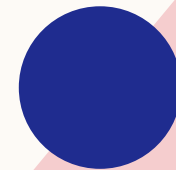


KVANTNI NOVAC

Mihajlo Madžarević
55/20RN

OPIŠ PROJEKTA

Kvantni novac je projekat čija je glavna suština implementacija standardnih bankarskih operacija kreiranja, izdavanja, verifikacije novčanica, kao i pokušaja falsifikovanja novca zarad provere zaštite sistema upotrebom kvantnih tehnologija. Kvantni novac pruža implementaciju prostog bankarskog sistema koji se koristi kvantnim tehnologijama u svrhu kriptografske zaštite novca. Projekat nam obraća pažnju na potencijalni savremeniji i bezbedniji sistem za zaštitu digitalnih valuta.



KORISNIČKI INTERFEJS

```
Welcome to the Quantum bank!  
Chose an action:  
1. See all your quantum money.  
2. Request a money note from the bank.  
3. Verify your money note.  
4. Try falsification of money.  
5. Exit  
Enter a number of an action:
```

Korisnički interfejs je jednostavam. Korisniku se ispisuju dostupne funkcionalnosti i njihov redni broj. Od korisnika se traži da unese redni broj akcije koju želi da obavi.

```
Enter a number of an action:2  
Bank note added to the wallet.
```

Primer: Zahtev izdavanja novčanice korisniku. Korisnik dobija potvrdu da je novčanica izdata.

```
Enter a number of an action:1  
Available money notes: 6
```

Primer: Korisnik zahteva pregled svojih dostupnih novčanica i dobija ispis ID-eva novčanica.

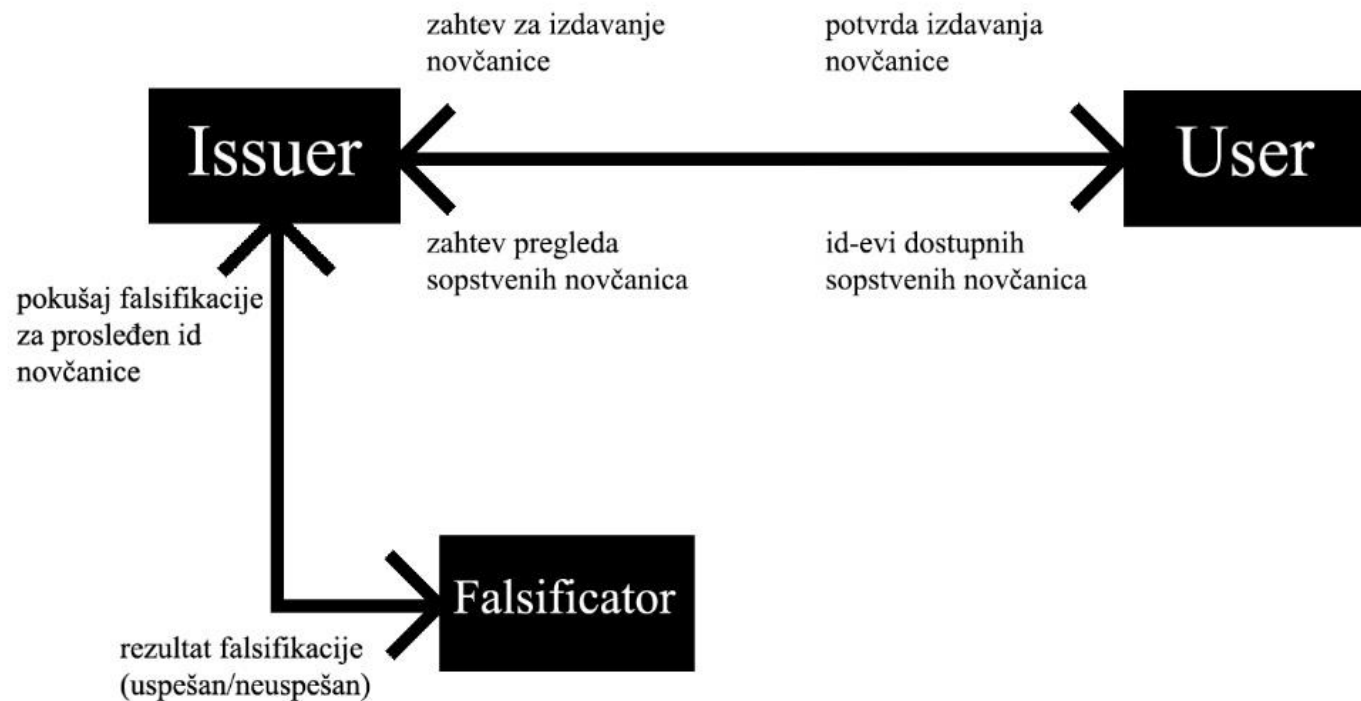
```
Enter a number of an action:3  
Enter money note id:6  
Valid!
```

