

Bitcoin: la rivoluzione della decentralizzazione

Come la moneta digitale volontaria porterà un'ondata di
innovazione dirompente

4 dicembre 2014
aggiornato il 24 febbraio 2016

*Da qui al 2005, diverrà chiaro che
l'impatto di Internet sull'economia non
sarà stato più grande di quello del fax.¹*

1998 — Paul R. Krugman
Premio Nobel per l'economia 2008

La rivoluzione dal basso

È POSSIBILE CHE DALLE IDEE DI UN PERFETTO SCONOSCIUTO parta un fenomeno nuovo che in pochi anni vada a perturbare le agende di Governi e Istituzioni Finanziarie a livello globale?

Sì, se lo sconosciuto è *Satoshi Nakamoto* e il fenomeno si chiama *Bitcoin*.

Il termine “rivoluzione” è spesso usato in contesti inappropriati, per il marketing *un prodotto è rivoluzionario*, per un partito politico una proposta di legge è rivoluzionaria, per i tecno-entusiasti *un telefonino può essere rivoluzionario*. Ma se togliamo il termine da questi contesti dove può suonare esagerato quando non ridicolo, immagineremo probabilmente sommosse popolari, sangue e violenza. Per il *Wikizionario* (anni fa avremmo citato il *Devoto-Oli*) la “rivoluzione” è un “improvviso *cambiamento di idee*, condizioni sociali, economiche, culturali, politiche in forte contrapposizione a quelle precedenti”².

L'energia elettrica è stata rivoluzionaria, il motore a scoppio lo è stato, il computer sicuramente. Ma questi furono cambiamenti accettati come *rivoluzionari solo dai posteri*; quando l'innovazione arrivò nel sistema per la prima volta l'atteggiamento fu molto diverso. Per fare un esempio: i primi proprietari di auto in Inghilterra dovevano per legge avere a bordo un pilota, un ingegnere e una persona con una bandierina con

¹<http://web.archive.org/web/19980610100009/www.redherring.com/mag/issue55/economics.html>

²Enfasi dell'autore: <http://it.wiktionary.org/wiki/rivoluzione>

il compito di precedere il mezzo di trasporto e fare largo tra carri e pedoni³. I primi automobilisti erano dunque visti come degli eccentrici, dei pazzi che rischiavano la vita con macchinari puzzolenti che procedevano a passo d'uomo e che non avevano proprie strade dove essere usati.

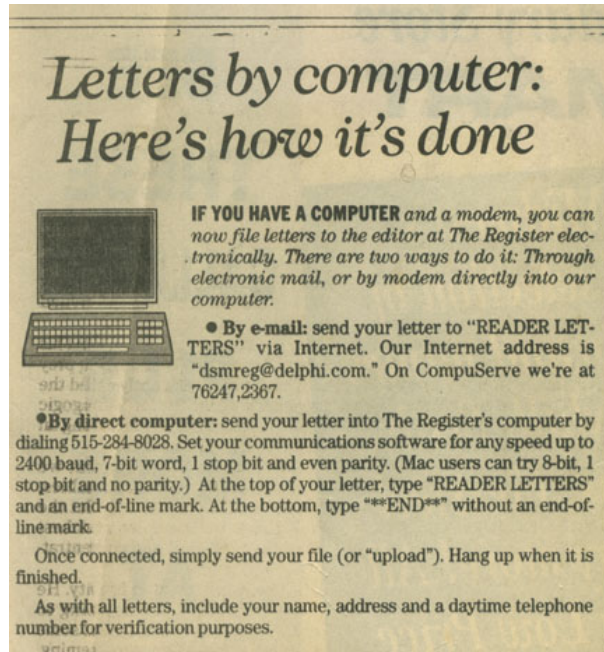
Per citare tempi più recenti, quanto poteva sembrare assurda l'idea stessa dell'email ad un comune cittadino italiano nei primi anni '90? Serviva un computer da circa 2 milioni di lire, un modem quasi altrettanto costoso ed una connessione ad Internet, magari presso un provider che avrebbe richiesto una carissima telefonata interurbana per connettersi; peggio ancora, anche il nostro destinatario avrebbe dovuto avere una configurazione compatibile con la nostra.

La rivoluzione, mentre accade, non è quasi mai vissuta dai contemporanei per quello che è, c'è sempre una forza, di abitudine, di stasi, di mancanza di fantasia, che si oppone al cambiamento.

Siamo ora in una fase di questo tipo, dove è da poco arrivato uno strumento di innovazione dirompente che fa leva su una tecnologia rivoluzionaria: il Bitcoin⁴; ma andiamo con ordine.

