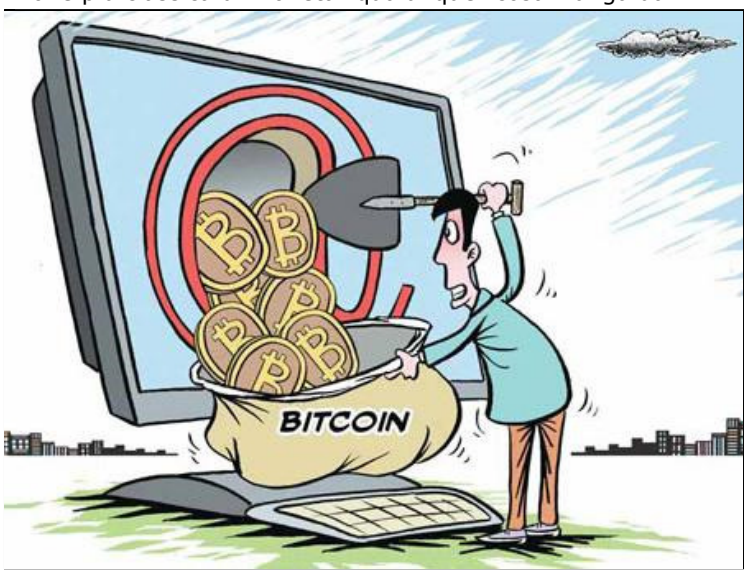
18 gennaio 2014 **Giovani**

Bitcoin: moneta o giocattolo?

Altroconsumo Finanza – 8 gennaio 2014

Cresce l'interesse e il successo della nuova moneta virtuale. Non è un gadget hi tech, ma una cosa seria, te ne diciamo pregi e limiti. (Analisi al 2/12/2013)

Che cos'è il bitcoin?
Il *bitcoin* è una moneta. E lo è secondo la definizione più classica di moneta: qualunque "cosa" funga da mezzo di pagamento e di conseguenza sia utilizzabile come unità di conto e riserva di valore. Infatti il *bitcoin* è sempre più utilizzato per gli scambi di beni ed esiste un fiorente mercato dove i *bitcoin* possono essere convertiti in altre valute (il prezzo era 1.210 dollari per un *bitcoin* venerdì sera, ma lunedì mattina era già sceso intorno ai 1.080).



Nella pratica, come funziona?
Innanzitutto devi avere un computer o uno *smartphone android* connessi a internet su cui scarichi il *client* (un programmino) che costituisce il tuo portafoglio virtuale, detto *wallet* (la terminologia è inglese), nel quale mettere i tuoi *bitcoin*.
A questo *wallet* è associato uno (o più, dipende da quanti te ne crei) *bitcoin address*, ossia il tuo indirizzo *bitcoin* (è paragonabile a un indirizzo e-mail personale) che sarà indissolubilmente collegato ai *bitcoin* in tuo possesso, al punto che se non te lo annoti e lo perdi (è una stringa di 34 caratteri alfanumerici, ci sta anche su un *post-it*) perdi per sempre i tuoi *bitcoin*. Ed è un fatto interessante perché mostra come *bitcoin* e euro cartacei funzionino allo stessa maniera.
Perdere il *bitcoin address* equivale a bruciare una banconota: come la banconota bruciata non può essere recuperata, i *bitcoin* collegati all'indirizzo che hai perso van persi per sempre.
Una volta che hai il tuo *wallet* sei pronto per comprare *bitcoin* con euro (veri) o "generarne"di nuovi. Sì, proprio generarne, ma non stiamo parlando di un asino che "produce" oro con quel che mangia come in un Paese del Bengodi.
La generazione di *bitcoin* (detta *mining*, in analogia con le miniere d'oro) avviene poco per volta ed è la ricompensa per il fatto che offri parte delle capacità computazionali del tuo computer alla rete che genera i *bitcoin*. Ogni *bitcoin* è infatti generato solo attraverso calcoli molto complessi che possono essere eseguiti da un gruppo esteso di computer connessi tra loro.
Non generi quindi *bitcoin* per magia, ma offrendo ore di lavoro del tuo computer e pagando tutta l'elettricità che consuma.
Anche qui c'è analogia con le monete d'oro fisiche, ed è il fatto che per generare *bitcoin* occorre energia, tempo e fatica, proprio come scavare in miniera. Beh, forse un po' meno. L'acquisto dei *bitcoin*, invece, lo fai via internet, tramite siti che fanno da mercato e lo fai, ovviamente, in euro.

