištenje edukativne licence za sve *JetBrains* proizvode. Pravo na licencu možete dobiti prijavom putem svoje FER email adrese na stranici <https://www.jetbrains.com/student/>. Uz IDE se preporuča korištenje *Maven* sustava za upravljanje ovisnostima.

Uz svaku laboratorijsku vježbu studenti će dobiti zadatak i početni kod pisan u programskom jeziku Java (verzije 1.8) s Maven podrškom. Unutar projekta će se nalaziti `pom.xml` datoteka u kojoj su zapisane sve ovisnosti projekta. Kako bi postavili projekt potrebno je:

- pokrenuti *IntelliJ IDEA*,
- kliknuti na “Import Project” te
- navigirati do datoteke `pom.xml` te je otvoriti.

Nakon toga će se projekt otvoriti te će se automatski dohvatiti sve ovisnosti potrebne za normalno pokretanje projekta.

### Uvod

Cilj vježbe je upoznati se s Bitcoin transakcijama i *Bitcoin Script* jezikom. Dobiveni početni kod koristi `bitcoinj` Java biblioteku (čija je dokumentacija dostupna na <https://bitcoinj.github.io>). U razredu `WalletKit` implementirana je logika spajanja na testni blockchain, na kojeg se spaja kroz adresu `bujica.zemris.fer.hr:8080` koristeći `bitcoinj` biblioteku. Kako biste se upoznali s `bitcoinj` bibliotekom, u početnom kodu možete naći primjer implementirane *Pay-to-Public-Key* (P2PK) transakcije unutar razreda `PayToPubKey`. Implementirane su metode za generiranje *locking* (*scriptPubKey*) i *unlocking* (*scriptSig*) skripti - iako se *unlocking* skripta koristi tek pri trošenju novčića u idućoj transakciji. Kako bi se testirale obje skripte, primijetite da se u testovima izvršavaju dvije transakcije - prvo se novčići zaključavaju implementiranom *locking* skriptom, a potom se vraćaju pomoću *unlocking* skripte natrag na vlastitu adresu u sklopu novčanika (pogledajte implementaciju u `ScriptTest#testTransaction` metodi).

## Upute

U sklopu prve laboratorijske vježbe potrebno je izvršiti nekoliko transakcija. Kako bi mogli izvršavati transakcije potrebni su vam novčići. Da bi dohvatili novčiće prvo morate napraviti novčanik koji ima adresu na koju je moguće uplatiti novčić. Novčanik možete napraviti tako da pokrenete `ScriptTests#printAddress` test. Pokretanjem testa `bitcoinj` biblioteka će stvoriti novčanik u direktoriju projekta (samo prvi put kad pokrenete test) pod imenom "wallet". Datoteke `password.spvchain` i `password.wallet` spremaju informaciju o novčaniku i stanje raspodijeljene glavne knjige (*engl. blockchain*). Nakon što se test izvrši pronađite liniju s adresom vašeg novčanika. U trenutku kada vam je poznata adresa vašeg novčanika, novčiće možete dobiti tako da upišete vaš JMBAG i adresu novčanika u formu na adresi <https://bujica.zemris.fer.hr/faucet>.

## Zadaci

U sklopu ove laboratorijske vježbe potrebno je implementirati *locking* i *unlocking* skripte za zadane transakcije, te pokrenuti odgovarajuće testove implementirane u sklopu početnog koda. Minimalni uvjet za polaganje vježbe je ispravno riješen prvi zadatak.

1. Implementirajte *Pay-to-Public-Key-Hash* (P2PKH) transakciju koja će poslati mali broj novčića na proizvoljnu adresu. Adresu možete generirati upotrebom `bitcoinj` biblioteke tako da stvorite novi `ECKey` objekt. Sav kod morate napisati unutar razreda `PayToPubKeyHash`. Provjerite svoju implementaciju transakcije tako da pokrenete `ScriptTests#testPayToPubKeyHash` test. Izvršenu transakciju možete provjeriti koristeći blockchain explorer na adresi <https://bujica.zemris.fer.hr>.
2. Alice i Bob vlasnici su tvrtke i sukladno tome žele da se sva sredstva čuvaju u transakciji koja zahtjeva njihove potpise da bi se potrošila. No, oboje su također svjesni da bi u slučaju „iznenadnog nestanka“ druge strane ta sredstva mogla ostati zauvijek zaključana! S obzirom na to Alice i Bob odluče se objaviti *TimeLock* transakciju koja, osim što se uvijek može uspješno izvršiti s njihovim potpisima, ima i dodatno svojstvo da se nakon 1.10.2014 u 00:00:00 (UTC) može uspješno izvršiti s potpisom samo jednog od vlasnika (Alice ili Boba) i treće strane — odvjetnice Eve.

Vaš zadatak je napisati *locking* skriptu navedene *TimeLock* transakcije koja će omogućiti opisanu funkcionalnost. Preciznije, *locking* skripta mora raditi sljedeće.