La nascita del Bitcoin

IL 31 OTTOBRE DEL 2008 veniva postato⁵, su una mailing list di crittografia, un pdf che sta cambiando permanentemente il paradigma monetario e finanziario nel quale siamo immersi da più di un secolo. Una parte del paradigma riguarda la presunta necessità che la moneta sia gestita o debba essere di proprietà di un autorità superiore, sia essa lo Stato, il Sovrano o una Banca Centrale; questo ora non sarà più necessario, ma alla più conveniente, prima di divenire obsoleto.



Interfacce amichevoli - User friendliness.

³https://en.wikipedia.org/wiki/Locomotive_Acts

⁴<https://bitcoin.org/it/>

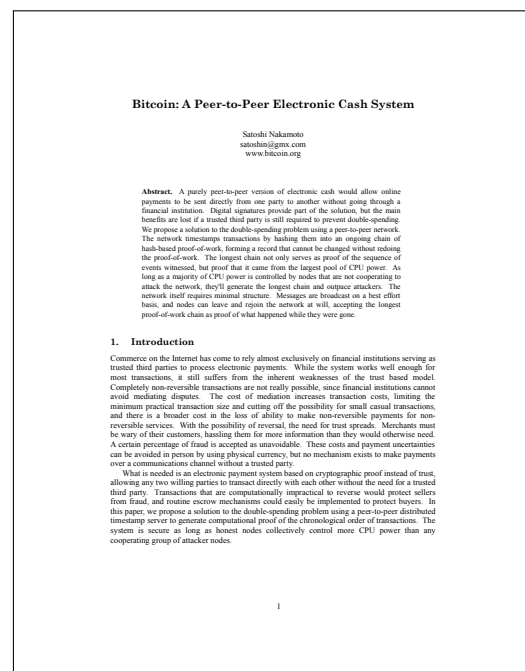
⁵<http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>

Il pdf si intitolava “*Bitcoin: A Peer-to-Peer Electronic Cash System*”⁶ e definiva il funzionamento di una moneta digitale, decentralizzata, non controllata da un ente ed emessa in base ad un algoritmo.

L'accettazione tra i crittografi che seguivano la mailing list non fu unanime, anzi, l'incredulità era forse il sentimento più diffuso. Del resto non possiamo biasimarli, è facile la prima volta che si legge di Bitcoin pensare solamente che sia un'idea curiosa, divertente, *un giochino intellettuale per nerd* e poco altro. Il problema d'accettazione del Bitcoin deriva dal fatto che non solo veniva introdotto un concetto al quale non siamo abituati, cioè una l'idea di *una moneta non a corso legale ma ad uso volontario*, ma anche dalla ragione che per farlo, Satoshi aveva creato un sistema informatico che non aveva precedenti: la tecnologia del *registro delle transazioni distribuito* permetteva funzionalità mai state prima disponibili in informatica e la moneta digitale era solo una prima applicazione di tale tecnologia.

Monete digitali erano esistite anche prima, c'era stato l'*e-gold*⁷, i *beenz*⁸, i *liberty dollars*⁹, tutti progetti centralizzati che erano in diversi modi naufragati o fatti naufragare, perché *avevano un unico punto di vulnerabilità (single point of failure)* ed erano facilmente attaccabili o delicati. Satoshi probabilmente pensò alla differenza tra Napster¹⁰, altra tecnologia dirompente, e Bittorrent¹¹; il primo, centralizzato era stato chiuso da una banale operazione dell'FBI, mentre Bittorrent, decentralizzato, si era già dimostrato non solo inarrestabile, ma anche *antifragile*. Il termine *antifragile*, significa che più una cosa viene attaccata e più diventa resistente; è una proprietà che il bitcoin ha di progetto.¹²

Tenendo chiari gli *svantaggi di corruzione e fallibilità*, la *centralizzazione* ha anche alcuni vantaggi rispetto alla *decentralizzazione*. La decentralizzazione è spesso più complessa e meno efficiente: una monarchia assoluta è tecnicamente un sistema più semplice di una democrazia.



L'articolo originale, il Satoshi's paper.

⁶Originale: <https://bitcoin.org/bitcoin.pdf>, e traduzione in italiano: <https://docs.google.com/file/d/0B1UsG65HCLkuMjA3Mzk2ZTUyYjQ4Ni00MjE5LTgzN2ItMjI3ODU0M2Y4MGUx/edit>

⁷<http://en.wikipedia.org/wiki/E-gold>

⁸<http://en.wikipedia.org/wiki/Beenz.com>

⁹http://en.wikipedia.org/wiki/Liberty_Dollar

¹⁰<http://it.wikipedia.org/wiki/Napster>

¹¹<http://it.wikipedia.org/wiki/BitTorrent>

¹²<http://bitcoin.stackexchange.com/questions/11867/is-bitcoin-antifragile>

Nel caso di una moneta digitale, una *terza parte autorevole* permette di evitare la spesa multipla di uno specifico oggetto digitale (es. un ammontare di bitcoin) tenendo un solo registro, un solo *libro mastro delle transazioni* su un sistema informatico centrale, a costi minori di un sistema decentrato. Ma la complessità del sistema fiduciario necessario per regolare l'accesso a questa unica risorsa di controllo, può essere molto costosa da mantenere ed eclissare anche i pochi vantaggi di efficienza potenziale.

