Kvantni novac

Veljko Živanović 122/20RN

Apstrakt - Ovaj projekat se fokusira na primenu kvantnog računarstva u razvoju inovativnih softverskih rešenja, koristeći Qiskit, biblioteku specijalizovanu za kvantne simulacije. Glavni cilj projekta je razvijanje softverske aplikacije koja koristi kvantne algoritme za obradu i analizu podataka, integrirajući pritom elemente klasičnog računarstva kao što su baze podataka i korisnički interfejsi. Kroz implementaciju i primenu kvantnih kola i algoritama u simuliranom kvantnom okruženju, projekat istražuje potencijale i izazove kvantnog računarstva u praktičnim aplikacijama.

Korišćenje SQLite3 baze podataka omogućava efikasno upravljanje podacima, dok Tkinter pruža interaktivni korisnički interfejs, čineći aplikaciju pristupačnom i upotrebljivom. Ovaj projekat ne samo da demonstrira tehničku izvodljivost integracije kvantnih i klasičnih tehnologija, već takođe istražuje nove paradigme u obradi podataka, nudeći uvide u buduću primenu kvantnog računarstva u različitim industrijskim i istraživačkim sektorima.

Ključne reči: Kvantno računarstvo, Qiskit, SQLite3, Tkinter, kvantni algoritmi, obrada podataka, softverska integracija.

I UVOD

U eri digitalne transformacije, kvantno računarstvo se pojavljuje kao revolucionarna tehnologija koja obećava značajna poboljšanja u brzini i efikasnosti obrade podataka u poređenju sa klasičnim računarima. Ovaj projekat se bavi jednim od ključnih izazova u kvantnom računarstvu: kako efikasno integrirati kvantne algoritme u tradicionalne računarske sisteme i aplikacije. Fokusiran je na razvoj softverske platforme koja kombinuje moć kvantnih kola i algoritama, implementiranih pomoću Qiskit biblioteke, sa pouzdanošću i pristupačnošću klasičnih baza podataka i korisničkih interfejsa.

II PREGLED LITERATURE

[1] U 1968. godini, Stephen Wiesner, tada postdiplomski student na Univerzitetu Columbia, predstavio je revolucionarnu ideju u svom istraživačkom radu. On je predložio korišćenje polarizovanih fotona za prenos podataka i uveo koncept kvantnog novca. Njegov rad, poznat kao "Conjugate coding", bio je znatno ispred vremena u kojem je nastao i nije odmah shvaćen niti prihvaćen od strane akademske zajednice. Tek nakon petnaest godina, 1983. godine, ovaj rad je objavljen, skoro tri decenije pre nego što su kvantni računari postali realnost. Ideje koje je Wiesner predstavio imale su značajan uticaj na razvoj kvantne teorije informacija, kvantnih kriptografskih metoda i kvantnih komunikacijskih protokola u narednim godinama.

[2] 2019 godine, kvantni računar je obavio složen zadatak za 4 minuta, dok bi superkompjuterima bilo potrebno 10.000 godina. Ovo brzo izračunavanje nudi velike mogućnosti, ali i predstavlja rizik za digitalnu komunikaciju. Trenutna kriptografija, koja štiti podatke od sajber napada, može biti ugrožena budućim kvantnim računarima koji bi mogli razbiti njene šifre za nekoliko sati. To bi ugrozilo digitalnu bezbednost, posebno u bankarstvu, što je kritično zbog obilja osetljivih informacija koje se oslanjaju na kriptografiju.

III METODOLOGIJA

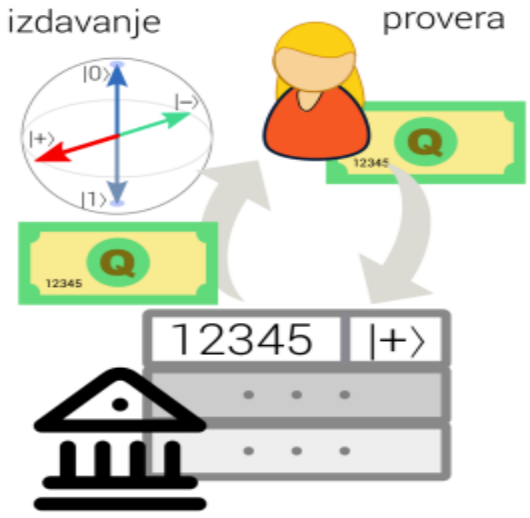
Korišćenje SQLite3 za upravljanje bazom podataka:U ovom projektu se implementira SQLite3 za kreiranje i upravljanje bazama podataka novcanice.db i novcanik.db. Ovo uključuje kreiranje tabele, unos podataka i njihovo pretraživanje ili ažuriranje.

