Cos'è la moneta quantistica?

Piero A. Bonatti, Paolo Strolin e Arturo Tagliacozzo

Per poter capire cosa è la moneta quantistica e quali benefici ci aspettiamo di ottenere quando la potremo realizzare, iniziamo ricapitolando cosa è stato e cosa è diventato il denaro nel corso dei millenni.

In origine, vengono usati come monete oggetti presenti in natura, come le conchiglie. Col tempo si passa a oggetti appositamente costruiti, come le monete e le banconote. Con l'avvento dell'era dell'informazione, anche la moneta diventa un oggetto digitale (un file, una stringa di bit), che può essere speso semplicemente trasmettendolo su di una rete di comunicazione. Queste monete vengono dette *elettroniche*.

Una lista non esaustiva di monete elettroniche di cui si è parlato sui media:

PayPal, eCash, WebMoney, Bitcoin

- Caratteristiche di una moneta ideale:

Ovviamente una moneta - reale o virtuale che sia-

- non dovrebbe essere falsificabile
- non dovrebbe essere alterabile (per es. aumentandone il valore)
- non dovrebbe essere spendibile piu' volte
- non dovrebbe essere tracciabile (dovrebbe garantire l' anonimato dello scambio)

L'ultimo punto e' il meno ovvio ed il piu' delicato:

Discussione: In realtà, per scoprire frodi e per combattere delinquenza organizzata e terrorismo, può essere utile violare la privacy dei malintenzionati. Il giusto equilibrio tra il rispetto della privacy e il supporto alle indagini degli investigatori continua a suscitare vivaci dibattiti, come testimoniato dal recente confronto tra FBI e Apple. Si veda:

http://www.ilpost.it/2016/02/17/apple-fbi-iphone/

Pur tuttavia uno stato Panopticon e' uno stato autoritario.

Ricordare il carcere ideale progettato nel 1791 dal filosofo e giurista Jeremy Bentham. Ricordare "Sorvegliare e punire" di Michel Focault

- non dovrebbe essere falsificabile. Sappiamo tutti che ad oggi questo non è possibile, la falsificazione può solo essere resa abbastanza difficile e costosa da renderla rara (limitandone così i danni). Ad esempio, per le monete "reali" si adottano filigrane o inchiostri particolari e strisce metalliche inserite nelle banconote. Per le monete elettroniche, invece, si fa uso della *crittografia a chiave pubblica*.

Per capire, in una parola, che significa "*crittografia a chiave pubblica*", immaginate che voi, A, vogliate ricevere un pacco da B con la sicurezza che nessuno possa aprirlo e curiosarvi dentro prima che giunga fino a voi. Allora voi spedite a B un lucchetto aperto, alla luce del sole (pubblicamente), del quale trattenete la chiave. B sigillera' il pacco chiudendo l'imballo con il lucchetto e lo spedirà a voi e solo voi, avendo la chiave di quel lucchetto, potete aprirlo.Naturalmente, se voi potete con la vostra chiave aprire il pacco, avete la sicurezza che quel pacco è destinato a voi.

La crittografia a chiave pubblica permette quindi di fare diverse cose:

1. *Cifrare* una informazione in modo da renderla comprensibile solo a chi ha il permesso di leggerla;

2. *Firmare* una informazione in modo da garantirne l'autenticità;

3. Garantire l'*integrità* di una informazione, cioè che non sia stata alterata (cosa non banale nel mondo digitale dove modificare una stringa di bit è estremamente facile).

La crittografia a chiave pubblica si basa sull'esistenza di operazioni per le quali non sono noti algoritmi "abbastanza veloci". Pertanto violare la cifratura (cioè decodificare un messaggio, falsificare una firma, alterare una informazione senza essere scoperti) è possibile ma *richiede troppo tempo* per essere utile in pratica ai malintenzionati: nel frattempo la chiave crittografica sarà cambiata, l'informazione scoperta o alterata sarà vecchia e sorpassata, e così via. In questo senso diciamo che la crittografia a chiave pubblica non è inerentemente sicura ma solo *computazionalmente sicura*.