Essendo nel mondo digitale, poco costoso effettuare *copie perfette*, come si può evitare di copiare perfettamente del denaro digitale senza fare uso di un'autorità centrale che permetta di evitare una spesa multipla (*double spend problem*)?

Satoshi si appropriò di strumenti informatici preesistenti e li assemblò in maniera innovativa: usò la *crittografia*¹³ per firmare digitalmente le transazioni, da Bittorrent prese l'idea e la tecnologia per ottenere il *libro mastro distribuito* come se fosse un file di un film in condivisione e infine, da un progetto pensato per ridurre lo spam nell'email¹⁴, prese l'idea di associare una quantità di lavoro crittografico¹⁵, cioè energia elettrica trasformata in calcoli, e di usare questo lavoro come se fosse un voto in una democrazia (da una testa uguale un voto ad un calcolatore uguale un voto) per stabilire il consenso in una rete di computer.¹⁶ Per l'uso massiccio di strumenti crittografici le valute come il Bitcoin vengono ora generalmente chiamate *crittovalute* (*crypto-currencies*) o anche *monete matematiche*.

La crescita esponenziale

DIFFICILE RIUSCIRE AD IMMAGINARE il futuro in prospettiva, molto più facile è fare una retrospettiva. Che cosa è successo in questo ultimo anno al progetto Bitcoin?

In questa tabella si vedono alcuni parametri relativi all'ultimo anno (2013); i negozi online e fisici che accettano Bitcoin sono esplosi, i *bancomat bitcoin* (BTM, 6 in Italia, con altri in arrivo) erano un fenomeno sconosciuto, l'*Hash Rate* globale, che è una misura della sicurezza della rete, è aumentato di 216 volte. La crescita dei progetti *Github*¹⁷ significa che gli sviluppatori software stanno lavorando sempre più per produrre strati tecnologici, servizi e nuovi modi di usare la tecnologia Bitcoin per usi impensabili (qualcuno lo citerò più avanti).

Quanto costa un bitcoin

Il bitcoin è un bene scarso, ce ne sono in circolazione 13 milioni circa e al massimo nel 2140 ce ne saranno 21 milioni, non uno di più. Un bitcoin, ad oggi sul finire del 2014, è

¹³ECDSA, firma crittografica a curva ellittica di tipo secp256k1, http://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

¹⁴Hashcash, <http://en.wikipedia.org/wiki/Hashcash>

¹⁵*Proof of Work*, il lavoro crittografico è una ripetizione di una funzione hash (double sha256) dello stato delle transazioni degli ultimi 10 minuti. Vedi <http://it.wikipedia.org/wiki/Proof-of-work>. Questo meccanismo è usato in un nuovo tipo di firma crittografica, la "DMMS", *Dynamic-Membership Multiparty Signature*, per la prima volta delineata nell'articolo sulla tecnologia delle *sidechains*: <http://www.blockstream.com/sidechains.pdf>

¹⁶Per spiegazioni più dettagliate su questo funzionamento, l'articolo originale di Satoshi risulta una fonte chiara e sufficientemente accessibile.

¹⁷<https://github.com/>

Key Bitcoin Adoption Metrics

	Quarterly			Last 12 Months	
	Sep-14	Jun-14	Q/Q Δ	Sep-13	Δ
Commerce					
Wallets	6,559,978	5,427,688	21%	1,353,201	5x
Merchants	76,000	63,000	21%	10,000	8x
Merchants' annual revenue (\$bn)	86	29	196%	0	N/A
ATMs	251	103	144%	0	N/A
Unique bitcoin addresses	184,554	136,152	36%	61,734	3x
Industry					
All-time VC investment (\$m)	317.0*	225.3	41%	30.4	10x
Number of VC-backed startups	66*	50	32%	14	5x
Media					
Mainstream media mentions	9,398	9,024	4%	1,794	5x
Technology					
Network Hash Rate (billion/second)	261,900,382	111,194,683	136%	1,213,246	216x
Github no. of updated repositories	18,753	15,109	24%	1,573	12x
Valuation					
Bitcoin market capitalization (\$bn)	5.2	8.3	-37%	1.5	3x

*Includes recent Q4 deals (eg Blockchain \$30.5m).

Sources: CoinDesk, [Blockchain.info](#), [BitcoinPulse](#), [Github](#), [Coin ATM Radar](#). Figures used are as of end of quarter.

State of Bitcoin Q3 2014

CoinDesk

6

Report trimestrale Q3 2014 – redatto da <http://www.coindesk.com>

scambiato per circa 300 €, ma se ne possono possedere anche delle frazioni, essendo divisibile in 100 000 000 unità (chiamate come il creatore, “satoshi”)¹⁸.

