Moj projekat

Moje ime i e-mail adresa

***Apstrakt***— Kvantni novac je kvantno kriptografski

protokol za kreiranje i verifikaciju virtualne

novčanice. Projekat „Kvantni novac" ima za cilj

implementaciju osnovnih funkcija kvantnog

bankarskog sistema u svrhu kreiranja, izdavanja i

provere kvantnih novčanica kao i analizu

bezbednosti kvantnog novca.

*Ključne reči* — Ključne reči ili fraze koje pomažu u indeksiranju i pretrazi rada.

Quskit:

Otvoreni softverski paket za kvantno programiranje razvijen od strane IBM-a. Omogućava kreiranje, simulaciju i pokretanje kvantnih kolača na kvantnim računarima.

Python:

Visokonivojski programski jezik koji je popularan zbog svoje čitljivosti i fleksibilnosti. Često se koristi u naučnim izračunavanjima, veb razvoju, automatizaciji, analizi podataka i veštačkoj inteligenciji.

Kriptografija:

Nauka i praksa šifrovanja i dešifrovanja informacija. Kriptografija se koristi za zaštitu podataka i komunikacija od neovlašćenog pristupa.

Kvantno racunarstvo:

Oblast računarstva koja koristi kvantne fenomene poput superpozicije i kvantnog preplitanja za obavljanje operacija na podacima. Kvantni računari imaju potencijal da rešavaju određene probleme mnogo brže nego klasični računari.

kutije falisifikatora:

Metaforički izraz koji se može odnositi na metode ili alate koje koristi falsifikator (npr. u kvantnoj kriptografiji) za pokušaj kršenja sigurnosti sistema.

Hadamarova kapija:

Osnovna operacija u kvantnom računarstvu koja menja stanje kubita tako da ga stavlja u superpoziciju. Jedan od ključnih elemenata za kreiranje kvantnih algoritama.

Kubit:

Osnovna jedinica kvantnog računarstva, slična bitu u klasičnom računarstvu. Kubiti mogu biti u stanju 0, 1, ili u superpoziciji oba stanja.

Kvantna pozicija:

Možda ste mislili na "kvantnu superpoziciju", što je osnovni kvantni fenomen gde kubit može biti u više stanja istovremeno.

Stanja kubita:

Opisuje različite moguće konfiguracije kubita. Osim osnovnih stanja '0' i '1', kubiti mogu biti u superpoziciji ovih stanja, kao i u različitim stepenima kvantnog preplitanja.

Baza podataka:

Organizovana kolekcija podataka, često čuvana i pristupana elektronički iz računarskog sistema. Baze podataka omogućavaju skladištenje, pretragu i manipulaciju podacima.

I. UVOD

U savremenom svetu, gde se finansijske transakcije sve više digitalizuju, postoji stalna potreba za poboljšanjem sigurnosti i efikasnosti tih transakcija. Sa razvojem kvantnog računarstva, pojavila se nova perspektiva u kreiranju novčanih sistema - koncept kvantnog novca. Kvantni novac predstavlja revolucionarni pristup u digitalnom bankarstvu, obećavajući povećanu sigurnost zahvaljujući principima kvantne kriptografije. Ovo istraživanje ima za cilj da istraži implementaciju sistema kvantnog novca koristeći Python i Qiskit.

Istraživanje se fokusira na tri ključna aspekta sistema kvantnog novca: emitera, koji je zadužen za izdavanje i kreiranje kvantnih novčanica; korisnika, koji inicira zahteve za dobijanje i verifikaciju kvantnih novčanica; i falisifikatora, koji predstavlja potencijalni pokušaj falsifikovanja kvantnog novca. Kroz analizu ovih aspekata, cilj je da se razvije dublje razumevanje kako kvantni novac funkcioniše, kao i da se identifikuju potencijalni izazovi i rizici u njegovoj primeni.

