Kvantni denar

Luka Skeledžija

Mentor: prof. dr. Rok Žitko

Seminar, 3. letnik

Oddelek za fiziko, FMF, UL, 2022/2023

Povzetek
V kvantni mehaniki srečamo nekatere fizikalne pojave, ki jih iz klasične fizike nismo vajeni. Čeprav čudna, nam takšna nova fizika omogoča razvoj tehnologij, ki v okviru klasične fizike ne bi bile mogoče. Takšen primer je izrek o prepovedi kloniranja, ki predstavlja teoretično osnovo za veliko družino kvantnih kriptografskih protokolov. V okviru tega seminarja preletimo osnovne koncepte kvantne informacijske teorije, izpeljemo in dokažemo izrek o prepovedi kloniranja ter z njegovo pomočjo teoretično varno rešimo problem ponarejanja denarja.

Kazalo

1 Uvod

Zakaj imajo kovanci in papirnati bankovci v našem žepu kakršno koli vrednost? Kratek odgovor bi bil, da jim je vrednost in uporabo odredila zaupanja vredna institucija (npr. centralna banka po naročilu države) *in hkrati* obstaja le omejena količina tako izdanih bankovcev in kovancev. Zaradi drugega pogoja je fizičen denar opremljen z različnimi varnostnimi elementi, ki močno otežujejo njihovo ponarejanje in varujejo vrednost valute. Ponarejanje v praksi je sicer *težko*, vendar nas vedno zanimajo še boljše (in morda teoretično brezhibne) rešitve, ki se ne zanašanjo na otip papirja, hologramski, vodni, UV, infrardeči ter miniaturni tisk [Ban18]. V uporabi so tudi še bolj zanimive metode npr. digitalni filtri v orodjih kot so Adobe Photoshop in nekaterih tiskalnikih, ki onemogočajo procesiranje slik bankovcev [Sof].

1.1 Aktualne rešitve

Zanimivo je, da nas pri plačevanju s kartico težave ponarejanja denarja očitno ne pestijo, saj se vse dogaja znotraj bančnega sistema, kjer avtentičnost denarja pred vstopom vanj preverijo. Vendar pa morajo biti tudi bančne kartice na nek način zaščitene pred neavtoriziranim kopiranjem. Vsaka kartica namreč vsebuje polprevodniški mikročip in sistem simetrične kriptografije - torej uporabljajo isti ključ za šifriranje in dešifriranje [Cs1]. Na čipu je shranjena kopija šifrirnega ključa, ki ob vsaki transakciji zakodira unikatno sporočilo (npr. dovolj dolg naključni niz ali današnjo časovno oznako, angl. timestamp), ki ga nato pošlje na banko, kjer hranijo kopijo šifrirnega ključa. Banka sporočilo dešifrira in s tem potrdi avtentičnost transakcije. Bistvo te sheme je, da šifrirni ključ polprevodniškega čipa nikoli ne zapusti, ampak s t.i. reševanjem unikatnih izzivov (šifriranjem nizov) banki dokazuje, da šifrirni ključ pozna [Cs1]. Ker je ključ shranjen znotraj izjemno majhnega kosa polprevodnika, je branje le-tega izjemno zahtevno [Chr+06] in zato za povprečnega ponarejevalca pretežko.

V teoriji bi lahko vsak bankovec opremili s takšnim polprevodniškim elementom in tako potrjevali avtentičnost. Vendar je to po eni strani potratno, po drugi pa nas kvantna mehanika lahko pripelje še bližje tudi teoretično varnemu sistemu.

1.2 Kvantni denar

Leta 1983 je Stephen Wiesner objavil članek v katerem predlaga shemo t.i. "Kvantnega denarja"[Wie83]. V splošnem je Wiesnerjeva shema kvantni kriptografski protokol (zaenkrat še brez praktične implementacije), ki opisuje kako ustvariti in verificirati bankovce odporne na ponarejanje [Qua]. Poleg unikatne serijske številke bi vsak bankovec opremili še z nizom izoliranih dvonivojskih kvantnih sistemov. Tedaj po Izreku o prepovedi kloniranja ni mogoče ustvariti identične in neodvisne kopije poljubnega neznanega kvantnega stanja, saj to krši osnovna načela kvantne mehanike (konkretno linearnost) [Noc]. Za vsak sistem v nizu dvonivojskih kvantnih sistemov obstaja verjetnost 3/4 [MVW12], da bo kopija neznanega stanja popolna [Qua]. Če je število kvantnih sistemov v nizu enako N, je tedaj verjetnost za nastanek popolne kopije niza $(3/4)^N$. Upoštevamo, da je na niz na bankovcu dolg in tako za velike N kaj hitro ugotovimo, da je verjetnost za slučajen nastanek popolne kopije celotnega niza eksponentno majhna.

2 Kvantna informacijska teorija

Ker se Wiesnerjeva shema naslanja na poglavja iz kvantne informacijske teorije (npr. Izrek o prepovedi kloniranja), moramo za globlje razumevanje na tej ravni v nadaljevanju razložiti še nekaj idej s področja kvantne mehanike.

2.1 Lastnosti kvantnih sistemov

V klasični fiziki lastnosti sistema obstajajo neodvisno od meritve in so del realnosti. Meritev te lastnosti le razkrije. V kvantni mehaniki pa vektor stanja določa le verjetnosti, da bomo pri meritvi dobili določen rezultat. Dva delca, ki sta na začetku opisana z enakim vektorjem stanja, lahko ob isti meritvi vrneta dva različna rezultata. Kvantno mehaniko lahko razumemo kot matematično ogrodje za razvoj fizikalnih teorij, ki smo ga izoblikovali na podlagi več deset let fizikalnih eksperimentov in ugibanja, kako se obnaša narava na skali atomov in podatomskih delcev. Osnovni postulati kvantne mehanike tako predstavljajo povezavo med fizičnim svetom in matematičnim formalizmom.