Il prezzo del bitcoin è dato unicamente dal Mercato, seguendo le leggi della domanda e dell’offerta. Esistono diversi cambiavalute, che siano essi attrezzature simil-bancomat, persone fisiche o servizi online (*exchange*), che permettono di vendere e comprare bitcoin per valuta a corso forzoso come euro o dollari (chiamate tecnicamente *fiat currencies*). In questa fase iniziale lo scambio del bitcoin per valuta fiat comporta che il prezzo sia molto volatile¹⁹, ma è una peculiarità che è destinata naturalmente a diminuire mentre l’adozione continua. Pensate che il primo scambio, ormai famoso, tra un bene e bitcoin è avvenuto nel 2010, dove una persona scambiò 10 000 bitcoin per due pizze²⁰ a domicilio, fissando impropriamente una quotazione del bitcoin a circa 0.002 € (supponendo 20 € per due pizze); quella stessa quantità ora vale circa 3 milioni di euro.²¹

Com’è potuto crescere il prezzo di più del 100 000% in qualche anno?

Il perché questo avvenga è semplice, perché il bitcoin è utile, ma scarso.

Non se ne possono stampare di più, la loro creazione dipende solo dall’algoritmo e viene generata in maniera predicibile e distribuita da chi partecipa con risorse di calcolo alla

¹⁸Ultimamente la community di bitcoiners sta spingendo per utilizzare un sottomultiplo del bitcoin, cioè il “bit” che equivale a un milionesimo di bitcoin, o in altri termini 100 *satoshi*, in modo da avere solo 2 decimali invece di 8, come capita per le monete tradizionali a corso forzoso alle quali siamo abituati; l’idea del cambiare il riferimento di base nasce dalla constatazione che dovremmo trovare più facile pagare un caffè 3000 bits piuttosto che 0.003 bitcoin.

¹⁹La volatilità è la proprietà di un bene di essere soggetto a variazioni percentualmente significanti del prezzo nell’arco del tempo; il bitcoin può ancora esprimere variazioni dell’ordine del 10% nell’arco di una giornata.

²⁰<https://bitcointalk.org/index.php?topic=137.0>

²¹<https://duckduckgo.com/?q=10000+bitcoin+euro>



10 000 bitcoin, le pizze più costose della storia.

sicurezza della rete (chi fa questo usa computer specializzati che vengono chiamati “miner”²²). Va da sé che più si diffonde il fenomeno (sia tra gli utenti, che come tecnologia) e più ne aumenta il prezzo, perché, a fronte di un’emissione in costante declino, una domanda statica o in crescita porta ad un aumento del prezzo di ciascun bitcoin. Ma gli aspetti speculativi sono marginali rispetto all’utilità sia del Bitcoin come valuta che della tecnologia sottostante.