Quantum Circuit creation using Qiskit: Koristi se Qiskit biblioteka za kreiranje kvantnih kola. Qiskit se koristi za simulaciju kvantnih stanja pomoću kvantnih kapija kao što su X kapija (koja menja stanje kubita) i Hadamardova kapija (koja stvara superpoziciju stanja).

Generisanje kvantnih stanja: Generišu se različita kvantna stanja kubita, koje mogu biti '|0>', |'1>', |'+>', ili '|->'. Ovo pokazuje osnovne koncepte kvantne mehanike, kao što su superpozicija i kvantna merenja.

Tkinter za grafički korisnički interfejs: Tkinter se koristi za kreiranje grafičkog korisničkog interfejsa (GUI), što omogućava interakciju sa korisnikom.

Integracija kvantnog računarstva i klasičnog računarstva: Projekat predstavlja primer integracije kvantnih algoritama (koristeći Qiskit) i klasičnog računarstva (SQLite3 baza podataka i Tkinter GUI).



Slika 1. Predlog Stephen Wiesner-a o implementaciji kvantnog novca

Slika 2. Grafički korisniči interfejs (GUI) aplikacije

1. **Emitent:** Klasa koja upravlja kvantnim bankovnim operacijama, uključujući kreiranje kvantnih novčanica i njihovo praćenje u bazi podataka.
    - ***Izdaj novčanicu:*** Generiše se nasumičan četvorocifreni serijski broj za novčanicu, kojem se dodeljuje određeni broj kubita (nasumičan broj od 1 do 8), nakon što su oni prošli kroz simulaciju kvantnog kola, kvantno merenje, primenjivanje Hadamardove i/ili X kapije.
    - ***Pregled novčanica:*** Otvara bazu podataka "novcanice.db" u novom prozoru gde se može videti svaki serijski broj novčanice, kvantno stanje svakog njenog kubita i stanje novčanice koje je "Izdata" ukoliko je onda izdata korisniku ili "U banci" ukoliko se ona nalazi u kvantnoj banci.
    - ***Verifikuj novčanicu:*** Otvara se novi prozor koji traži od emitenta da se unese serijski broj novčanice koja treba da se verifikuje. Kada se unese serijski broj, sistem prolazi kroz bazu podataka "novcanice.db" i traži da li postoji novčanica sa zadatim serijskim brojem.
    - ***Obriši sve novčanice:*** Briše sve novčanice iz obe baze podataka.
2. **Korisnik:** Predstavlja klijenta banke u kvantnom bankarskom sistemu, sa mogućnošću zahtevanja i korišćenja kvantnih novčanica.
    - ***Zahtevaj novčanicu:*** Kreira novu novčanicu, sa novim serijskim brojem, novim brojem kubita i novim kvantnim stanjem svakog kubita. Dodaje je u bazu podataka "novcanice.db" sa statusom "Izdata". Nakon toga, enkodira[1] kvantno stanje svakog kubita i dodaje ih u bazu podataka "novcanik.db". Na ovaj način korisnici znaju serijski broj i broj kubita svoje novčanice, ali ne i stanje tih kubita.
    - ***Pregled novčanika:*** Otvara bazu podataka "novcanik.db" u novom prozoru gde se može videti svaki serijski broj novčanice i enkodirana stanja svakog kubita.
    - ***Obriši ceo novčanik:*** Briše sve novčanice koje se nalaze u bazi podataka "novcanik.db". Zatim prolazi kroz bazu podataka "novcanice.db" i svako stanje novčanice koje je bilo "Izdata" menja u "U banci".
3. **Falsifikator**: Klasa predstavlja osobu koja pokušava da falsifikuje kvantne novčanice, testirajući sigurnost i integritet kvantnog bankarskog sistema.
    - ***Pokušaj falsifikovanja[2]:*** Otvara se novi prozor koji traži od falsifikatora da prosledi serijski broj novčanice. Ukoliko on ne postoji, iskočiće poruka "Novčanica sa unetim serijskim brojem ne postoji!" i pokušaj falsifikovanja će biti obustavljen. U slučaju da postoji novčanica sa tim serijskim brojem, program će pokušati da pogodi broj kubita i kvantno stanje svakog kubita.