Postulat 1. *Kvantno stanje je element Hilbertovega prostora.*

Postulat 2. *V kvantni mehaniki opazljivkam ustrezajo hermitski operatorji.*

Postulat 3. *(Bornovo pravilo) Pri meritvi opazljivke A v stanju $|\psi\rangle$ bomo dobili rezultat λ_j z verjetnostjo $p_j = |\langle j|\psi\rangle|^2$.*

Postulat 4. *(Kolaps valovne funkcije) Če pri meritvi opazljivke $A = \sum_i \lambda_i |i\rangle \langle i|$ izmerimo vrednost λ_i, potem je takoj po meritvi sistem v lastnem stanju $|i\rangle$.*

Postulat 5. *Časovno spreminjanje kvantnega stanja opišemo z unitarnim operatorjem.*

S tem smo postavili osnove matematičnega formalizma, s katerim bomo delali v nadaljevanju. [Ž17]

2.2 Kubit

Bit je fundamentalni koncept klasičnega računalništva, klasične informacijske teorije in hkrati tudi najmanjša enota informacije. V kvantni mehaniki definiramo analogni koncept, kjer obravnavamo t.i. *kubite*. Če v klasični informacijski teoriji pripišemo bitu eno izmed izmed dveh stanj 0 ali 1, v kvantni mehaniki definiramo ortogonalni stanji $|0\rangle$ in $|1\rangle$ s to razliko, da so v kvantni mehaniki dovoljene tudi linearne kombinacije obeh stanj. Povedano z drugimi besedami, sta stanji $|0\rangle$ in $|1\rangle$ v superpoziciji, kar ponazorimo z enačbo

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \tag{1}$$

kjer velja $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$ in $|\psi\rangle$ normirana valovna funkcija. Zapis lahko dodatno poenostavimo, da velja $|0\rangle = [1, 0]^T$ in $|1\rangle = [0, 1]^T$, s čimer zapis kubita prevedemo na $|\psi\rangle = [\alpha, \beta]^T$. Kubit zavzame stanje $|0\rangle$ ali $|1\rangle$ šele ob meritvi, in sicer z verjetnostjo $|\alpha|^2$ oz. $|\beta|^2$. Stanje, ko je $|\alpha|^2 = 0.5$ in $|\beta|^2 = 0.5$ včasih označimo tudi z $|+\rangle$ za pozitivno predznačen β in $|-\rangle$ za negativno predznačen β. [NC12]

Ker je valovna funkcija normirana in velja $|\alpha|^2 + |\beta|^2 = 1$, lahko $|\psi\rangle$ brez izgube splošnosti zapišemo tudi kot:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle, \tag{2}$$

kjer θ in φ definirata (poljubno) točko na Blochovi sferi. Uporabnost takšne reprezentacije dvonivojskega sistema se pokaže pri izvajanju operacij na posameznem kubitu (npr. kvantna logična vrata). Vsaka taka operacija namreč pomeni rotacijo vektorja na sferi, ki jo lahko zapišemo z unitarno matriko. Vendar pa je takšna predstava kubita omejena, saj ne poznamo nobene preproste generalizacije Blochove sfere za več kubitov. [NC12]

Če primerjamo kubit s klasičnim bitom, ki lahko zaseda le dve diskretni stanji, ta na videz vsebuje manj informacije (npr. lahko bi izbrali tak θ, da decimalke shranijo poljubno količino informacije). Vendar pa je potrebno upoštevati naravo kubita, ko na njem izvedemo meritev. Meritev privede do kolapsa superpozicije, iz kubita dobimo tako natanko 1 bit informacije, in sicer stanje $|0\rangle$ ali $|1\rangle$. [NC12]

2.3 Več kubitov in kvantna prepletenost

Stanja večih kubitov zapišemo kot tenzorski produkt. Za dva kubita: $|\psi\rangle_a = c_{a0}|0\rangle_a + c_{a1}|1\rangle_a$ in $|\psi\rangle_b = c_{b0}|0\rangle_b + c_{b1}|1\rangle_b$, tedaj velja

$$\begin{aligned}
|\zeta\rangle &= |\psi\rangle_a \otimes |\psi\rangle_b \\
&= (c_{a0}|0\rangle_a + c_{a1}|1\rangle_a) \otimes (c_{b0}|0\rangle_b + c_{b1}|1\rangle_b) \\
&= c_{00}|0\rangle_a \otimes |0\rangle_b + c_{01}|0\rangle_a \otimes |1\rangle_b + c_{10}|1\rangle_a \otimes |0\rangle_b + c_{11}|1\rangle_a \otimes |1\rangle_b \\
&= c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle,
\end{aligned} \tag{3}$$

kjer smo na primer stanje $|0\rangle_a \otimes |1\rangle_b$ zapisali kot $|01\rangle$. Enako kot smo to storili z enim kubitom, lahko stanja dveh kubitov predstavimo z vektorjem: $|00\rangle = [1,0,0,0]^T$, $|01\rangle = [0,1,0,0]^T$, $|10\rangle = [0,0,1,0]^T$ in $|11\rangle = [0,0,0,1]^T$. Poljubno stanje dveh kubitov zapišemo kot $|\zeta\rangle = [c_{00}, c_{01}, c_{10}, c_{11}]^T$. Notacijo lahko posplošimo na poljubno število bitov. [Pom22]

Poljubnega stanja dveh ali več kubitov v splošnem *ne* moremo zapisati v produktni bazi kot $|\Psi\rangle_{ab} = |\psi\rangle_a|\phi\rangle_b$. Torej za dane koeficiente c_{00}, c_{01}, c_{10} in c_{11} ne moremo določiti koeficientov c_{a0}, c_{a1}, c_{b0} in c_{b1}. Takšnemu stanju pravimo, da je *prepleteno*. [Pom22]

Sistem z n kubiti ima 2^n možnih stanj, torej je stanje le-tega superpozicija 2^n lastnih stanj oziroma ima vektor stanja 2^n komponent. Ko izmerimo stanje sistema, kolapsiramo superpozicijo in izmerimo le eno od 2^n možnih stanj s točno določeno verjetnostjo. [Pom22]

2.4 Polarizacija svetlobe

Primer preprostega dvonivojskega kvantnega sistema je polarizacija svetlobe oz. fotonov. Za opis polarizacije svetlobe si lahko v optiki pomagamo z Jonesovim vektorjem in Jonesovim računom [Jon], kjer kompleksno amplitudo $\vec{E}$ elektromagnetnega valovanja opišemo kot

$$\vec{E}(t) = \begin{pmatrix} E_x(t) \\ E_y(t) \\ 0 \end{pmatrix} = \begin{pmatrix} E_{0x}e^{i(kz-\omega t+\phi_x)} \\ E_{0y}e^{i(kz-\omega t+\phi_y)} \\ 0 \end{pmatrix} = \begin{pmatrix} E_{0x}e^{i\phi_x} \\ E_{0y}e^{i\phi_y} \\ 0 \end{pmatrix} e^{i(kz-\omega t)}. \tag{4}$$

Jonesov vektor je tedaj definiran v ravnini xy kot $[E_{0x}e^{i\phi_x}, E_{0y}e^{i\phi_y}]^T$. Vektorju pripadajo tipične polarizacije v Tabeli 1.