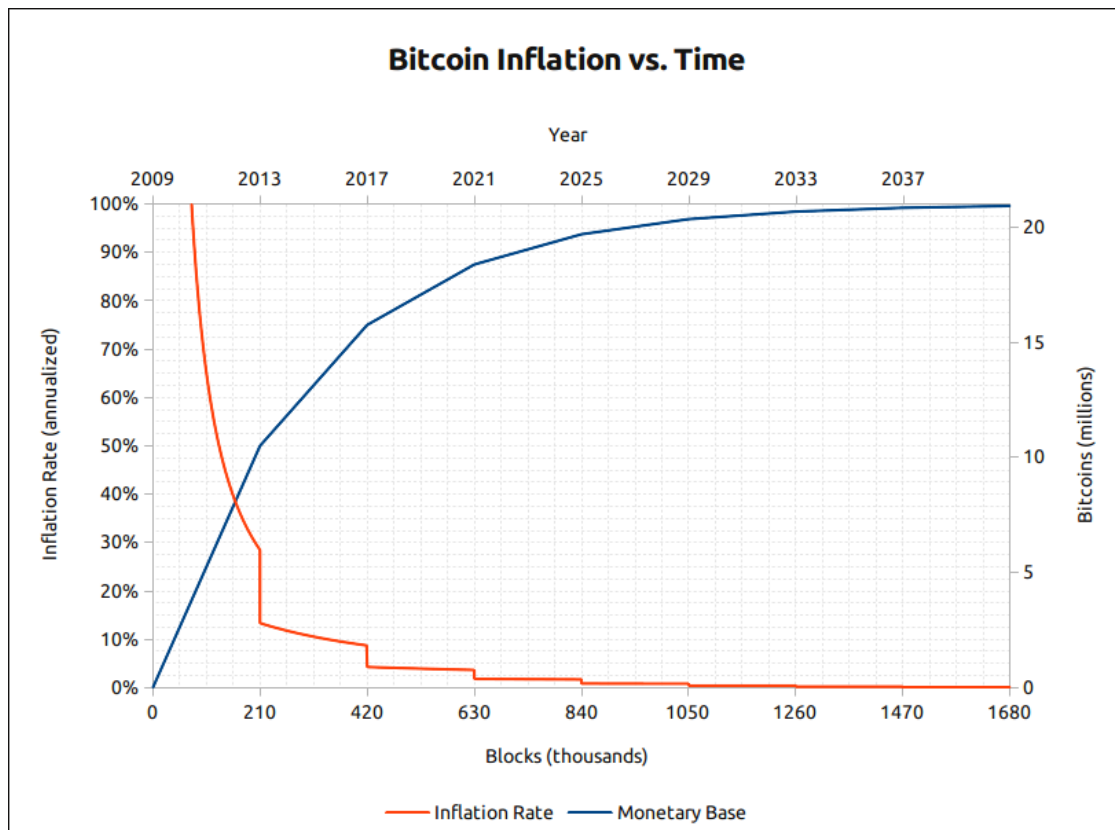
Il Bitcoin come valuta

PER CAPIRE CHE COSA È il Bitcoin come strumento per trasmettere valore, senza addentrarci in tecnicismi complicati (chi di voi mentre legge queste righe sa esattamente come funziona il protocollo TCP/IP o il linguaggio di markup HTML che rende il web possibile?) usiamo una metafora presa in prestito proprio da Satoshi:

Immaginate un metallo simile all’oro quanto a scarsità di presenza sulla superficie terrestre²³ e quanto a difficoltà di estrazione. Immaginatelo però di un colore grigiastro per nulla attraente, né duttile né malleabile, privo di funzioni ornamentali o costruttive, che non sia né un buon conduttore elettrico, ma nemmeno un buon isolante, brutto a vedersi al posto di un dente (va be’ che già l’oro...NDA), insomma, del tutto inutile.

²²Nel 2012 si poteva fare *mining* anche con un PC tradizionale, ma il fenomeno è stato così profittevole da far sì che venisse sviluppata una tecnologia specifica per il *mining*. Ora per *minare* servono delle attrezzature ottimizzate basate non su processori generici da PC e nemmeno GPU delle schede video, ma su degli ASIC – Application Specific Integrated Circuit – dei processori che eseguono solo la funzione necessaria al *mining* di bitcoin.

²³170 000 tonnellate estratte sin dagli albori dell’umanità.



Creazione di nuova moneta nel tempo, chiamata inflazione monetaria (non dei prezzi al consumo).

Però con una magica proprietà, cioè che può essere trasmesso attraverso un canale di comunicazione.²⁴

Capirete che un metallo del genere potrebbe avere un ruolo notevole per la trasmissione a distanza di potere d'acquisto.

Del resto che cos'è una moneta?

SECONDO LA DEFINIZIONE DI ARISTOTELE, la moneta doveva essere un bene *non deperibile*, *scarso* (cioè disponibile in *quantità limitata*), *facilmente divisibile* e con *valore intrinseco*. Secondo definizioni moderne è moneta ciò che può essere usato come mezzo di *trasmissione del valore*, come *unità di conto* e come *riserva di valore*.

Secondo entrambe queste definizioni il nostro euro non è proprio una moneta esemplare, perché riguardo la prima definizione manca di *valore intrinseco* o *valore d'uso*, cioè non ha altra utilità se non quella di scambio, mentre rispetto alla seconda definizione come riserva di potere d'acquisto, sul lungo periodo non si comporta molto bene, basti pensare a quanto si poteva acquistare 30 anni fa con 100 000 lire e paragonarle al potere d'acquisto degli attuali 50 €. La mancanza di valore d'uso della moneta *fiat* non è un problema fondamentale, visto che in realtà il valore d'uso non serve a molto se non

²⁴Libera traduzione da: <https://bitcointalk.org/index.php?topic=583.msg11405#msg11405>

come avvio del fenomeno, pensiamo per esempio all'oro o alle conchiglie, monete del passato, che avevano anche usi ornamentali che ne stimolavano la domanda iniziale.

Il bitcoin è una *moneta volontaria*. Chiunque può scambiarla e accettarla senza chiedere il permesso o a nessuno (*permissionless*). Le transazioni sono *permanenti, irreversibili* e con tariffe bassissime o nulle, in generale si parla di 0.3 centesimi di euro a transazione (che sia essa di un euro o di un milione di euro).

Per poter accettare bitcoin è sufficiente crearsi un indirizzo bitcoin all'interno di una delle tante applicazioni software gratuite disponibili online²⁵, chiamate *wallet* o *portafogli*²⁶; detto indirizzo, un numero di 256 cifre binarie quasi sempre rappresentato da una strana sequenza di numeri o lettere (es. 1FBKmA3gFzuT28MpA4EfuqQ5kJEFS9ows) svolge la funzione del tradizionale conto corrente bancario, senza tuttavia che siate costretti ad aprirne uno presso alcuna banca. Con Bitcoin infatti si può diventare banche di noi stessi.

