


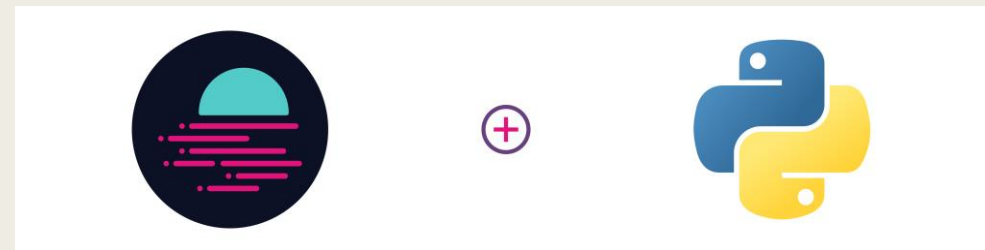


LUTRIJA IMPLEMENTIRANA NA ETHEREUM BLOCKCHAIN-U UZ POMOĆ PAMETNIH UGOVORA (SMART CONTRACTS)

Fakultet inženjerskih nauka
Profesor Vladimir M. Milovanović
Student Uroš Stanojkov 601/2018



Korišćene tehnologije



Testiranje softvera

- Svaki kreirani softver bi trebalo da prođe kroz nekoliko faza pre nego što se postavi na mainnet
1. Testiranje na lokalu uz pomoć Ganache-a
 2. Testiranje na testnetu
 3. Postavljanje ugovora na testnetu i izvršavanje transakcija
 4. Postavljanje ugovora na mainnet-u

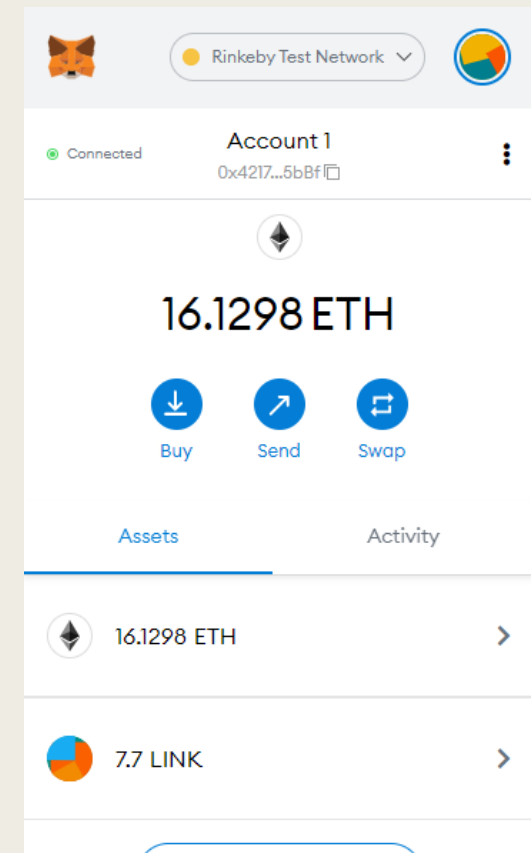
Ethereum-ov blockchain

- Pametni ugovori
- Novčanici (Adrese i privatni ključevi)
- Postavljanje ugovora na blockchain
- Vršenje transakcija
- Gas i naknada za transakcije

Kako dobiti sopstveni novčanik?

- Sopstvenu adresu kao i privatni ključ možemo dobiti instaliranjem mobilne aplikacije ili ekstenzije pretraživača pod nazivom **MetaMask**
- Test kriptovalute

- **NIKAD NE DELI PRIVATNI KLJUČ JAVNO, KAO NI SEKVENCU KOJU KORISNIK DOBIJA PRI PRAVLJENJU NALOGA!**



Projekat Lutrija

- Čemu služi ovaj projekat?
- Koja je razlika da li je projekat Lutrija ili bilo koja igra na sreću napravljena pomoću pametnih ugovora ili uz pomoć neke druge tehnologije?
- Kako da budem 100% siguran da su igre na sreću sigurne?
- Da li su igre na sreću koje su napravljene uz pomoć pametnih ugovora sigurne?