Un **esempio** importanitissimo di crittosistema a chiave pubblica è ***RSA***, pressochè onnipresente tra i sistemi e le applicazioni informatici protetti da crittografia.

RSA si basa sul calcolo del *logaritmo discreto* nei gruppi finiti:

Dati tre numeri naturali m,n,c trovare un numero k tale che $m^k \bmod n = c$.

(mod 12 è l'aritmetica dell'orologio: dopo l'ora 12, si ricomincia daccapo).

Il calcolo dei logaritmi discreti è strettamente connesso con la scomposizione di grossi numeri interi in numeri primi tra loro. RSA è sicuro perchè non sono noti algoritmi per risolvere questo problema "velocemente".

Nel caso della moneta elettronica, la sua "zecca digitale" (la banca) può produrre monete elettroniche che in pratica non sono falsificabili o alterabili semplicemente apponendo la propria *firma digitale* su ogni moneta.

Tuttavia la "banca" potrebbe memorizzare a quale utente ha rilasciato ogni moneta, e quando un commerciante torna alla banca per accreditarla sul proprio conto, la banca potrebbe identificare chi l'ha spesa facendo una ricerca nei propri archivi (tacciare l'operazione di scambio). Importante per la privacy è che il contante sia anonimo.

In alcuni casi, con opportune tecniche crittografiche, si può permettere di identificare chi ha speso il denaro *solo in presenza di una violazione*. Ad esempio questo è possibile per risolvere un potenziale problema che affligge solo le monete elettroniche detto *double spending*. Mentre una moneta reale è un oggetto fisico che in ogni istante può essere nelle mani di una sola persona, una stessa moneta elettronica potrebbe essere copiata e spesa più volte, con commercianti diversi. Sono stati sviluppati algoritmi crittografici che alla seconda spesa permettono di ricostruire l'identità dell'utente che ha speso il denaro più volte - sia egli il cliente o il commerciante.

- Perche' la moneta elettronica diventera' insicura.

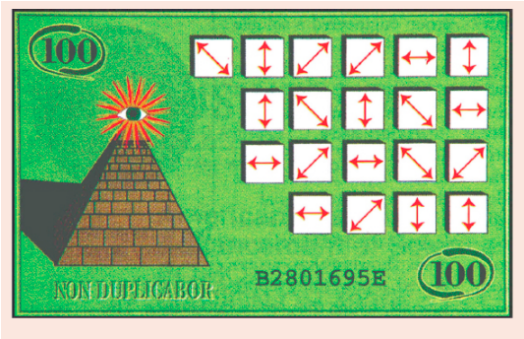
La moneta elettronica da' garanzie grazie ad algoritmi di criptazione come l' RSA. Rompere con la "forza bruta" questi algoritmi va oltre la capacità di elaborazione del piu' rapido dei computer attuali. Nel 1994 Peter Shor propose "a tavolino" un algoritmo che usa la sovrapposizione tra stati quantistici per scomporre grossi interi in numeri primi dimostrando che velocita' di elaborazione riduce così tanto i tempi da divenire, in principio fattibile. Naturalmente il computer quantistico capace di elaborare questo algoritmo quantistico non esiste ancora. Due anni dopo Lov Grover ha fatto lo stesso con l'algoritmo DES. La moneta elettronica diventera' insicura.

Intuizione: se il calcolo quantistico e' in grado di infirmare la moneta elettronica, non e' possibile usarlo invece per sviluppare una moneta quantistica inattaccabile?