Polarizacija	**Jonesov vektor**	**Tipična ket notacija**
Horizontalno	$(1,0)^T$	$\|H\rangle$
Vertikalno	$(0,1)^T$	$\|V\rangle$
Desno	$\frac{1}{\sqrt{2}}(1,-i)^T$	$\|R\rangle = \frac{1}{\sqrt{2}}\big(\|H\rangle - i\|V\rangle\big)$
Levo	$\frac{1}{\sqrt{2}}(1,+i)^T$	$\|L\rangle = \frac{1}{\sqrt{2}}\big(\|H\rangle + i\|V\rangle\big)$

Tabela 1: Tipi polarizacij in pripadajoči Jonesov vektor. Dodatno označena tudi tipična ket notacija. [Jon]

2.5 Razločljivost neortognalnih stanj

Eno izmed poglavitnih vprašanj v kvantni mehaniki (in ozadje mnogih kvantnih tehnologij) je problem razločljivosti neortogonalnih stanj. Pretvarjajmo se za trenutek, da lahko razločimo med poljubnimi kvantnimi stanji. Imamo znan kriptografski par Alice in Bob, ki si delita par prepletenih kubitov (npr. fotonov) v stanju $(|00\rangle + |11\rangle)/\sqrt{2}$. Če Alice izvede meritev v računski bazi (ena izmed možnih baz), skupna valovna funkcija (saj sta delca prepletena) kolapsira v stanje $|00\rangle$ z verjetnostjo 1/2 ali stanje $|11\rangle$ z verjetnostjo 1/2. Zaradi kolapsa valovne funkcije bo tedaj tudi Bob (ki je daleč stran od Alice) izmeril enako vrednost kot ona, in sicer 0 z verjetnostjo 1/2 ali 1 z verjetnostjo 1/2. Lahko pa bi Alice kubit izmerila tudi v bazi $|+\rangle$ in $|-\rangle$. Z malo računanja ugotovimo (mešani členi se namreč odštejejo), da lahko začetno prepleteno stanje v novi bazi zapišemo kot $(|++\rangle + |--\rangle)/\sqrt{2}$. Po meritvi je Bobov sistem v stanju $|+\rangle$ z verjetnostjo 1/2 ali $|-\rangle$ z verjetnostjo 1/2. Sledi, da če bi Bob imel napravo, ki razlikuje med stanji valovne funkcije $|0\rangle$, $|1\rangle$, $|+\rangle$ ali $|-\rangle$, bi lahko ugotovil, v kateri izmed dveh baz je merila Alice. Še več, to bi lahko ugotovil natanko ob izvedbi meritvi, tudi če je Alice daleč stran. To bi pomenilo, da lahko informacija o izbiri baze potuje s hitrostjo večjo od hitrosti svetlobe. Iz teorije relativnosti vemo, da to ruši kavzalnost in je v nasprotju z do sedaj znanimi fizikalnimi zakoni. Iz te ugotovitve sledi, da v kvantni mehaniki ni mogoče razločiti med neortogonalnimi stanji. [NC12]

3 Izrek o prepovedi kloniranja

Zdaj že vemo, da informacija zaradi teorije relativnosti (in ohranitve kavzalnosti) ne more potovati hitreje kot svetloba. Kljub temu je leta 1982 Nick Herbert v reviji Foundations of Physics objavil članek z naslovom *FLASH—A superluminal communicator based upon a new kind of quantum measurement*, kjer predlaga shemo naprave, ki naj bi omogočala komunikacijo hitrejšo od hitrosti svetlobe [Her82]. Da ima članek napako, so slutili tako recenzenti kot najverjetneje tudi Herbert sam. Vendar so objavo članka vseeno omogočili, saj nihče od njih napake ni znal poiskati, njen izvor pa bi najverjetneje pripeljal do odkritja nove fizike [Per03]. Na srečo so kmalu po izidu članka napako našli [WZ82] in, kot napovedano, ob enem odkrili tudi izrek o prepovedi kloniranja za kvantne sisteme.

3.1 Izpeljava

Izrek o prepovedi kloniranja zgodovinsko izpeljemo v dveh korakih.

3.1.1 Prepoved superluminalne komunikacije

V prvem koraku rigorozno pokažemo, da je obstoj superluminalne komunikacije nemogoč. Če želimo biti povsem natančni, posebna teorija relativnosti superluminalne komunikacije sama po sebi ne prepoveduje. Einsteinova teorija predpostavi le, da je hitrost svetlobe v vakuum vedno enaka c in to neodvisno od gibanja telesa, ki jo odda.

Kateri delci bi torej lahko informacijo sploh prenašali hitreje kot svetloba? Pri masnih delcih ugotovimo, da smo omejeni s količino energije. Velja namreč

$$p = \frac{mv}{\sqrt{1 - \frac{v^2}{c^2}}}, \tag{5}$$

kjer je p gibalna količina delca. Ko se hitrost v bliža c, gibalna količina p limitira proti neskončnosti. Ker smo s količino energije omejeni, masnih delcev ne moremo pospešiti do svetlobne hitrosti in naprej. Na voljo nam ostanejo fotoni in drugi brezmasni delci. Zato se na tej točki raje bolj splošno vprašamo, kaj bi se zgodilo s kavzalnostjo, če bi lahko informacije prenašali s hitrostjo večjo od hitrosti svetlobe. [Mara]