1. Ako je na vrhu stoga 0 onda zahtjeva potpise od Alice i Boba koristeći `OP_CHECKMULTISIG`.
2. Ako je na vrhu stoga 1 onda:
  - (a) Koristi `OP_CHECKLOCKTIMEVERIFY` s argumentom koji predstavlja *Unix time* od 2014-10-01T00:00:00Z (UTC);
  - (b) Provjerava *hash* javnog ključa i valjanost potpisa od Eve (vidi P2PKH);
  - (c) Zahtjeva potpis jednog od vlasnika (Alice ili Boba) koristeći `OP_CHECKMULTISIG`.

Što konkretno radi `OP_CHECKLOCKTIMEVERIFY`? Kakvu ulogu ima `nLockTime`? Pročitajte <https://en.bitcoin.it/wiki/NLockTime>.

Rješenje zadatka treba se nalaziti u razredu *TimeLock*. Provjerite svoju implementaciju koristeći `ScriptTest#testTimeLock*` testove.

3. Alice i Bob žele uz Vašu pomoć igrati igru „bacanja novčića“ koristeći Bitcoin. Pravila igre su sljedeća: sudionici se unaprijed dogovore tko će biti „pismo“ (Alice), a tko „glava“ (Bob); svaki sudionik odabere broj: 0 ili 1; ako je operacija „logičko ili“ (**OR**) odabranih brojeva 0 pobjeđuje „pismo“, inače pobjeđuje „glava“. Da bi spriječili situaciju u kojoj jedan sudionik vidi broj od drugog te sukladno tome promijeni svoj izbor, Alice i Bob slože se da će koristiti shemu obvezivanja (*commitment scheme*):

1. Odaberi tajni broj  $N \in \{0, 1\}$ .
2. Generiraj nonce  $R$  veličine  $N + 16$  bajtova (dakle 16 ili 17 bajtova).
3. Izračunaj javno obvezivanje (*public commitment*)  $C = \text{HASH160}(R)$ .

Na ovaj način osigurali smo da Alice (Bob) ne vidi odabrani broj Boba (Alice) prije početka igre te da ne može naknadno promijeniti svoj odabrani broj. Vaš zadatak je, za zadanu *unlocking* skriptu koja sadrži redom: potpis igrača,  $R_A$  i  $R_B$ , napisati *locking* skriptu koja se uspješno izvršava ako potpis iz *unlocking* skripte pripada pobjedniku igre (Alice ili Bob). *Locking* skripta treba raditi sljedeće:

1. Osigurati da  $R_A$  i  $R_B$  odgovaraju redom  $C_A$  i  $C_B$ .
2. Izračunati  $N_A$  i  $N_B$  iz redom  $R_A$  i  $R_B$ .
3. Odrediti tko je pobjednik.
4. Provjeriti ispravnost potpisa u *unlocking* skripti za javni ključ pobjednika.

Rješenje zadatka treba se nalaziti u razredu CoinToss. Provjerite svoju implementaciju koristeći `ScriptTest#testCoinToss*` testove.

## Naputci

- Informacije o naredbama koje Bitcoin Script podržava možete naći na stranici <https://en.bitcoin.it/wiki/Script>.
- Za potrebe laboratorijske vježbe koristi se privatni testnet na kojem se blokovi rudare s najmanjom težinom (vrijeme potrebno za rudarenje je minimalno). Takav oblik testneta se zove *regtest*, i vrlo je pogodan za testiranje. Regtest je u laboratorijskoj vježbi korišten iz razloga što se rezultati transakcije mogu vidjeti u vrlo kratkom roku (svakih 3 minute se rudari novi blok, za razliku od testneta gdje je brzina rudarenja  $\sim 10$  min/blok). Više o regtestu i kako ga možete podesiti na svom računalu možete naći na <https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch09.asciidoc> i <https://samsclass.info/141/proj/pBitc1.htm>.
- Nakon pokretanja `ScriptTests#printAddress` ponekad trebate malo pričekati da Vam novčići „sjednu na račun“.

## Predaja i obrana

Laboratorijsku vježbu možete rješavati sami ili u grupi od najviše dva studenta. Ako se odlučite raditi laboratorijsku vježbu u grupi, morate ispuniti obrazac: <https://forms.gle/sNGNbQkfKdsX4rmW6>. **Obrazac morate ispuniti najkasnije do 10.11.2022 u 23:59.**

Laboratorijsku vježbu predajete putem sustava Moodle tako da učitate, *.zip* datoteku koja mora sadržavati samo izvorni kod laboratorijske vježbe. Naziv predane datoteke mora biti u obliku *ime-prezime-jmbag.zip*. Ukoliko radite u grupi, neka naziv datoteke bude ime, prezime i JMBAG jednog od studenata iz grupe. **Rok za predaju laboratorijske vježbe je 13.11.2021 do 23:59.**

Laboratorijska vježba ocijeniti će se na temelju predanog izvornog koda i usmene obrane koja obuhvaća pitanja vezana za gradivo laboratorijske vježbe. **Prag za prolaz laboratorijske vježbe je riješen prvi zadatak.**

Pitanja za laboratorijsku vježbu moguća su putem elektroničke pošte [rgkk@fer.hr](mailto:rgkk@fer.hr) ili konzultacija uz prethodni dogovor putem elektroničke pošte.