Il Bitcoin (con la "B" maiuscola) indica invece il protocollo, il codice Open Source che permette di implementarlo e la rete peer-to-peer dove vengono trasmesse le transazioni.

Bitcoin è questione di libertà. Le transazioni possono essere *anonime* a piacere o *trasparenti a piacere*, dato che il libro mastro delle transazioni, chiamato *Blockchain*, è pubblico e chiunque può vedere tutte le transazioni avvenute dal primo blocco iniziale, il *Genesis Block*,²⁷ ad oggi. Le transazioni avvengono tra *pseudonimi*, cioè gli indirizzi bitcoin, da quello del mittente a quello del destinatario,²⁸ se però, ad esempio, rendessi pubblico sul mio blog personale il mio indirizzo bitcoin, permettendo di associarlo alla mia persona, ecco che dall'anonimato scaturirebbe una funzionalità inaspettata e dirompente: la *trasparenza*.

Il valore della trasparenza

PENSATE AD UN PARTITO POLITICO che pubblicasse il suo indirizzo bitcoin per le donazioni da privati o per il ricevimento di soldi pubblici. Potrebbe farsi vanto di avere realizzato una forma di *trasparenza finanziaria totale*. Chiunque, giornalisti e cittadini, avrebbero modo di vedere dove fluiscono i soldi e come vengono spesi. Idem per la pubblica amministrazione.

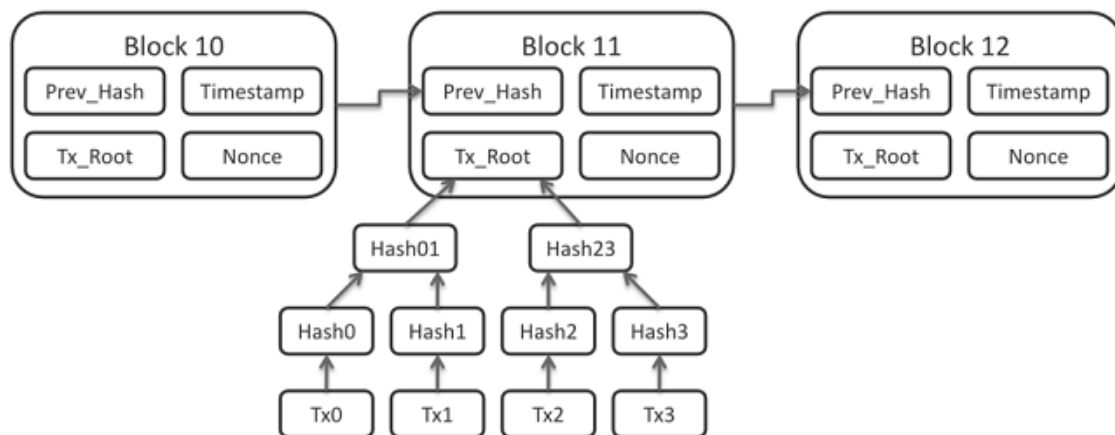
Oppure pensiamo al privato, dove un produttore di cibo biologico mostrasse che i suoi bitcoin arrivano, veramente e ad ogni nostro acquisto, ai fornitori di materia prima biologica *certificando in automatico la sua filiera* ad un livello oggi impensabile.

²⁵Un esempio di *wallet online*, non web, sicuro e versatile è <https://electrum.org/>

²⁶Sarebbe più corretto chiamarle *portachiavi*, visto che memorizzano e gestiscono delle *chiavi private*, ma gli ingegneri non sono sempre a loro agio con le metafore.

²⁷<https://blockchain.info/it/tx/4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b>

²⁸Questo per semplificare il concetto, nella pratica che si sta diffondendo (standard BIP0032 sugli *hd-wallet*), si usano indirizzi nuovi ad ogni transazione e si mette al sicuro solo una *masterkey*, che può generare tutti gli indirizzi dei quali potremmo aver bisogno in alcune vite. Questa degli indirizzi bitcoin è una parte che il pubblico vedrà sempre meno, analogamente a quello accaduto per gli indirizzi internet con l'introduzione del DNS.



Un diagramma che rappresenta concettualmente la Blockchain.

Parliamo di una moneta potenzialmente *autotracciante*, che si *autodocumenta* in maniera pubblica. Si noti come questa funzionalità, tra qualche tempo, potrebbe impensierire i commercialisti, il cui ruolo ad oggi è quello di fornire dei servizi che il Bitcoin implementa automaticamente.

