Računarski fakultet / projekat (2023/2024)

Kvantni novac

Vanja Kovinić
vkovinic4220rn@raf.rs

Apstrakt — Kvantni novac predstavlja kvantno-kriptografski protokol dizajniran za generisanje i proveru virtualnih novčanica. Projekat 'Kvantni novac' implementira osnovne principe kvantnog bankarskog sistema s fokusom na kreiranje, izdavanje i verifikaciju kvantnih novčanica. Osim toga, projekat podrazumeva i analizu bezbednosnih aspekata kvantnog novčanog sistema kako bi se osigurao njegov integritet i zaštita od potencijalnih pretnji.

Ključne reči — Kvantni novac, kriptografija, kvantni bankarski sistem.

I. UVOD

Rapidan napredak u digitalnoj sferi finansija pokrenuo je potrebu za razvojem efikasnijih i sigurnijih sistema virtuelnih valuta. U tom kontekstu, klasične metode bezbednosti i transakcionih protokola u budućnosti neće biti u stanju da zadovolje zahteve bankarskog sektora. Stoga, istraživanje kvantnog novca predstavlja odgovor na izazove vezane za bezbednost, verifikaciju i generisanje virtuelnih novčanica primenom kvantnih kriptografskih tehnika. Ovaj rad ima za cilj da istraži osnove kvantnih protokola u bankarstvu kako bi se razvio kvantni novčani sistem koji će efikasno odgovoriti na izazove digitalnog doba, pružajući istovremeno visok stepen sigurnosti i funkcionalnosti.

II. PREGLED LITERATURE

Jedan od problema sa novcem jeste mogućnost pravljenja kopija. Kvantna stanja zadovoljavaju teoremu o nemogućnosti kopiranja, koja kaže da nije moguće napraviti kopiju nepoznatog kvantnog stanja [1].

Upravo to je ono što je inspirisalo Viznera. Godine 1968, Stiven Vizner, postdiplomski student na Kolumbija Univerzitetu, unapređuje ideju o prenosu podataka putem polarizovanih fotona i koncept kvantnog novca [2]. Međutim, njegov revolucionarni rad "Conjugate coding" nailazi na nerazumevanje i odbijanje, te se prvi put objavljuje tek 1983, 15 godina kasnije, iako je bio ispred svog vremena. Ipak, ove ideje, koje su se pojavile gotovo tri decenije pre kvantnih računara, imaju presudan uticaj u razvoju kvantne teorije informacija, kvantnih kriptografskih metoda i kvantnih komunikacionih protokola u narednim godinama.

III. METODOLOGIJA

Rad je implementiran u programskom jeziku python, uz pomoć biblioteke za kvantno računarstvo - qiskit [3]. Sastoji se od 3 glavne radnje koje će biti opisane u nastavku, a to su izdavanje novčanice od strane banke, verifikacija novčanice koju takođe vrši banka i pokušaj falsifikovanja novčanice koju izvodi haker.

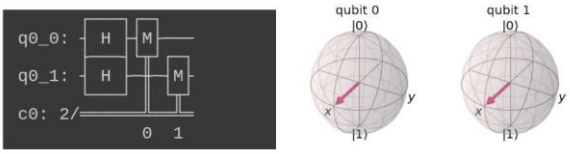
Izdavanje novčanice

Na zahtev korisnika, kvantne novčanice izdaje emitent, npr. centralna banka, u obliku uređenog digitalno/kvantnog para $Q_n = (s, q)$, gde je:

- s jedinstveni četvorocifreni serijski broj u digitalnoj formi,
- q je kubit u kvantnom stanju koje je poznato banci, ali ne i korisnicima novčanice. Kvantno stanje kubita banka bira po slučajnom izboru, iz skupa

$$|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle.$$

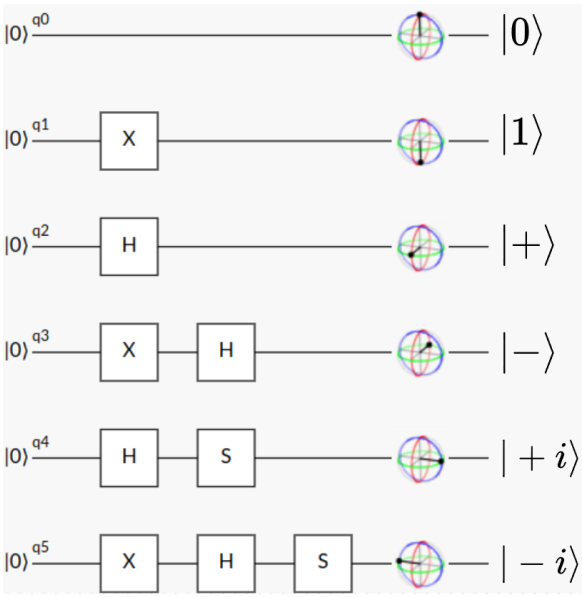
Pošto u klasičnom programiranju stvarno nasumičnost nije moguća, za generisanje nasumičnog stanja koristimo kvantni algoritam (videti sliku 1) koji u zavisnosti od broja koji želimo da generišemo stavlja određeni broj kubita u superpoziciju i nakon njihovog očitavanja nam vraća nasumično generisan broj.