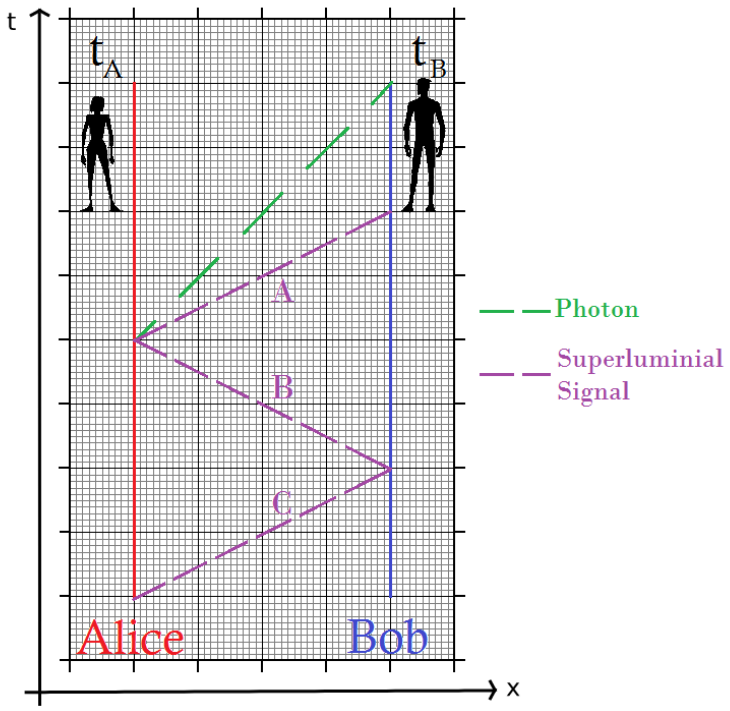
Na diagramu Minkowskega na Sliki 1 zopet nastopa znan kriptografski par Alice in Bob. Tokrat sta Alice in Bob vsak na svojem planetu, kjer je planet A od planeta B oddaljen za razdaljo d. Alice in Bob si izmenjujeta signale. Z zeleno črtkano črto je na Sliki 1 prikazan svetlobni signal. Če je superluminalna komunikacija mogoča, lahko Alice s hitrejšim signalom A (vijolična črta) Boba opozori, da bo prejel svetlobni signal. Še več, ker je hitrost signala sedaj hitrejša od hitrosti svetlobe, lahko Alice pošlje signal B, ki ga Bob prejme še preden ga Alice sploh pošlje! Bob se na signal B odzove s signalom C, ki ga Alice prejme še pred pošiljanjem signala B. Tako smo s superluminalno komunikacijo iznašli komuniciranje v preteklost. Alice lahko npr. opozori sebe na nekaj, kar bo storila v prihodnosti, kar nas pripelje v paradokse in poruši kavzalnost (vzročnost dogodkov). [Mara]

Da superluminalna komunikacija zares omogoča komunikacijo v preteklost, lahko potrdimo tudi matematično. Z $A - B$ označimo razdaljo med planetoma A in B. Če signal potuje s hitrostjo a, je tedaj čas potovanja signala, merjen v inercialnem sistemu ko sta točki A in B pri miru, enak

$$\Delta t = t_1 - t_0 = \frac{B - A}{a}. \tag{6}$$

Velja, da je dogodek A (oddaja signala) vzrok dogodka B (prejem signala). Za opazovalca v nekem drugem inercialnem sistemu, ki se giblje s hitrostjo v, lahko čas prejema signala v B izračunamo s pomočjo Lorentzove transformacije, kjer je c hitrost svetlobe. Tedaj velja

$$\begin{aligned} \Delta t' = t'_1 - t'_0 &= \frac{t_1 - vB/c^2}{\sqrt{1 - v^2/c^2}} - \frac{t_0 - vA/c^2}{\sqrt{1 - v^2/c^2}} \\ &= \frac{1 - av/c^2}{\sqrt{1 - v^2/c^2}} \Delta t. \end{aligned} \tag{7}$$



Slika 1: Diagram Minkowskega. Diagram prikazuje komunikacijo med Alice in Bobom. Čas po vertikalni osi, razdalja po horizontalni. [Marb]

Precej preprosto lahko pokažemo, da lahko za vrednosti $a > c$ izberemo tak v, da ima koeficient pred Δt negativen predznak. To se zgodi že, če uporabimo $a = c^2/(1\,\frac{\mathrm{m}}{\mathrm{s}})$ in $v = 2\,\frac{\mathrm{m}}{\mathrm{s}}$. Z drugimi besedami - v tem inercialnem sistemu se je dogodek B zgodil še pred dogodkom A. Einstein je leta 1907 zaključil, da, čeprav v tem izrazu ne vidi nobene logične kontradikcije, je takšen rezultat kontradiktoren vsem našim izkušnjam iz realnega življenja. To pa v dovoljšnji meri dokazuje, da je primer, ko je $a > c$, nemogoč. [Tac]

3.1.2 Komunikator FLASH

Nick Herbert je leta 1982 predlagal shemo superluminalnega komunikatorja FLASH (Slika 2), katerega osnova je prepleten par fotonov (EPR par). Za komunikacijo uporablja dejstvo, da ima meritev enega izmed prepletenih fotonov takojšnji učinek na drugega.