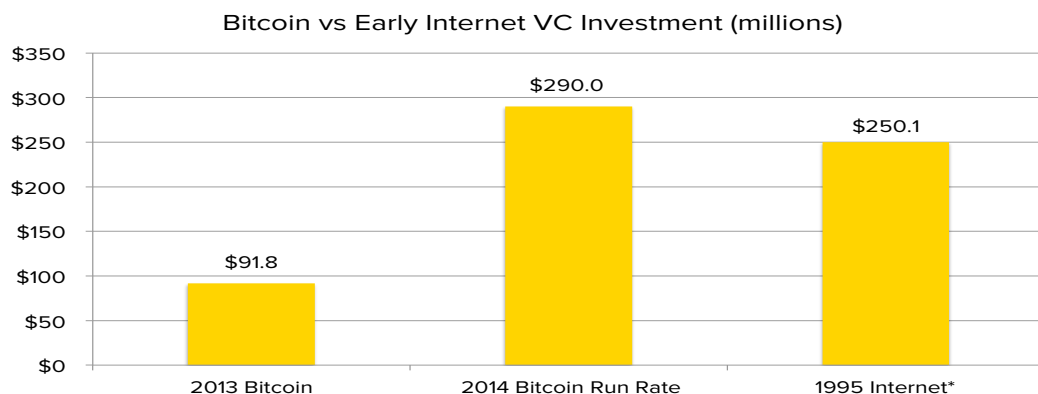
Ovviamente pensando ad una valuta globale, oltre alla trasparenza, la *pseudonimità* è un grande valore negli scambi *tra privati*. Non possiamo supporre che i governi o le istituzioni siano sempre benevole, ci sono parti del mondo dove questo non è vero e la possibilità di effettuare scambi in maniera anonima potrebbe proteggerci da aggressioni o ritorsioni. Questo è possibile dato che *l'associazione* tra indirizzo Bitcoin ed individuo è *solo volontaria*.

Attualmente *i commercianti* che accettano bitcoin sono in *forte aumento*, questo anche perché sono già mature sul mercato soluzioni che azzerano il problema della fluttuazioni dei valori di cambio rendendolo molto appetibile. Un negozio, con solo uno smartphone, un tablet o semplicemente un QRcode adesivo di un indirizzo bitcoin, può accettare questa moneta direttamente e senza rischi. Ci sono aziende, come inbitcoin²⁹, che dato un prezzo in euro, permettono ai commercianti di accettare pagamenti in bitcoin continuando però a ricevere euro sul conto in banca, mascherando completamente al mercante la volatilità momentanea del bitcoin e a 0% di tariffe, rendendo per un negoziante il Bitcoin un sistema di pagamento molto più vantaggioso di bancomat o carte di credito, che hanno tariffe non trascurabili.

Limitatamente a questo ambito, i *vantaggi immediati per il consumatore*, oltre alle partecipazioni ai *minori costi* dei negozianti sotto forma di promozioni, sono il *non dover fornire a terzi dati sensibili non necessari*, evitando di dover “tremare” ogni volta che si sente la notizia di dati personali o numeri di carte di credito, trafugati da qualche sistema informatico centralizzato (ancora dei *punti di vulnerabilità* dei sistemi tradizionali).

²⁹<https://inbitcoin.it>, nota bene, è l'azienda del quale l'autore è founder.

2014 Bitcoin VC Investment Projected to Surpass Early-Stage Internet Investments



*Includes first sequence venture deals but excludes late-stage 1995 internet investments (\$257.6m). For additional disclosure on methodology see <http://www.coindesk.com/following-money-trends-bitcoin-venture-capital-investment/>

Source: CoinDesk, PricewaterhouseCoopers

State of Bitcoin Q3 2014

CoinDesk

32

Investimenti in aziende nascenti, o Startup, legate al Bitcoin

Bitcoin è globale

IN EUROPA, soprattutto nel Regno Unito, in Germania e in Olanda, il Bitcoin è un fenomeno generalmente più noto che in Italia, dove spesso purtroppo si è in ritardo sulle nuove tecnologie rispetto ai nostri cugini d'oltralpe. Questo dicembre a Monaco, si terrà un evento per la creazione della prima banca che fornirà servizi integrati sulle *cryptovalute* come il Bitcoin³⁰ e la Svizzera già da giugno ha fatto progressi per attirare innovazione, facendo chiarezza sulle interpretazioni tributarie, suggerendo di trattare i bitcoin come valuta estera.³¹

Oltre allo scenario commerciale europeo, o alla febbre Bitcoin dei *capitalisti di ventura* (vc) statunitensi che investono sulle nuove imprese Bitcoin cifre paragonabili a quelle investite nei primi anni di Internet, ricordiamoci che il Bitcoin è un fenomeno globale, non riguarda solo l'Italia o il benestante "occidente" ma anche il 50% della popolazione mondiale che non ha accesso al credito e agli strumenti bancari.