II. Pregled literature

U literaturi o kvantnom novcu, postoje različiti pristupi i ideje kako konstruisati javno proverljive kvantne novčane sisteme, kao i metode za njihovo obaranje. Jedno od značajnih istraživanja u ovoj oblasti i rad na koji sam prvo naišao dok sam radio istraživanje je rad koji predstavlja novi javno proverljiv kvantni novčani sistem. Ovaj sistem je značajan jer ispunjava tri ključna kriterijuma: sigurnost zasnovana na verovatnim pretpostavkama, dokaz da je šema novca sigurna protiv crne kutije falisifikatora i jednostavan proces verifikacije koji prihvata sve važeće novčanice​​.

Izvor: <https://ar5iv.labs.arxiv.org/html/1203.4740>

Praktična nekopirabilnost kvantnog novca: Jedno istraživanje fokusira se na praktičnu implementaciju nekopirabilnog kvantnog novca, ističući izazove u stvaranju i proveri kvantnih novčanica u realnim uslovima. Ovo istraživanje pokazuje kako sistemski nedostaci mogu uticati na tačnost verifikacije kvantnog novca.

Izvor: <https://www.nature.com/articles/s41534-018-0058-2>

Razvoj novih kvantnih novčanih šema: Ovo je uvod u nove pristupe dizajniranja kvantnog novca, uzimajući u obzir apstraktne osobine neophodne za dokazivanje sigurnosti. Autori predlažu nekoliko novih koncepta i tehnika koje bi mogle biti korisne za dizajn i analizu kvantnih novčanih sistema.

Izvor: <https://ar5iv.labs.arxiv.org/html/2211.11994>

Ova istraživanja zajedno pružaju duboko razumevanje kako kvantni novac funkcioniše, koje su njegove prednosti i izazovi, kao i budući pravci razvoja u ovoj dinamičnoj oblasti.

III. Metodologija

Metodologija ovog istraživanja obuhvata korišćenje interneta i pretraživanje Google-a za pronalaženje radova o kvantnom novcu. Prikupljanje podataka je izvedeno čitanjem izvora koji se odnose na izdavanje, falsifikovanje kvantnih novčanica, kao i na princip rada kvantnih sistema i relevantnih fizikalnih zakona. Projektna struktura je bila pažljivo organizovana, sa posebnim fokusom na razvijanje svake komponente modela zasebno, njihovo testiranje i korišćenje u programskom jeziku Python uz Qiskit okruženje. Korišćeni algoritmi uključuju kreiranje kubita u kvantnim pozicijama korišćenjem Hadamardove kapije.

Klasa Emitent se koristi za simulaciju emisije kvantnih novčanica. Svaka funkcija ima svoju specifičnu ulogu:

* \_\_init\_\_: Inicijalizuje bazu podataka za čuvanje informacija o kvantnim novčanicama.
* generisi\_serijski\_broj: Generiše jedinstveni četvorocifreni serijski broj za svaku novčanicu.
* generisi\_kvantno\_stanje: Kreira kvantno stanje kubita koristeći Hadamardovu kapiju i merenje, i na osnovu toga određuje kvantno stanje novčanice.
* izdaj\_novcanicu: Spaja generisanje kvantnog stanja i serijskog broja da bi izdala kvantnu novčanicu i čuva informacije u bazi podataka.
* ispisi\_sve\_novcanice: Ispisuje sve novčanice koje su pohranjene u bazi podataka.
* verifikuj\_novcanicu: Proverava da li postoji novčanica sa određenim serijskim brojem u bazi podataka.
* \_\_del\_\_: Zatvara konekciju sa bazom podataka kada se klasa više ne koristi.

|  |  |  |
| --- | --- | --- |
| Stanje | Očekivanje | Verovatnoća |
| |0> | 25% | 25% |
| |1> | 25% | 25% |

Klasa Korisnik interaguje sa klasom Emitent za upravljanje kvantnim novčanicama:

* \_\_init\_\_: Inicijalizuje objekat klase Korisnik sa referencom na objekat Emitent.
* zahtevaj\_novcanicu: Korisnik šalje zahtev za izdavanje kvantne novčanice određenog broja kubita. Ova funkcija vraća serijski broj izdate novčanice.
* verifikuj\_novcanicu: Korisnik šalje zahtev za verifikaciju novčanice koristeći njen serijski broj. Funkcija vraća informaciju o tome da li je novčanica pronađena u bazi podataka Emitent klase.