Slika 1 – Primer postavljanja 2 kubita u superpoziciju korišćenjem Hadamarovog kola. Ukoliko želimo da generišemo nasumičan prirodan broj do n , onda nam je za to potrebno $floor(\log_2(n)) + 1$ kubita

U radu je reč o 6 nasumično odabranih stanja, tako da nam je potrebno 3 kubita za generisanje nasumičnog broja koji odabira ta stanja. Pošto koristimo kvantnia svojstva za nasumičnost, verovatnoća da se primenom generatora slučanjih brojeva uniformne raspodele generiše neki od 6 vektora iznosi 1/6.

Kada smo dobili nasumični broj, njega koristimo za postavljanje kubita u jedno od sledećih stanja: $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle$. Algoritam za postavljanje kubita u neko od ovih stanja se može videti na slici 2.

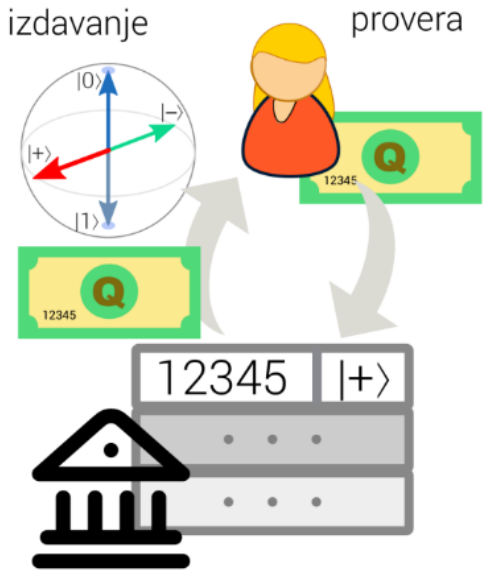


Slika 2 – Algoritam za postavljanje kubita u željeno kvantno stanje

Za svaku izdatu kvantnu novčanicu banka u json formatu čuva listu parova (s, q). Sistem je napravljen da bude fleksibilan što se tiče broja kubita koji se generišu uz s , sa većim brojem kubita raste bezbednost sistema, o čemu će biti reči u narednim odeljcima. Radi testiranja izrađenog rešenja u radu smo koristili novčanice sa jednim kubitom. Takođe, ono što je implementirano da bude fleksibilno jeste broj stanja u kojima svaki pojedinačni kubit može da se nađe.

Verifikacija novčanice

Pre prihvatanja novčanice kao sredstva plaćanja, vrši se njena verifikacija slanjem (s, q) para banci. Banka čitajući vrednosti iz json fajla proverava validnost novčanice i obaveštava korisnika o rezultatu kao što se može videti na slici 3.

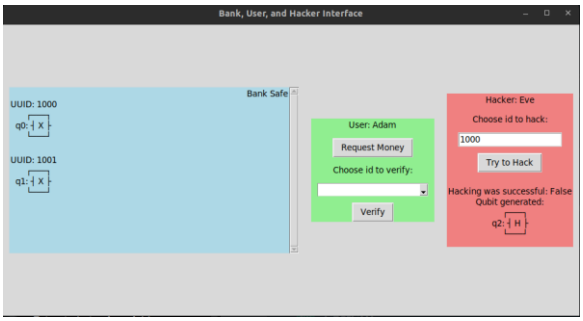


Slika 3 – Verifikacija novčanice

Pokušaj falsifikovanja

Da bi haker falsifikovao novčanicu, mora da ima pristup serijskom broju i stanju kubita. U ovom radu zanemarili smo mogućnost sakrivanja serijskog broja, pa pretpostavljamo da je dostupan hakeru. Pod ovom pretpostavkom, hakeru je i dalje potrebno pronaći stanje kubita. Prema teoremi kvantne mehanike o zabrani kopiranja, savršeno dupliranje nepoznatog kvantnog stanja je nemoguće. To znači da haker ne može napraviti verodostojnu kopiju kvantne novčanice bez poznavanja kvantnog stanja originalne novčanice.

U cilju ilustracije datog eksperimenta, napravljena je i aplikacija sa grafičkim prikazom (slika 4), koja ima ranije navedene akcije (redukovane radi jednostavnosti upotrebe).