La crittografia quantistica

Dai computer quantistici - quando saranno effettivamente disponibili - ci si aspetta un notevole guadagno in velocità. I problemi che i computer quantistici sono in grado di risolvere "abbastanza velocemente" (ovvero in un tempo che cresce come un polinomio al crescere della dimensione del problema) corrispondono alla classe di problemi nota come BQP (*Bounded-error Quantum Polynomial-time*) che comprende alcuni dei problemi che *non* sappiamo come risolvere velocemente con un calcolatore tradizionale. Tra i problemi in BQP troviamo anche il già citato calcolo del logaritmo discreto, la cui difficoltà è l'unica garanzia di sicurezza per la crittografia RSA. Di conseguenza, con l'avvento dei calcolatori quantistici, la maggior velocità di soluzione di simili problemi difficili renderà insicuri gli attuali metodi di

crittografia. Per questa ragione, sono già in fase di studio nuovi metodi crittografici che forniscano garanzie di sicurezza anche rispetto a un computer quantistico.



- Inattaccabilita' della moneta quantistica: non tirate gatti che non conoscete contro cancellate!

Considerate un fotone. Ha due possibili polarizzazioni ortogonali: il campo elettromagnetico oscilla lungo una direzione lineare o la sua direzione ortogonale. Gli occhiali Polaroid sono riposanti perche' agiscono nei confronti della luce come la cancellata che circonda un edificio: solo se si tirano contro la cancellata bastoni orientati parallelemente alle sue aste questi possono attraversarla. Se i bastoni sono orientati in direzione ortogonale cadono miseramente a terra nell'urto. Cosi' i fotoni che attraversano il reticolo Polaroid hanno solo polarizzazione fissata, per la gioia dei nostri occhi. Solo chi ha preparato il fotone con una polarizzazione data potra' usare una fenditura orientata allo stesso modo che lo fara' passare indenne. Così il fotone manterrà la sua polarizzazione e il proprietario della moneta avra' verificato che essa non e' falsa. Se uno privo di questa informazione dovesse provarci con una fenditura in una direzione "altra" rispetto alla polarizzazione dei fotoni, una meta' dei fotoni passerebbe con polarizzazione ruotata secondo la direzione della fenditura, l'altra meta' verrebbe respinta all'indietro. Questo perché l'orientazione della polarizzazione del fotone lungo una direzione assegnata (diciamo quella diagonale) e' equivalente alla sovrapposizione di due stati quantistici di fotone, ciascuno orientato in una di due direzioni ortogonali (in questo caso la direzione verticale della fenditura e quella orizzontale) . Se il fotone polarizzato in diagonale fosse un gatto che l'intruso vuole lanciare in diagonale contro la cancellata verticale, esso gatto è la sovrapposizione di "gatto vivo" e "gatto morto" (leggi: le due polarizzazioni orizzontale e verticale). Al 50 % di probabilita' il gatto si troverebbe come gatto vivo al di la' della cancellata e al 50% al di qua di essa come gatto morto[*nota al fondo*].

In ogni caso, nel passaggio attraverso una fenditura non orientata secondo la polarizzazione del fotone, la memoria della polarizzazione primitiva viene persa. La moneta che cade nelle mani di un intruso si autodistrugge. La probabilita' che una lunga stringa di fotoni polarizzati in varie direzioni possa essere letta da un intruso che non saprebbe come orientare appropriatamente la successione di fenditure per non alterare la stringa e' estremamente piccola quanto piu' e' lunga la stringa.

La polarizzazione scelta per il fotone viene costruita facendo vivere il fotone in un *qubit,* il mattone elementare della computazione quantistica, cosi' come il transistor lo è per un calcolatore classico. Operazioni di questa natura sono fattibili e verificate in laboratorio con fotoni gia' da una quindicina d'anni.

-Moneta quantistica reale (banconota quantistica)

Sul supporto-banconota si puo' immaginare di mettere dei qubit nella forma di un singolo atomo intrappolato in una nanocavita' che emette e riassorbe il fotone incessantemente. (pensate al forno delle pizze con la luce infrarossa (il calore) che urta da una parete all'altra e la pizza che si cuoce). La forma della cavita' determina la polarizzazione del fotone che viene emesso e riassorbito dall'atomo. Tante trappole atomiche integrate sulla banconota ne custodiscono la sua "firma" e garantisce la sua integrità. Inoltre, per definizione, la banconota, passando di mano in mano non puo' essere spesa due volte. L'idea originale dell'ideatore delle monete quantistiche, Stephen Wiesner, prevedeva però che per controllare l'autenticità di una banconota quantistica la si dovesse presentare alla banca che l'ha creata. Questa può confrontare lo stato dei qubit con quello memorizzato al momento della creazione e verificare così se la banconota è

autentica. Il problema è che questo in pratica crea un collo di bottiglia e un potenziale rischio per la privacy (questo sistema non è anonimo: basta che la banca ricordi a quale cliente ha consegnato la banconota per identificare chi ha speso il denaro, perchè con questo sistema dopo il primo acquisto la banconota torna subito nelle mani della banca emittente).