[1] Stanje kubita se enkodira tako što se za svako stanje bira nasumičan broj od 0 do 1000

[2] Za *n* kubita, verovatnoća pogađanja kvantnih stanja je $(3/4)^n$

ANALIZA I REZULTATI

Funkcionalnost koda: Kod kombinuje elemente kvantnog računarstva sa tradicionalnim programskim tehnikama. Osnovna funkcionalnost uključuje generisanje kvantnih stanja, upravljanje podacima u SQLite3 bazi podataka, i interakciju sa korisnikom preko Tkinter GUI-ja.

Generisanje i simulacija kvantnih stanja: Korišćenjem Qiskit-a, kod generiše kvantna stanja i simulira ih na kvantnom simulatoru. Ova funkcija je ključna za demonstraciju kvantnih koncepata kao što su superpozicija i kvantna merenja.

Upravljanje bazom podataka: Kod efikasno upravlja bazom podataka, omogućavajući kreiranje, čuvanje i ažuriranje podataka. Ovo je važno za skladištenje i praćenje kvantnih stanja i drugih relevantnih informacija.

Grafički korisnički interfejs: Tkinter se koristi za kreiranje intuitivnog GUI-ja, što omogućava korisnicima da lako interaguju sa sistemom.

Efikasnost: Kod radi efikasno s obzirom na korišćenje laganog SQLite3 sistema za upravljanje bazom podataka i Qiskit-a za simulaciju kvantnih operacija.

Preciznost: Preciznost u kvantnom računarstvu može varirati zbog prirode kvantnih simulacija i merenja. Ovaj projekat koristi simulator, što može ograničiti preciznost u poređenju sa stvarnim kvantnim računarom.

Izazovi: Među izazovima su integracija kvantnih i klasičnih tehnologija, upravljanje složenosti kvantnih operacija, i osiguravanje korisničkog interfejsa koji je istovremeno moćan i jednostavan za korišćenje.

DISKUSIJA

Ovaj projekat predstavlja značajan doprinos u polju kvantnog računarstva, posebno u kontekstu integracije kvantnih tehnologija sa klasičnim programskim okruženjima. Korišćenjem Qiskit biblioteke za simulaciju kvantnih kola i operacija, projekat dodiruje trenutnu granicu istraživanja u kvantnom računarstvu, istražujući mogućnosti i ograničenja kvantnih simulacija.

Integracija sa SQLite3 bazom podataka i Tkinter GUI-om ilustruje kako se kvantne tehnologije mogu primeniti u realnom svetu, nudeći praktična rešenja i otvarajući put ka korisnički orijentisanim aplikacijama. Ovo je posebno relevantno jer industrija teži ka stvaranju kvantnih računara koji su pristupačni i upotrebljivi ne samo u teorijskim istraživanjima, već i u komercijalnim i svakodnevnim aplikacijama.

ZAKLJUČAK

Sve u svemu, ovaj projekat demonstrira kako se teorija kvantnog računarstva može prevesti u praktične aplikacije, što je ključno za dalji razvoj i popularizaciju ove tehnologije. Kroz ovaj rad, ilustruju se potencijali i izazovi u primeni kvantnih tehnologija u praktičnim aplikacijama, naglašavajući kako kvantno računarstvo može postati dostupnije i primenljivije u različitim oblastima. Projekat ne samo da doprinosi tehničkom razvoju u polju kvantnog računarstva, već i otvara nove mogućnosti za buduća istraživanja i inovacije.

BIBLIOGRAFIJA

1. S. Wiesner, "Conjugate coding", 1983.
2. J. Onkenhout, “ Secure payments in the Quantum Era: A technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector”, 2023.