Primer: Korisnik podlaže zahtev verifikacije svoje novčanice i dobija odgovor o validnosti od banke.

```
Enter a number of an action:4  
Enter money note id to try falsification:6  
Falsification failed.
```

Primer: Korisnik pokušava da falsifikuje svoju postojeću novčanicu i ne uspeva.

ALGORITAM

**Issuer():**`create_money(num_qubits):``land_money():``verify_money(money_note):``save_money_data():`**User():**`see_balance():``request_money(issuer):``check_money_validity(issuer, money_id):`**Falsificator():**`bank_attack(issuer,
money_id_to_try,
num_of_qubits):`

KLJUČNI SEGMENTI

```
# Calculate the state fidelity  
fidelity = state_fidelity(state_vector1, state_vector2)
```

Upoređivanje stanja dva kubita kako bi se utvrdilo da li su isti (koristi se za verifikaciju novčanica).
Upoređuju se uglovi između vektora dva kvantna stanja.

```
quantum_state = QuantumCircuit(2, 2)  
quantum_state.h(0)  
quantum_state.h(1)  
quantum_state.measure(0, 0)  
quantum_state.measure(1, 1)
```

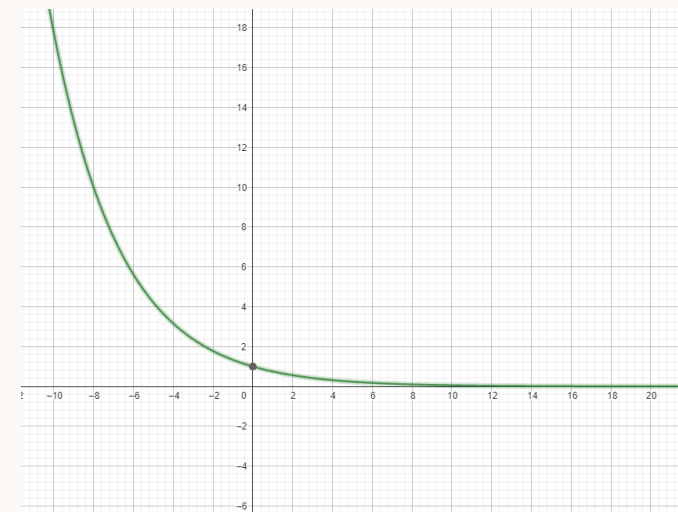
Primer generisanja nasumičnog broja od 0 do 4 upotrebom dva kubita. Ovo se koristi prilikom odabira nasumičnog kvantnog stanja novčanice i pri pokušaju falsifikacije novčanice nasumičnim pogađanjem kvantnog stanja novčanice poznatog id-a.

TESTOVI

Testiranje je vršeno u vidu pokušaja falsifikovanja novčanica korisnika. Falsifikacija novčanice koja za svoje kvantno stanje koristi samo jedan kubit nije bio izazov, puno uspeha falsifikacije sam ostvario kroz par pokušaja. Broj kubita sam povećao na pet i uočio promenu. Nisam uspeo da falsifikujem novčanicu a test sam probao oko dvadeset puta.

ZAKLJUČAK

Uočio sam kroz testove da povećanjem broja kubita smanjujemo mogućnost falsifikacije novčanica. Sa n kubita verovatnoća uspešne falsifikacije je $(3/4)^n$. Na grafu možemo videti kako se smanjuje mogućnost falsifikacije sa povećanje broja kubita (y osa). Još jedno zapaženje koje treba napomenuti je da bi potencijalni falsifikator morao da zna broj kubita u kvantnom stanju jedne novčanice što otežava falsifikaciju.





HVALA NA PAŽNJI

Mihajlo Madžarević 55/20RN