Quindi la maggior parte della ricerca di questi ultimi anni dedicata alla moneta quantistica ha cercato di rimuovere questo problema cercando meccanismi diversi, che permettano ad ognuno di verificare personalmente l'autenticità delle monete quantistiche. Una sorta di ibrido tra la crittografia a chiave pubblica (che risolve elegantemente questo problema per le monete elettroniche) e la moneta quantistica originale. Per quanto siano stati proposti diversi schemi per la realizzazione di monete quantistiche auto-verificabili, a tutt'oggi nessuno è stato in grado di dimostrare che il proprio schema è effettivamente sicuro, perchè queste soluzioni comprendono forme di crittografia che sono solo *computazionalmente* sicure.

La moneta quantistica non e' duplicabile. *Uno stato quantico* custodito dal qubit *non puo' essere clonato*. Grosso-modo, il motivo e' che, all'atto della sua preparazione, esso viene irreversibilmente intrecciato con lo stato dell'ambiente in cui viene creato. Se uno prova a farne uno "uguale", questo non potra' risultare intrecciato esattamente allo stesso modo dell'altro con un ambiente identico all'altro. La " firma" della banconota non puo' essere identica.

- Moneta quantistica virtuale

Ogni supporto può essere eliminato. Occorre una sorgente di fotoni che emetta due fotoni in direzione opposta verso i soggetti della transazione pecuniaria. La transazione avviene per "teletrasporto". Colui che "paga", operando sul suo qubit-fotone con la sua fenditura, determina automaticamente che il fotone che giunge all'altro partner sia esattamente polarizzato come quello che aveva lui.

Teletrasporto di un qubit

Come detto, un singolo atomo in una trappola è in conpresenza con un fotone la cui polarizzazione e' la sovrapposizione di due polarizzazioni ortogonali, in una combinazione che caratterizza lo "stato" del qubit. Trattasi di un "qubit-fotone". Alice ha con sè uno stato di qubit-fotone che chiamiamo stato A e vuole teletrasportarlo a Bob che e' in altro luogo. Al giorno d'oggi e' possibile emettere una coppia di fotoni (B,C) che viaggiano in direzione diversa e che, generati insieme, restano quantisticamente "intrecciati" (entanglement) (se il percorso non e' rettilineo, basta far viaggiare B e C in fibra ottica). Ad Alice giunge il fotone B, a Bob quello C.

La successione di operazioni e' la seguente:

1. Alice sovrappone il fotone A con quello B creando la coppia (A,B). Ora tutti e tre i fotoni sono intrecciati.
2. Alice sceglie di far passare il fotone A in una fenditura orientata a suo piacere e quello B in un'altra (in gergo si dice che compie una misura, anche se poi non guarda il risultato). Queste operazioni hanno conseguenze sulla coppia (A,B) che, per altro, Alice nemmeno conosceva in dettaglio, ma anche sul fotone C di Bob, che e' intrecciato con la coppia (A,B) a distanza.
3. Alice telefona a Bob e gli comunica come erano orientate le fenditure nella misura che ha fatto.
4. Bob ruota (alla cieca) la polarizzazione del fotone C in base alla indicazione di Alice.

Il risultato sara' che Bob ha ricostruito il fotone A senza che nessuno abbia mai conosciuto la polarizzazione di alcun fotone.