Sono sicuri i bitcoin?
Qui occorrerebbe entrare in dettagli tecnici e parlare di crittografia asimmetrica. Senza arrivare a tanto si può dire che i *bitcoin* sono concepiti in modo che una persona non possa spendere due volte lo stesso *bitcoin* (e qui c'è una analogia con la moneta di carta). Questo è garantito dal fatto che ogni singolo

Crittografia asimmetrica
E' un modo per trasmettere dati via internet e tenerli segreti ed è un modo per firmare qualche cosa e dimostrare che la propria firma è autentica.
Caso uno, invio di dati segreti da me a te. Il principio è quello di un lucchetto e di una chiave. Tu mi spedisci il lucchetto aperto di cui hai la chiave. Io chiudo il messaggio col lucchetto e te lo rispedisco. Solo tu puoi aprirlo con la tua chiave. Il lucchetto aperto è detto in crittografia chiave pubblica perché puoi spedirlo a chiunque voglia mandarti un messaggio segreto. La chiave del lucchetto è detta chiave privata perché solo tu lo detieni, non va in giro e non c'è rischio che qualcuno se ne impossessi. Mentre se qualcuno intercetta il lucchetto, amen, perché non se ne fa nulla.
Caso due, firma autentica. Si fa più o meno il contrario, invece di usare la chiave pubblica per secretare il messaggio e quella privata per leggerlo, si usa la chiave privata per rendere segreta la firma e quella pubblica per "leggere" questa firma. Visto che la chiave pubblica che mi hai dato è in grado di "leggere" esclusivamente le

bitcoin riporta tutti i proprietari passati (come una banconota su cui hai scritto il tuo nome) e che le informazioni su ogni singolo *bitcoin* sono verificate e condivise in tutta la rete dei "partecipanti al gioco". Quindi pubbliche.

> firme fatte con la tua chiave privata è chiaro allora che solo tu puoi esserne il mittente.

Manipolare i *bitcoin* sarebbe quindi come convincere con l'ipnosi tutti i testimoni oculari del concerto dei Pink Floyd a Venezia del 1989 che gli autori di *The Wall* non si sono mai esibiti nella laguna: puoi anche riuscire a ipnotizzarne alcuni, ma non tutti.

Un rischio più serio viene da un progresso tecnologico (come dai computer quantistici) tale da rendere insicure le crittografie attuali. Ma non sembra un problema che si porrà a breve.

Una critica ai *bitcoin* è che dietro di essi non c'è nessuno Stato che gli dà forza legale. Il che significa che potrebbero smettere di essere una "moneta" qualora dovesse si smettesse di considerarla come tale.

Perché piacciono tanto?

La formula che genera i *bitcoin* è programmata in modo tale che il tetto massimo di *bitcoin* generati sia di 21 milioni (attualmente se n'è prodotta circa la metà). In assenza di nuove coniazioni il *bitcoin* è quindi una moneta che non dovrebbe subire inflazione, anzi, dovrebbe rivalutarsi nel tempo (deflazione). Questa è una delle principali attrattive per i *bitcoin* in questo periodo in cui le Banche centrali stampano soldi a pieno ritmo e fanno temere a molti che ci sarà presto inflazione.

Il problema è che, come abbiamo visto, i *bitcoin* possono venire persi, per cui una volta raggiunto il tetto dei 21 milioni non solo non cresceranno più, ma potranno anzi divenire meno, accentuando la deflazione. Storicamente la deflazione non è mai stata un buon fenomeno, ma visto che il *bitcoin* è solo una moneta tra tante siamo in un campo inesplorato. In secondo luogo piace perché è slegata dalle Banche centrali e dagli Stati e in un momento di polemiche sul *signoraggio* (la "tassa" imposta implicitamente da chi batte moneta) e di sfiducia verso i governi questo ha un certo *appeal*. In terzo luogo il *bitcoin* è una moneta che garantisce transazioni anonime.

Questo piace molto, non da ultimo a chi gestisce traffici illegali.

Che ci faccio coi bitcoin?

Per ora coi *bitcoin* ci fai degli acquisti con chi li accetta come moneta, ma soprattutto li puoi usare per speculare. Un *bitcoin* a settembre valeva meno di 140 dollari, ora ne vale 1.080.

Attento: è evidente che si tratta di un mercato estremamente ballerino, capace di grandi scivoloni e grosse impennate. La scorsa primavera si era arrampicato a quasi 240 dollari e poi è piombato in breve sotto gli 80. Ora cresce, ma il percorso è tutt'altro che semplice.

E' molto remota la possibilità che tu ripeta il miracolo di quello studente norvegese che ci aveva investito 19 dollari quattro anni fa nell'ambito di una ricerca universitaria e che dopo quattro anni ci si è comprato una casa.

Nel breve periodo il rischio di farti male coi *bitcoin* è molto, molto alto. Nel lungo periodo c'è qualche probabilità in più che si rivelino una scommessa con cui fare soldi.

Ma attenzione: i *bitcoin* sono stati premiati anche perché sono una innovazione tecnologica importante come lo furono i primi motori di ricerca internet. Ma non è detto che il primo attore di un nuovo mercato (quello della moneta virtuale) sia quello che poi vincerà la competizione.

A metà anni '90 avevamo *Lycos, Virgilio, Arianna, Altavista*, poi è arrivato *Google* e oggi praticamente si usa quasi solo quello. In soldoni il rischio è che il successo di *bitcoin* sia oscurato da quello di qualche altra moneta fatta meglio.