Klasa Falsifikator u Python-u služi za simulaciju pokušaja falsifikovanja kvantnih novčanica:

* \_\_init\_\_: Inicijalizuje bazu podataka za čuvanje informacija o kvantnim novčanicama.
* generisi\_nasumicne\_kvantne\_brojeve: Generiše niz nasumičnih kvantnih stanja iz preddefinisane liste mogućih stanja, na osnovu zadate dužine niza.
* pokusaj\_falsifikovanja: Pokušava da pronađe kvantno stanje koje odgovara generisanom nasumičnom nizu u bazi podataka, simulirajući na taj način pokušaj falsifikovanja kvantne novčanice.

Analiza i rezultati

Na osnovu analize prošlih linkova došao sam do rezultata koje predstavljam u obliku teza koje imaju uticaj na arithekturu projekta i samo shvatanje kvantnog novca.

1. Sigurnost: Osnovana na verovatnim pretpostavkama, što znači da su pretpostavke o sigurnosti zasnovane na verovatnoćama, a ne na apsolutnim garancijama.
2. Otpornost na Falisifikate: Posebno se naglašava otpornost na crne kutije falisifikatora, što ukazuje na sposobnost sistema da se odupre napadima čak i kad napadač poseduje napredne tehnološke sposobnosti.
3. Jednostavan Proces Verifikacije: Sistem treba da omogućava lako prepoznavanje i prihvatanje važećih novčanica, što je ključno za praktičnu upotrebu.
4. Izrada i Provera Kvantnih Novčanica: Identifikuje se niz izazova u procesu proizvodnje. Odabir broja kubita, arhitektura kvantnog kola.
5. Sistemski Nedostaci: Pokazuje se kako ovi nedostaci utiču na tačnost i efikasnost verifikacije, što je vitalno za pouzdanost kvantnog novčanog sistema.
6. Novi Koncepti i Tehnike: Istraživanje uvodi inovativne ideje za dizajniranje kvantnog novca.
7. Dokazivanje Sigurnosti: Poseban naglasak na apstraktnim karakteristikama neophodnim za dokazivanje sigurnosti, što može unaprediti celokupnu pouzdanost sistema.
8. Eksperimentalna Demonstracija: Istraživanje obuhvata praktično testiranje pripreme i verifikacije kvantnih novčanica.

Diskusija

Interpretiraju se rezultati, analiziraju implikacije istraživanja i razmatraju eventualna ograničenja. Takođe se povezuje sažet sa prethodnim istraživanjima i teorijama.

Primena prošlih hipoteza u mom python kodu se može videti u procesima zaštite. Nparimer metoda za falsifikovanje generisanje nasumičnog stringa vrednosti kubita koji se može koristiti ako je poznat broj kubita novčanici da se dobije iz baze tražena novčanica. Postupak je povezan sa hipotezama 1 i 2.

Proces provere kvantnih novčanica (3), tj. verifikacije se radi na osnovu identifikacionog broja koji se prosledjuje klasi Emiter koja proverava da li takav kubit postoji.

Za izradu broja kubita kvantne novčanice(4) se koristio jedan kubit za testiranje a u prakticne svrihe 8 kubita. Celo kvantno kolo se sastoje od jedne hadamarove kapije koja služi za prebacivanje kubita u kvantnu poziciju, posle čega sledi merenje kubita koje tera kubit da postane jedno stanje.

Pored takve implementacije postoje dosta nedostataka u načinima pristupa bazi i mogućnostima pristupu podataka. Postojeći sistemi mogu imati nedostatke koji utiču na preciznost i efikasnost verifikacije kvantnih novčanica (5). Kvantni novac kao svaka nova ideja zahtevaju temeljno testiranje i evaluaciju pre nego što postanu deo standardnih praksi.

Demonstracija Interfejsta:



Zaključak

Značaj ovog istraživanja leži u njegovom doprinosu razvoju bezbednih i efikasnih digitalnih finansijskih sistema u eri kvantnog računarstva. S obzirom na rastuću potrebu za sigurnim digitalnim transakcijama, rezultati ovog istraživanja mogu ponuditi vredne uvide u implementaciju kvantnog novca kao robustnog rešenja za buduće finansijske operacije.