Lokalni blockchain

- Pomoću Ganache-a je moguće imitirati blockchain, ali na lokalu
- Testiranje se vrši na lokalu, glavni razlog je brzina, kao i to što se ne plaćaju transakcije
- Ganache sadrži nekoliko adresa i njihove ključeve
- Za developere je vrlo praktičan, ne postoji nikakva šansa izgubiti pravi novac

```
Ganache CLI v6.12.2 (ganache-core: 2.13.2)

Available Accounts
=====
(0) 0xf9bF5615c4AEb3C5f2651C311D0dC959Deb489bc (100 ETH)
(1) 0xB1666c26D9733548C61A4bCEA63A63892aAdb5F0 (100 ETH)
(2) 0xB6EdeF2b8103aea198f404C1feE30Ea44f48b5bd (100 ETH)
(3) 0x0Cd34aaE598394aDa7a503f886b4F889baA9c8b2 (100 ETH)
(4) 0x7150CB05Fab8a9d672f865febE2dFA88c95b6780 (100 ETH)
(5) 0x8FcBf0478C59517bD35072D6e43D0B9057607c2d (100 ETH)
(6) 0x880a8e4C8b271fc810602b48bB91EE83BF78d5dC (100 ETH)
(7) 0x8Fc927f4a1f71d4eC8255f86A1C018E16F26A418 (100 ETH)
(8) 0xFf168b1Fe376F1B1CE8D2AAB5a55D3ef0Ff52A02 (100 ETH)
(9) 0xBE1f11EeE51aaA57B94f9cB931551074F97E1f13 (100 ETH)

Private Keys
=====
(0) 0xfd151b927173fec343f239da0f353d944ae617094d64968dbad14db587d3bdce
(1) 0x7b3a20758ab624d7bab84ae659fd7ad666dbc7308b969cf9bfed05835ea4a316
(2) 0x86a170d96ce2e245b12f1b89b3fb12b255e274f5da9275b664e8533af286b3f0
(3) 0xd9ff1f87746ad5d594ac60510dd1ffd851c11f054bbe5ec87d493104302faa1f
(4) 0x8613a58e6ef47872ab59247b36e25e9c130f2406a534dcbaf3d8fe573f818ca5
(5) 0x899fd4d1d9bc0b0e31c99d331ff847c5ccbdf368d676f6c50fc614314428496
(6) 0xb52c12bb874112a160b6cf4d03d9970613029cc856aa51887e0524ff2fcdf36d
(7) 0x60d5f75b545f586c4d90fbfd3494592d899fe33943d817b9db95b819f16fffe4
(8) 0xfd89379bc19b52da09ecc3022ecf1a4c4bd70e02caa72000b3751ba9cb2e6a38
(9) 0x39be9424dd440058ae5c9840ef0f7130c06934b629526372277ea694c4b36a8

HD Wallet
=====
Mnemonic:      art enhance inspire damage mixed cry illegal jump noise immune oak sense
Base HD Path:  m/44'/60'/0'/0/{account_index}

Gas Price
=====
2000000000

Gas Limit
=====
6721975

Call Gas Limit
=====
9007199254740991

Listening on 127.0.0.1:8545
> 
```

Testnet i test kriptovalute

- Testnet predstavlja alternativni pristup Blockchain-u gde se može vršiti takođe testiranje ugovora, raznih transakcija
- Koriste se test kriptovalute (fauceti)
- Mainnet
- Testnet-ovi za Ethereum su: Görli, Kovan, Rinkeby, Ropsten
- Gas za transakcije na Ethereumu

Dobijanje nasumičnog pobjednika

- Da li je algoritam keccak256 odgovarajući za dobijanje nasumičnog pobjednika?
- Request-Receive metoda
- VRF Coordinator ugovor - funkcija koje zahtevaju nasumični broj i funkcija koja vraća nasumični broj
- Potrebno je sačekati dovoljno vremena da se ovaj algoritam izvrši
- Nikad ne pozivati request više puta ako nismo dobili nasumični broj

Struktura projekta Lutrija

- Za projekat je korišćen Python framework Brownie pomoću kog je omogućena i pojednostavljena implementacija na Ethereum blockchain

```
> .pytest_cache
✓ build
  > contracts
  ✓ deployments
    > 4
    {} map.json
  > interfaces
  {} tests.json
✓ contracts
  ✓ test
    ◆ LinkToken.sol
    ◆ MockV3Aggregator.sol
    ◆ VRFCoordinatorMock.sol
    ◆ Lottery.sol
  > interfaces
  > reports
```

```
✓ scripts
  > __pycache__
  ◆ __init__.py
  ◆ deploy.py
  ◆ help.py
✓ tests
  > __pycache__
  ◆ test_lottery_integration.py
  ◆ test_lottery_unit.py
  ⚙ .env
  ◆ .gitattributes
  ◆ .gitignore
  ! brownie-config.yaml
  ⓘ README.md
```

Prednosti i mane projekta

- Prednosti: Poverenje, dostupnost koda, jasna implementacija i cilj
- Mane: Brzina

Postavljanje ugovora na Mainnet-u

- Kada se priča o ceni, rudarenju Ethereum-a, sve se to odvija na mainnet-u
- Sve transakcije na mainnet-u se naplaćuju pravi Ethereum-om koji ima stvarnu vrednost
- Mainnet ima dosta više čvorova nego testnet, što ga čini boljim
- Koja je cena da se izvrši neka transakcija, da se postavi ugovor na mainnet?
- Sve funkcioniše pomoću gasa

HVALA NA PAŽNJI!