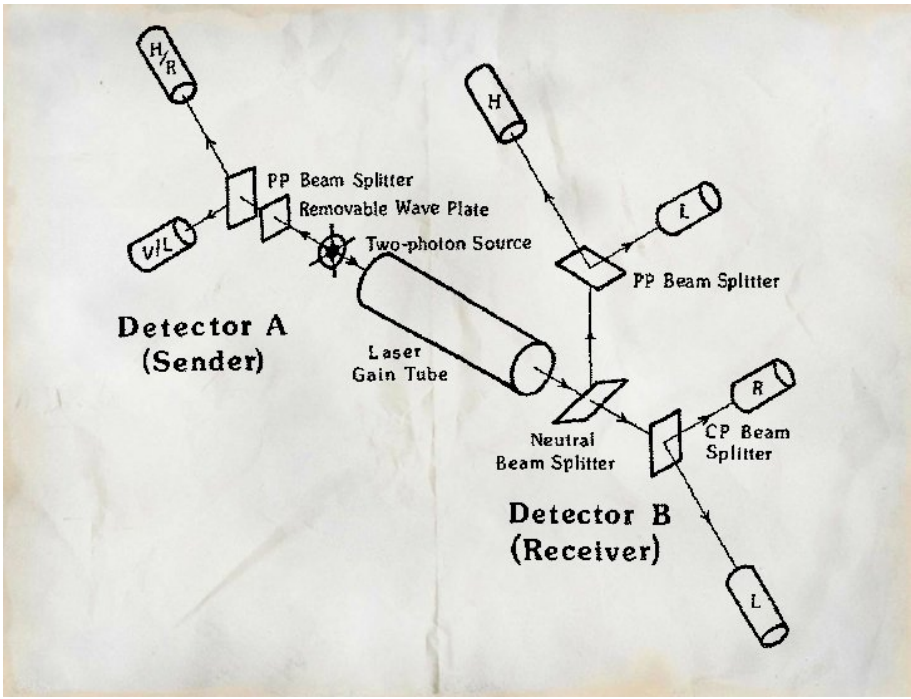
Par prepletenih fotonov ustvarimo v dvofotonskem izviru in jih pošljemo v smeri dveh opazovalcev, npr. Alice in Bob. Stanje dveh fotnov je podano v rotacijsko invariantnem stanju

$$\frac{|HH\rangle + |VV\rangle}{\sqrt{2}}, \tag{8}$$

kjer sta H in V horizontalna in vertikalna polarizacija. Enako prepleteno stanje bi lahko zapisali tudi v bazi krožne polarizacije in sicer kot

$$\frac{|RR\rangle + |LL\rangle}{\sqrt{2}}, \tag{9}$$

kjer sta R in L desna in leva polarizacija. Ko Alice prejme svoj foton, mu lahko izmeri eno izmed dveh polarizacij, tj. linearno ali krožno. Tedaj bo tudi Bobov foton kolapsiral



Slika 2: Originalna shema komunikatorja FLASH. [Her82]

v linearno ali krožno polarizacijo. Bob svoj foton pred meritvijo pošlje v lasersko pomnoževalko ("Laser Gain Tube"), ki iz n fotonov naredi $4n$ enako polariziranih fotonov. Bob razdeli fotonski curek na 4 dele po n fotonov in izmeri polarizacije H, V, R in L. Rezultati meritev so tedaj kot v Tabeli 2. Vse kar mora Bob sedaj storiti, je pogledati kateri izmed njegovih detektorjev je detektiral 0 fotonov. S tem izve, v kateri bazi je merila Alice. S tem v trenutku meritve (torej hipno) prejme 1 bit informacije. Po drugi strani pa smo že prej pokazali, da takšna hipna komunikacija ni možna. Kje se torej skriva napaka te sheme? [Mara]

Ob objavi Herbertovega članka je bilo dobro znano, da imajo izhodni fotoni iz laserske fotopomnoževalke enako polarizacijo kot vhodni. Vendar pa je Herbert spregledal, da lahko stanje npr. $|H\rangle$ zapišemo kot superpozicijo stanj $|R\rangle$ in $|L\rangle$:

$$|H\rangle = \frac{|R\rangle + |L\rangle}{\sqrt{2}}. \tag{10}$$

Laserska fotopomnoževalka v tem primeru dejansko pomnoži stanja $|R\rangle$ in $|L\rangle$, vsakega z verjetnostjo $1/2$. Torej na izhodu dobimo $2n$ fotonov v stanju $|R\rangle$ in $2n$ fotonov v stanju $|L\rangle$. Rezultat Bobovih meritev bi bil tedaj vedno (in neodvisno od originalne polarizacije, ki jo izmeri Alice) enak $n/2$ fotonov za vse 4 polarizacije H, V, L in R. [Mara]

Napaka sheme torej leži v predpostavki, da lahko kloniramo naključno kvantno stanje.

3.2 Formulacija in dokaz

Iz prejšnjih ugotovitev lahko sedaj formuliramo izrek in ga tudi formalno dokažemo [NC12].

Izrek o prepovedi kloniranja. *V kvantni mehaniki ni mogoče ustvariti neodvisne in identične kopije poljubnega neznanega kvantnega sistema.*

Alice izmeri	**Bob - H**	**Bob - V**	**Bob - R**	**Bob - L**
H	1	0	1/2	1/2
V	0	1	1/2	1/2
R	1/2	1/2	1	0
L	1/2	1/2	0	1

Tabela 2: Tabela rezultatov meritev. Žarek $4n$ fotonov razdelimo na 4 dele. Tabela prikazuje kolikšen delež n fotonov, ki potujejo na posamezen detektor, bo detektiran pri Bobu glede na polarizacijo originalnega fotona.

Dokaz. Predpostavimo, da imamo delujočo napravo za kvantno kloniranje. Naprava ima dve reži označeni z A in B. Reža A je podatkovna reža (vhod), v katero vstavimo kvantni sistem, ki ga želimo klonirati. Sistem mora biti reprezentabilen z valovno funkcijo $|\psi\rangle$ (tj. zahtevamo, da je vhodno stanje čisto). Reža B je naslovna reža (izhod). Predpostavimo, da za vse namene kloniranja v reži B začnemo s standardno valovno funkcijo, ki jo lahko reprezentiramo s $|s\rangle$. Tedaj je začetno stanje naprave za kloniranje

$$|\psi\rangle \otimes |s\rangle. \tag{11}$$

Postopek kloniranja simboliziramo z uporabo operatorja unitarne časovne evolucije U (želimo namreč ohranjati verjetnost/skalarni produkt). Zanj velja, da iz začetnega stanja naprave ustvari sledeče

$$|\psi\rangle \otimes |s\rangle \xrightarrow{\mathrm{U}} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle. \tag{12}$$

Predpostavimo, da opisani postopek deluje za dve stanji reprezentabilni z valovnimi funkcijami $|\psi\rangle$ in $|\varphi\rangle$. Tedaj dobimo

$$\begin{aligned} U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle \\ U(|\varphi\rangle \otimes |s\rangle) &= |\varphi\rangle \otimes |\varphi\rangle. \end{aligned} \tag{13}$$