Notare che

- Dai fotoni che sono usciti dalle fenditure di Alice, Alice non ha possibilità di risalire all'originario fotone A: il fotone A e' scomparso dalle mani di Alice ed e' comparso nelle mani di Bob. Non c'e' stata clonazione ma teletrasporto.

- Non c'è violazione del principio che l'informazione non puo' viaggiare tra due punti a velocita' superiore a quella della luce. Qui l'unica informazione e' stata trasferita per canale convenzionale (telefono).

Il fatto che i qubit non possano essere copiati senza modificarli previene anche il problema del *double spending* senza bisogno di misure aggiuntive. Nemmeno la banca che crea le banconote potrebbe crearne due uguali. Copiare dei qubit senza modificare gli originali è impossibile.

- Monete quantistiche e monete elettroniche a confronto

Premessa: le monete quantistiche non sono ancora realizzabili con la tecnologia attuale, e non lo saranno ancora per diversi anni, mentre le monete elettroniche sono già una realtà. Quindi il confronto verterà necessariamente sulle loro proprietà teoriche.

Le monete quantistiche non sono duplicabili *in assoluto* per le leggi fisiche che governano la meccanica quantistica, mentre come abbiamo visto la contraffazione delle monete elettroniche è "solo" computazionalmente difficile (la probabilità di contraffare una moneta e potersene avvantaggiare è infinitesimale e maggiore di zero). Le monete quantistiche, ovviamente, presentano lo stesso vantaggio anche rispetto a quelle tradizion

Leggere la polarizzazione del fotone

La banconota che la Fisica Quantistica garantisce non possa essere contraffatta, avrà, al posto della striscia argentea dell'ologramma, venti fotoni separati, ciascuno in uno stato di polarizzazione definito. Venti trappole di singolo fotone ("ion trap, atomic trap, photon trap"). I fotoni debbono essere singoli e non sovrapponibili altrimenti la loro polarizzazione può cambiare nel tempo.

In un registro custodito presso la banca saranno catalogati numero di serie della banconota e relative orientazioni delle polarizzazioni di ciascun fotone. La banca è l'unica titolata a gestire la verifica di autenticità dando indicazione su come orientare " il reticolo polaroid " nella direzione opportuna quando si vada a misurare. Solo con l'orientazione giusta la polarizzazione del fotone non sarà turbata e la banconota riconosciuta vera. Con un'orientazione sbagliata, la polarizzazione del fotone sarà anche alterata e la banconota annullata. E' come al bancomat dove è prevista l'inchiostratura automatica delle banconote in caso di effrazione.

Come sempre, tra il dire ed il fare c'è di mezzo tanta evoluzione tecnologica. Le domande sono ovvie:

- Come intrappolare un fotone?
- Come leggerne la polarizzazione lasciando poi il fotone lì dove è?
- Come garantire che perturbazioni esterne non ne cambino lo stato di polarizzazione?
- Come correggere eventuali errori (eventi indesiderati di alterazione) che dovessero essere indotti da cause accidentali?

Intrappolare un fotone non è difficile: occorre una cavità ottica fatta di specchi che lo riflettano avanti e dietro senza farlo sfuggire. Difficile è "leggerne" la polarizzazione lasciandolo lì dove è. "Leggerlo" senza perderlo. Il nostro occhio legge i fotoni che arrivano ma la pupilla li assorbe ed essi scompaiono. Per un singolo fotone, un processo analogo lo realizza un atomo introdotto nella cavità detta sopra. Se l'atomo passa dallo stato fondamentale ad uno stato eccitato vuol dire che il fotone c'era e l'atomo lo ha assorbito. Certo l'atomo può diseccitarsi e riemettere il fotone, ma non è più lo stesso fotone di prima, con la polarizzazione di prima. La banconota si è danneggiata.