Slika 4 - Grafičko okruženje za sprovođenje eksperimenta

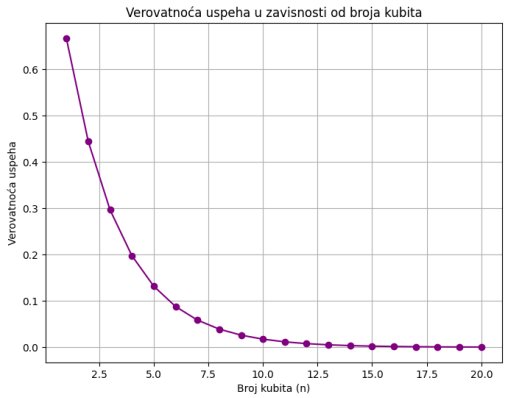
U levom delu nam se nalazi banka gde možemo videti listu svih novčanica koje banka poseduje. U centralnom delu se nalazi korisnik koji može tražiti izdavanje nove novčanice, kao i verifikaciju neke od svojih novčanica. Na desnoj strani se nalazi haker, koji može da za uneti serijski broj, izgeneriše kubit po datom algoritmu (slika 5) i prikaže nam taj kubit, kao i to da li je falsifikovanje uspešno ili ne.

```
# hidden tecnique for generating states that will be used
rand_nums = [(len(self.name)+ random.randint(0, 3))%n_quantum_states
```

Slika 5 – Algoritam koji haker koristi kako bi izgenerisao kubit u određenom stanju, pod pretpostavkom da haker zna sva validna stanja u kojima se kubit može naći

ANALIZA I REZULTATI

Pošto su kvantna stanja nasumična, a mi ih u eksperimentu imamo 6, to znači da je verovatnoća za svako stanje 1/6. Kao što smo već naveli teorema kvantne mehanike ga sprečava da duplira stanje originalne novčanice, bez da zna koja je to novčanica, što znači da su njegove šanse da pogodi novčanicu sa jednim kubitom jednake 2/3 (verovatnoća da haker pogodi osu merenja iznosi 1/3, ali u preostale 2 ose, odnosno 2/3 se ipak može slučajnom redukcijom dobiti tačan rezultat, pa imamo račun $\frac{1}{3} + \frac{2}{3} \cdot \frac{1}{2} = \frac{2}{3}$) i ne mogu biti bolje od toga (po našem trenutnom shvatanju sveta i kvantne fizike). Kako bismo smanjili šansu da haker pogodi kubite na našoj novčanici, prosto ćemo povećati broj kubita, a pošto je svako stanje nezavisno od prethodnog, verovatnoća da haker pogodi stanje je $\left(\frac{2}{3}\right)^n$ gde je n broj novčanica (vidi sliku 6).



Slika 6 - Verovatnoća da će haker uspeti da pogodi kvantno stanje naše novčanice opada sa povećanjem broja kubita

DALJI RAD

Ovaj rad je bio samo demonstracija načela kvantnog računarstva sa primenom u bankarstvu, gde smo videli da je tako nešto izvodljivo. On je i dalje daleko od praktične primene u industriji. Ostaje nam da ovaj sistem dalje unapređujemo, a neke od stavki za sledeću iteraciju su:

- Rad sa više kubita
- Uvođenje novih stanja u kojima se kubit može naći (jer povećavanjem q u izrazu $\left(\frac{1}{q}\right)^n$, gde je q broj stanja, a n broj kubita, takođe smanjujemo šanse hakeru da pogodi stanje)
- Korišćenje protokola za enkripciju serijskog broja
- Korišćenje naprednijih tipova skladištenja podataka

ZAKLJUČAK

Kvantni koncepti pružaju zanimljive mogućnosti u zaštiti novčanica od falsifikovanja. Na osnovu teoreme kvantne mehanike o nemogućnosti savršenog kopiranja kvantnih stanja, jasno je da povećanje broja kubita na novčanici značajno smanjuje šanse hakeru da uspešno replicira stanje svih kubita. Ovo ukazuje na potencijalnu korist kvantne tehnologije u domenu bezbednosti novčanica. Međutim, dok ovi koncepti pokazuju obećavajuće rezultate, njihova primena zahteva dalje istraživanje i razvoj kako bi se garantovala praktična primenljivost i sigurnost u široj upotrebi.

BIBLIOGRAFIJA

[1] https://simons.berkeley.edu/sites/default/files/docs/15601/qmoney-berkeley.pdf
[2] S. Wiesner, "Conjugate coding," ACM SIGACT News, vol. 15, no. 1, pp. 78-88, 1983.
[3] https://www.ibm.com/quantum/qiskit