V nadaljevanju vzamemo zgornji dve enačbi in izračunamo notranji produkt za levo in desno stran

$$\langle\, U(|\psi\rangle \otimes |s\rangle)\,,\, U(|\varphi\rangle \otimes |s\rangle)\,\rangle = \langle\, |\psi\rangle \otimes |s\rangle\,,\, |\varphi\rangle \otimes |s\rangle\,\rangle = \langle\psi,\varphi\rangle\,\langle s,s\rangle = \langle\psi,\varphi\rangle \tag{14}$$

$$\langle\, |\psi\rangle \otimes |\varphi\rangle\,,\, |\psi\rangle \otimes |\varphi\rangle\,\rangle = \langle\psi,\varphi\rangle\,\langle\psi,\varphi\rangle = (\langle\psi,\varphi\rangle)^2\,. \tag{15}$$

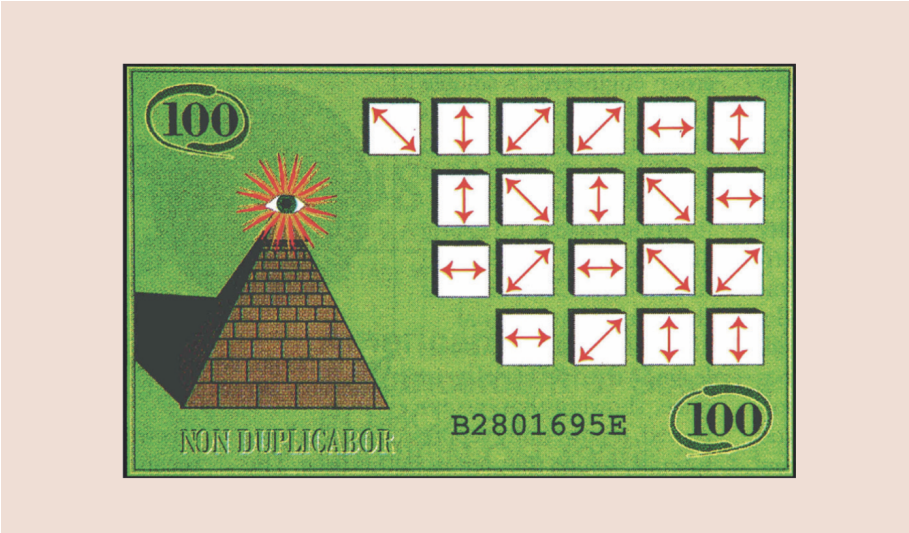
Rezultata enačimo in dobimo

$$\langle\psi,\varphi\rangle = (\langle\psi,\varphi\rangle)^2\,. \tag{16}$$

Vidimo, da imamo enačbo oblike $x = x^2$, ki ima le dve rešitvi, $x = 0$ in $x = 1$. Rezultat si interpretiramo takole: če bi takšna naprava lahko uspešno klonirala vsaj dve valovni funkciji $|\psi\rangle$ in $|\varphi\rangle$, tedaj mora veljati, da je $|\psi\rangle = |\varphi\rangle$ ali pa sta valovni funkciji $|\psi\rangle$ in $|\varphi\rangle$ ortogonalni. Iz teoretičnega rezultata zaključimo, da naprave za popolno kloniranje poljubnih neznanih kvantnih sistemov ni mogoče ustvariti. □

4 Kvantni denar

Izrek o prepovedi kloniranja postavi kar nekaj omejitev za nastajajoče kvantne tehnologije. Hkrati pa tudi odpira nove, prej nedosegljive možnosti uporabe. Ena izmed njih (in hkrati glavna tema našega seminarja) je shema t.i. kvantnega denarja. Le-ta z uporabo izreka o prepovedi kloniranja uvaja koncept (tudi v teoriji) neponaredljivega fizikalnega sistema, če njegovih lastnosti v naprej ne poznamo.



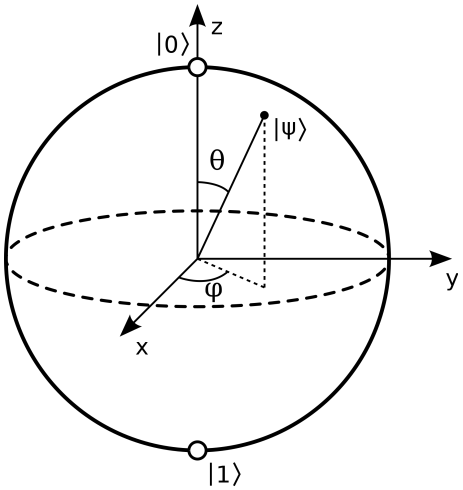
Slika 3: Ilustracija kvantnega bankovca. Papirnat bankovec na sliki je opremljen z različno polariziranimi kvantnimi spominskimi celicami in serijsko številko. [Aar+12]

4.1 Delovanje sheme

Shemo kvantnega denarja je leta 1983 v svojem članku konceptualno opisal Stephen Wiesner [Wie83]. Kot ilustrirano na Sliki 3, je vsak bankovec opremljen s serijsko številko in nizom kvantnih sistemov dolžine N, ki jih pripravimo v določeni (verjetno naključni) konfiguraciji $|\$_i\rangle$, $1 \leq i \leq N$. Naloga izdajatelja takih bankovcev je, da za vsak kvantni bankovec na varnem mestu shrani slovar serijskih številk in pripadajočo konfiguracijo $|\$_i\rangle$ za $\forall\, i$ (skrivni ključ). Varnost sistema se skriva v tem, da ponarejevalec ne ve, v kateri bazi vrne meritev sistema $|\$_i\rangle$ enoličen rezultat. Torej bo pri meritvi lahko naredil napako in jo izvedel v napačni bazi. Napačno stanje kubita bo nato zapisal na ponarejeni bankovec, kar bo pri preverjanju v banki, ki zaporedje pravilno izbranih baz pozna, detektirano. Ker je na bankovcu N kvantnih sistemov, verjetnost za popolno kopijo celotnega niza pada eksponentno z $P^N \to 0$. P predstavlja verjetnost, da posamezen kubit na ponarejenem bankovcu pri preverjanju producira pravilen rezultat. Dodatno zahtevamo še $0 < P < 1$. Za preprost poskus ponarejanja, kjer ponarejevalec med ponarejanjem nima dostopa do validacije bankovca, je bilo leta 2012 v [MVW12] pokazano, da za P ustreza vrednost $(3/4)$.

