Kvantni novac

Mihajlo Madžarevič | mmadzarevic5520rn@raf.rs

Apstrakt — Kvantni novac je projekat koji koristi kvantne tehnologije u svrhu enkripcije digitalne valute. Ideja projekta je pružiti jednostavan bankarski sistem i testirati njegovu primenu u zaštiti novca od falsifikovanja.

Ključne reči — Kvantni novac, kvantna novčanica, kubit.

I. UVOD

Osnova kvantnog novca je kvantna novčanica. Ona je sačinjena iz para $Q_n = (s, q)$, gde je

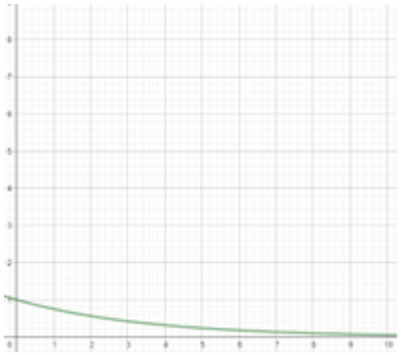
• s jedinstveni maksimalno četvorocifreni serijski broj u klasičnoj, digitalnoj formi,

• 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 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$.

Slika 1. Primer kvantne novčanice (12345, $|+\rangle$).

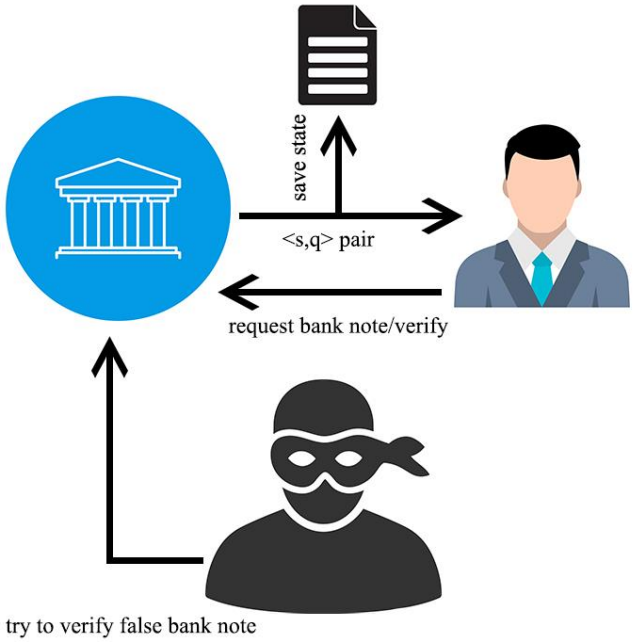
Emitent u svojoj bazi čuva podatke o svakoj izdatoj kvantnoj novčanici kako bi mogao da verifikuje validnost novčanice. Suština ovog projekta je da sagleda mogućnost zaštite od falsifikacije digitalne valute upotrebom kvantne tehnologije.

Potencialna falsifikacija bi bila moguća ukoliko korisnik zna jedinstveni serijski broj s kvantne novčanice, slučajnim pogađanjem kvantnog stanja novčanice. Verovatnoća pogađanja stanja jednog kubita je ekvivalentna (3/4), međutim za n kubita ova vrednost je ekvivalentna $(3/4)^n$. Ovakav pristup je neophodan jer teorema kvantne mehanike navodi da je nemoguće savršeno duplirati kvantno stanje.



Slika 2. Graf verovatnoće falsifikacije(y osa) u odnosu na broj kubita kvantne novčanice(x osa).

Kao što se vidi sa slike 2. mogućnost falsifikacije drastično opada (konvergira ka nuli) sa povećanjem broja kubita. Ovaj projekat treba da korisniku pruži mogućnost testiranja ove tvrdnje upotrebom jednostavnog korisničkog interfejsa.



Slika 3. Dostupne radnje projekta.

II. PREGLED LITERATURE

Godine 1968. Stiven Vizner, student postdiplomskih studija na Kolumbija Univerzitetu, u svom istraživačkom radu iznosi predlog o prenosu podataka korišćenjem polarizovanih fotona i ideju o kvantnom novcu [1]. Daleko ispred svog vremena

Viznerov rad “Conjugate coding”1 nailazi na nerazumevanje i odbijanje. Rad se prvi put objavljuje tek 1983, 15 godina kasnije ali još uvek skoro 3 decenije pre pojave kvantnih računara. U godinama koje slede, zahvaljujući Viznerovim idejama razvija se kvantna teorija informacija, kvantni kriptografski metodi i kvantni komunikacioni protokoli.

Na osnovu Viznerove ideje o kvantnom kodiranju informacija, predložena je implementacija kvantnog novca prikazana na slici 1.

III. Metodologija

Za potrebe pisanja projekta korišćen je Python programski jezik zajedno sa Qiskit bibliotekom koja nam omogućava manipulaciju kvantnih kola, pokretanja simulacija kvantnog računarstava...

Izdavanje novčanice

Izdavanje novčanice podrazumeva izdavanje sledećeg dostupnog jedinstvenog serijskog broja sa nasumično generisanim kvantnim stanjem iz skupa $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ od strane emitenta.

Verifikacija novčanice

Verifikaciju novčanice vrši emitent poređenjem kvantnog stanja prosleđenje novčanice sa kvantnim stanjem ekvivalentne novčanice po jedinstvenom serijskom broju u bazi emitenta.

Pokušaj falsifikovanja

Falsifikacija se vrši pokušajem pogađanja kvantnog stanja novčanice poznatog jedinstvenog serijskog broja.

Čuvanje podataka novčanica

Čuvanje kvantnih novčanica se vršilo u JSON datoteku radi jednostavnosti. Moguće je čuvati novčanice i u bazi podataka.

IV. Analiza, rezultati i diskusija

S obzirom korišćenja samo jednog kubita za čuvanje kvantnog stanja novčanica, falsifikacija nije bila izazov. Kroz par pokušaja je bilo moguće pogoditi kvantno stanje novčanice i samim time je lažno verifikovati. Pri upotrebi pet kubita za čuvanje kvantnog stanja rezultati su bili drastično drugačiji.

Nije bilo uspeha falsifikovanja čak ni sa dvadeset pokušaja. Faktor koji treba uzeti u obzir je da potencijalni falsifikator mora i da zna koliko kubita ima kvantna novčanica koju pokušava da falsifikuje. Ovo bi mogla biti dodatna mera zaštite, korišćenje različe količine kubita za kvantne novčanice kao i uvođenje stanja $\{|+i\rangle,|-i\rangle\}$.

V. Zaključak

Kvantni novac bi bio sigruniji sistem za standardne zaštite današnjih bankarskih sistema. Uprkos lakom uspehu falsifikacije na jednom kubitu primećujemo značajno bolje performanse zaštite novca kvantnog računara na samo pet kubita. Treba se prisetiti da standardni računar koristi bitove koji se mogu naći u jednom od dva stanja u datom trenutku, dok kvantni računari, zahvaljujući svojstvu superpozicije, se mogu nalaziti u više stanja od jednom, što čini prevaru ovakvog sistema značajno težom. Jedini način falsifikacije je nasumično pogađanje stanja kubita zbog već pomenute nemogućnosti o totalnom kopiranju kvantnog stanja. Moguća poboljšanja ovakvog sistema podrazumevaju dodavanje imaginarne ose za potencijalno stanje kubita kao i pridavanja različitog broja kubita kvantnim novčanicama.

Bibliografija

[1] S. Wiesner, "Conjugate coding," ACM SIGACT News, vol. 15, no. 1, pp. 78-88, 1983.

[2] Chat GPT