Come fare in modo che nel processo di "lettura" il fotone non venga assorbito e poi riemesso? Nel 2012 è stato dato il premio Nobel ad S.Haroche e D.J.Wineland per la loro capacità di manipolare atomi e fotoni in interazione.

http://nobelprize.org/nobel_prizes/physics/laureates/2012/advanced-physicsprize2012_02.pdf

In una parola il trucco per salvare il fotone è fare in modo che l'atomo abbia voglia di assorbirlo, ma non possa farlo perché il nostro fotone non è in grado di eccitare l'atomo (non ha l'energia sufficiente). L'atomo allora si eccita prendendo l'energia da un altro fotone ancillare, messogli da noi a disposizione. Come se il fotone che ci interessa catalizzasse il processo di eccitazione dell'atomo. Miracoli dell'ottica Quantistica.

La risposta alle altre due domande poste sopra, ancora frammentaria, contribuirete a darla voi se studierete nei prossimi anni questa Fisica.

- Nota a margine:

tutta la fisica moderna ha proceduto costruendo esperimenti concettuali (in tedesco "Gedanken Experiment"). Del resto, si vocifera che anche Galileo, i suoi esperimenti col piano inclinato, non li abbia mai fatti. Ed il suo meraviglioso esperimento che giustifica il principio di relativita' galileana e' splendidamente concettuale.

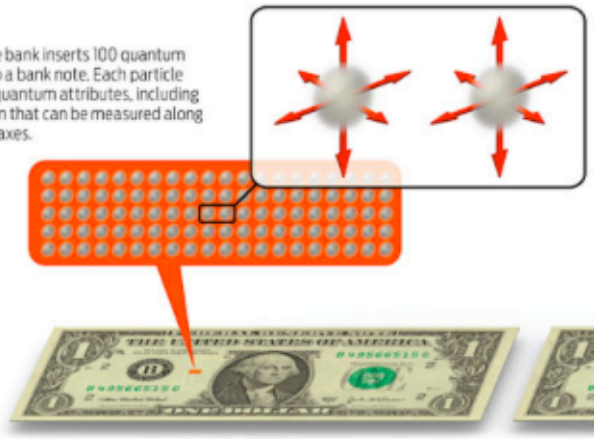
(" Riserratevi con qualche amico nella maggiore stanza che sia sotto coverta di alcun gran navilio, e quivi fate d'aver mosche, farfalle e simili animaletti volanti …" leggete il passo dal "Dialogo sopra i due massimi sistemi del mondo"

http://www.dima.unige.it/~denegri/PLS2/PENSIERO_SCIENTIFICO%20DEF/ESPERIMENTO_REALE/Pages/RELATIVITA'.htm

). Non parliamo poi di Einstein…

Esperimenti concettuali hanno scatenato diatribe sui fondamenti della Fisica Quantistica. L'emozione sta nel constatare che, con l'avanzare della tecnologia, questi esperimenti diventano, nel tempo, alla portata dei nostri laboratori e costituiscono la base per l'innovazione tecnologica seguente. Dunque è profonda convinzione delle persone che ci lavorano, che tutto questo che appare fantascienza, un prossimo domani diventerà realtà.

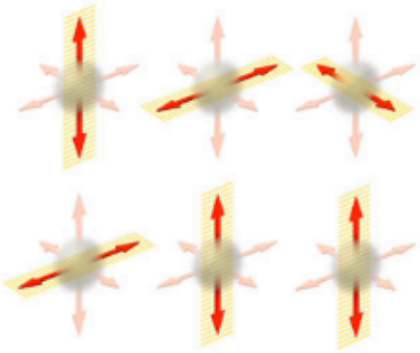
STEP 1: The bank inserts 100 quantum particles into a bank note. Each particle has various quantum attributes, including a polarization that can be measured along any of three axes.



STEP 2: A serial number is generated for the bill, and that number is linked to the polarization settings for the 100 particles.

STEP 3: To check a bill, the bank looks up its serial number in a database and gets a listing of which polarization measurement to perform for each particle.

STEP 4: The bank measures one direction of polarization for each of the 100 particles but leaves the other polarization directions unmeasured and therefore undisturbed. A counterfeiter trying to copy the bill would have to measure all the directions for each particle, which is impossible under the laws of quantum physics.



STEP 5: If the polarization measurements match the settings recorded in the database, the bank declares the bill valid.