4.2 Izbira baze za meritev

Kaj pomeni izbira baze, lahko fizikalno še malo bolje razložimo. Kot opisano v točki 2.2, je možno vsak kubit reprezentirati s točkami na Blochovi sferi kot prikazano na Sliki 4.



Slika 4: Blochova sfera. V smeri z sta definirani stanji $|0\rangle$ in $|1\rangle$. [Blo]

V smeri z definiramo stanji $|0\rangle$ in $|1\rangle$, ki predstavljata npr. spin dol in gor v smeri z. Vemo, da lahko spin merimo tudi v smeri x in y, odvisno od orientacije Stern-Gerlachove naprave. Tedaj bi želeli zapisati tudi valovno funckcijo takšnega sistema. Pri tem si lahko pomagamo z enačbo 2 in vanjo vstavimo primerne kote θ, φ za bazo v smereh x, y in z. Iz enačbe 2 tedaj dobimo 6 različnih normiranih valovnih funkcij (enačba 17). Vemo, da ima spin 2 lastni vrednosti, in sicer ± 1. Tedaj so matrični operatorji, ki ustrezajo tem lastnim vrednostim in lastnim vektorjem kar Paulijeve matrike σ_x, σ_y, σ_z. [Pau]

$$\begin{aligned} \psi_{x+} &= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \quad \psi_{x-} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}, \\ \psi_{y+} &= \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}, \quad \psi_{y-} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}, \\ \psi_{z+} &= \begin{bmatrix}1\\0\end{bmatrix}, \qquad \psi_{z-} = \begin{bmatrix}0\\1\end{bmatrix}. \end{aligned} \tag{17}$$

Če torej naš kvantni sistem pripravimo v stanju ψ_{x+} in merimo v smeri x, izmerimo lastno vrednost $+1$. V kolikor merimo ta isti sistem v smeri z ali y, izmerimo lastno vrednost $+1$ z verjetnostjo $1/2$ in -1 z verjetnostjo $1/2$. Z drugimi besedami: ob meritvi dobimo enoličen rezultat le, če merimo v smeri lastnega vektorja valovne funkcije, torej moramo valovno funkcijo že od začetka poznati.

4.3 Pomanjkljivosti in ranljivosti

Ena izmed poglavitnih težav Wiesnerjeve sheme kvantnega denarja je odvisnost od banke za preverjanje avtentičnosti bankovca. Banka mora biti vključena pri vsaki izmenjavi bankovca, saj bi z razkritjem skrivnih ključev na bankovcih padla celotna varnostna shema. Obstajata še dve pomanjkljivosti: relativno velika dolžina skrivnih ključev in ranljivost na interaktivne napade. V [Bro+16] so leta 2016 pokazali, da lahko samo z večkratno verifikacijo istega bankovca in metodo, ki bazira na kvantnem preizkuševanju (test za bombe Elitzurja in Vaidmana), uspešno ponaredijo bankovec. Kot edina rešitev se tukaj pokaže ponovna izdaja bankovca ob vsaki verifikaciji (in s tem povezano večanje velikosti skrivnega ključa).

Zadnji napaki se da odpraviti, še vedno pa ostaja prva. Zato je glavni cilj nadaljnjih raziskav razvoj protokola t.i. kvantnega denarja z uporabo javnih ključev. Analogno s klasično simetrično kriptografijo, originalna Wiesnerjeva shema ustreza kvantnemu denarju z zasebnim ključem, saj lahko avtentičnost preveri le banka. Kvantni denar z javnim ključem pa bi analogno asimetrični klasični kriptografiji omogočal verifikacijo vsakomur. Ena izmed poglavitnih težav te nadgrajene sheme izvira že iz kvantnega denarja z zasebnimi ključi. Z večkratnim verificiranjem lahko ponarejevalec pridobi dodatne informacije o stanju kvantnega sistema, ki ga želi klonirati. V članku [AC12] avtorji predlagajo sistem kvantnega denarja z zasebnim ključem, ki omogoča neomejeno verifikacij in še vedno ostaja varen, kot tudi nov varen sistem kvantnega denarja z javnim ključem.

4.4 Decentraliziran kvantni denar

Na podlagi sheme kvantnega denarja z javnim ključem [AC12] so v delu tudi naprednejše sheme, ki namesto centralne banke v vlogo verifikatorja postavijo decentraliziran sistem validatorjev. V članku Kvantni Bitcoin avtorji ([Jog19]) nadgradijo protokol veriženja blokov Bitcoin, ki ga uporabijo za verifikacijo in izdajo fiksne količine fizičnih kvantnih bankovcev kot primer decentralizirane valute, ki je ne nadzoruje nobena banka, temveč decentraliziran sistem validatorjev.

4.5 Fizična realizacija

Trenutno ne obstaja nobena praktična in cenovno ugodna tehnologija, ki bi omogočala masovno implementacijo katere koli prej opisane sheme. Za to namreč potrebujemo t.i. kvantni pomnilnik - komponento analogno npr. pomnilniku FLASH - ki je za daljše časovno obdobje sposobna shraniti stanje kubita in je odporna na motnje iz okolice. Trenutno je to eno izmed bolj aktivnih področij raziskav. Avtorjem nedavnega članka [Rob] je uspelo ustvariti dvokubitni register, ki lahko pri temperaturi 1.5 K shrani kvantno stanje fotonov za nekaj več kot 2 sekundi.

5 Zaključek

V okviru tega seminarja smo preleteli osnovne koncepte kvantne informatike, dokazali izrek o prepovedi kloniranja in pokazali njegovo uporabo na konceptu kvantnega denarja, ki rešuje praktičen problem ponarejanja. Poleg kvantnega denarja so aktivna področja raziskav tudi: super gosto kodiranje, kvantna izmenjava ključev (QKD), kvantne kode za popravljanje napak, kvantni algoritmi, itd. Zanimvo bo videti, kako hitro nam bo uspelo zapletene kvantne naprave iz laboratorijev preseliti v naš vsakdan.

Literatura

[Aar+12] Scott Aaronson in sod. "Quantum Money". V: *Communications of the ACM* 55.8 (avg. 2012), str. 84–92. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/2240236.2240258. URL: https://dl.acm.org/doi/10.1145/2240236.2240258 (pridobljeno 27. 3. 2023).

[AC12] Scott Aaronson in Paul Christiano. *Quantum Money from Hidden Subspaces*. 17. sep. 2012. DOI: 10.48550/arXiv.1203.4740. arXiv: 1203.4740 [quant-ph]. URL: http://arxiv.org/abs/1203.4740 (pridobljeno 17. 4. 2023). preprint.

[Ban18] European Central Bank. *Security Features*. European Central Bank. 11. sep. 2018. URL: https://www.ecb.europa.eu/euro/banknotes/security/html/index.en.html (pridobljeno 29. 3. 2023).

[Blo] *Bloch Sphere*. V: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=Bloch_sphere&oldid=1131941942 (pridobljeno 17. 4. 2023).

[Bro+16] Aharon Brodutch in sod. *An Adaptive Attack on Wiesner's Quantum Money*. Ver. 4. 10. maj 2016. DOI: 10.48550/arXiv.1404.1507. arXiv: 1404.1507 [quant-ph]. URL: http://arxiv.org/abs/1404.1507 (pridobljeno 17. 4. 2023). preprint.

[Chr+06] De Nardi Christophe in sod. "Descrambling and Data Reading Techniques for Flash-EEPROM Memories. Application to Smart Cards." V: *Microelectronics Reliability* 46 (1. sep. 2006), str. 1569–1574. DOI: 10.1016/j.microrel.2006.07.022.

[Cs1] *CS101 Introduction to Computing Principles*. URL: https://web.stanford.edu/class/cs101/security-8-emv.html (pridobljeno 27. 3. 2023).

[Her82] Nick Herbert. "FLASH—A Superluminal Communicator Based upon a New Kind of Quantum Measurement". V: *Foundations of Physics* 12.12 (1. dec. 1982), str. 1171–1179. ISSN: 1572-9516. DOI: 10.1007/BF00729622. URL: https://doi.org/10.1007/BF00729622 (pridobljeno 25. 3. 2023).

[Jog19] Jonathan Jogenfors. "Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics". V: *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Maj 2019, str. 245–252. DOI: 10.1109/BLOC.2019.8751473. arXiv: 1604.01383 [quant-ph]. URL: http://arxiv.org/abs/1604.01383 (pridobljeno 17. 4. 2023).

[Jon] *Jones Calculus*. V: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=Jones_calculus&oldid=1138252327 (pridobljeno 31. 3. 2023).

[Mara] Marco Cerezo. *Entangled Particles, Faster than Light Communications and the No-Cloning Theorem*. Entangled Physics: Quantum Information & Quantum Computation. URL: https://entangledphysics.com/2015/09/20/entangled-particles-faster-than-light-communications-and-the-no-cloning-theorem/ (pridobljeno 31. 3. 2023).

[Marb] Marco Cerezo. *Entanglement (I): How It All Began, the EPR Paradox*. Entangled Physics: Quantum Information & Quantum Computation. URL: https://entangledphysics.com/2015/03/28/entanglement-how-it-all-began-the-epr-paradox/ (pridobljeno 25. 3. 2023).

[MVW12] Abel Molina, Thomas Vidick in John Watrous. *Optimal Counterfeiting Attacks and Generalizations for Wiesner's Quantum Money*. 17. feb. 2012. DOI: 10.48550/arXiv.1202.4010. arXiv: 1202.4010 [quant-ph]. URL: http://arxiv.org/abs/1202.4010 (pridobljeno 17. 4. 2023). preprint.

[NC12] Michael A. Nielsen in Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 1. izd. Cambridge University Press, 5. jun. 2012. ISBN: 978-1-107-00217-3 978-0-511-97666-7. DOI: 10.1017/CBO9780511976667. URL: https://www.cambridge.org/core/product/identifier/9780511976667/type/book (pridobljeno 25. 3. 2023).

[Noc] *No-Cloning Theorem*. V: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=No-cloning_theorem&oldid=1127026717 (pridobljeno 25. 3. 2023).

[Pau] *Pauli Matrices*. V: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=Pauli_matrices&oldid=1148849186 (pridobljeno 17. 4. 2023).

[Per03] Asher Peres. "How the No-Cloning Theorem Got Its Name". V: *Fortschritte der Physik* 51.45 (7. maj 2003), str. 458–461. ISSN: 00158208, 15213978. DOI: 10.1002/prop.200310062. arXiv: quant-ph/0205076. URL: http://arxiv.org/abs/quant-ph/0205076 (pridobljeno 25. 3. 2023).

[Pom22] Miha Pompe. *Kvantni algoritmi*. 2022.

[Qua] *Quantum Money*. V: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=Quantum_money&oldid=1129889107 (pridobljeno 25. 3. 2023).

[Rob] *Robust Multi-Qubit Quantum Network Node with Integrated Error Detection — Science*. URL: https://www.science.org/doi/10.1126/science.add9771 (pridobljeno 17. 4. 2023).

[Sof] *Software Detection of Currency // Professor Steven J. Murdoch*. URL: https://murdoch.is/projects/currency/ (pridobljeno 29. 3. 2023).

[Tac] *Tachyonic Antitelephone*. V: *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?title=Tachyonic_antitelephone&oldid=1099786308 (pridobljeno 17. 4. 2023).

[Ž17] Rok Žitko. *Kvantne in Računalniške Tehnologije*. 1. izd. DMFA založništvo, 2017. ISBN: 978-961-212-278-2. URL: http://www.dmfa-zaloznistvo.si/zipf/2012.htm.

[Wie83] Stephen Wiesner. "Conjugate Coding". V: *ACM SIGACT News* 15.1 (1. jan. 1983), str. 78–88. ISSN: 0163-5700. DOI: 10.1145/1008908.1008920. URL: https://dl.acm.org/doi/10.1145/1008908.1008920 (pridobljeno 25. 3. 2023).

[WZ82] W. K. Wootters in W. H. Zurek. “A Single Quantum Cannot Be Cloned”. V: *Nature* 299.5886 (5886 okt. 1982), str. 802–803. ISSN: 1476-4687. DOI: 10.1038/299802a0. URL: https://www.nature.com/articles/299802a0 (pridobljeno 25. 3. 2023).