I Filippini cominciano ad usarlo per il mercato miliardario delle rimesse dei migranti, dove le commissioni sono in ordine dell'8% medio (e praticamente il bitcoin le azzerà); si stima che la maggior parte del PIL filippino derivi appunto dai soldi che i lavoratori emigrati mandano alle loro famiglie in patria.

In Kenya, paese africano in forte crescita, già il 40% del PIL è scambiato via SMS con Mpesa, usando telefonini "non smart" per noi ormai obsoleti. Mpesa è un'azienda monopolista che applica pesanti tariffe agli scambi e attua atteggiamenti anticompetitivi.

³⁰<https://www.cryptocurrency-bank.com/>

³¹<http://www.coindesk.com/swiss-report-lays-foundation-bitcoin-become-legal-money/>

Su quel mercato sta già muovendo i primi passi Bitpesa³², un interfaccia bitcoin a Mpesa per le rimesse dei migranti.

Ci sono state valute *iperinflazionate*³³ e ci sono valute a rischio nel mondo, dove il passaggio al bitcoin permetterebbe alla popolazione libera di effettuare scambi di merci e servizi in maniera più efficace (in Bangladesh la paura che la gente fugga nel bitcoin ha fatto sì che il bitcoin sia stato proibito per legge³⁴).

Oltre la valuta – Tecnologia Abilitante

AL DI LÀ DELLA VALUTA IN SENSO STRETTO, è la *Blockchain* la vera invenzione geniale di Satoshi. Oltre a tener conto in maniera *Trustless*, cioè *senza necessità di riporre la fiducia in alcuna autorità centrale*, delle transazioni bitcoin, è possibile associare dei dati ad una transazione nella Blockchain. Ora già alcuni di voi avranno intuito che se si possono scrivere dati in una struttura aperta, pubblica e crittograficamente protetta come la Blockchain, si sta facendo qualcosa di nuovo.³⁵

Certo, si possono scrivere dei dati nel *cloud*,³⁶ o su un sito web, ma questi dati non sono inalterabili e non ne è garantita la permanenza. Può incendiarsi un data center o rompersi l'attrezzatura nonostante le ridondanze prudenziali, ma quello che purtroppo può accadere è che *il gestore del cloud*, nel quale dobbiamo *necessariamente riporre fiducia*, può, per volontà o disattenzione, rovinare o cancellare i miei dati. Nella Blockchain questo non può accadere, non serve riporre fiducia in qualcuno, è *Trustless*.

Per la prima volta nell'informatica è stato creato un *Database Permanente e Inalterabile*.

Che cosa ci possiamo fare? *Decentralizzare* servizi che erano prima centralizzati o trasformare in *Trustless* una funzione *Trusted*.

Facciamo un esempio semplice, www.proofofexistence.com, permette di inserire la firma digitale di un documento qualsiasi nella blockchain per pochi centesimi di euro (5 millibitcoin).

A che cosa può servire? Beh, per avere una *prova matematica* di essere stati *in possesso di un certo documento* in una certa data, funzione questa fino ad oggi svolta da un notaio. Grazie alla Blockchain è svolta senza notaio e ad un costo in paragone risibile.

Bitcoin è *programmabile*. Possiamo usarlo per creare degli *Smart Contract*, cioè dei contratti "elettronici" nei quali una parte *non può essere disonesta*: questo significa che non serviranno le funzioni giuristizionali atte a garantire l'adempimento del contratto (es. la funzione della polizia per far rispettare il contratto o del tribunale per sanzionare comportamenti scorretti).

³²<https://www.bitpesa.co/>

³³Una valuta che dimezza il suo potere d'acquisto nell'arco di un mese si dice sia in *iperinflazione*, è accaduto di recente in Zimbabwe: http://it.wikipedia.org/wiki/Iperinflazione_nello_Zimbabwe.

³⁴È stato già individuato un nome a questo fenomeno, *Iperbitcoinizzazione*, una sorta di *iperinflazione* coadiuvata dal bitcoin: <http://nakamotoinstitute.org/mempool/hyperbitcoinization/>

³⁵Un buon video a questo riguardo lo si trova su <http://youtu.be/YIVAluSL9SU>

³⁶http://it.wikipedia.org/wiki/Cloud_computing



Un ascensore a monetine non programmabili del secolo scorso.

Per fare un esempio di *Smart Contract*, si può pensare alla gestione di fondi aziendali tramite un portafoglio bitcoin a *multifirma*³⁷, dove un socio da solo può spenderne al massimo l'1% al mese, 2 soci potrebbero spenderne il 20% e dove serve che ci siano tutte le firme dei soci per spenderne il 100%.

Possiamo immaginare proprietà digitali applicate ad oggetti fisici (*Smart Property*), per esempio un'automobile che si accende solo se la transazione Bitcoin di passaggio di proprietà è presente sulla Blockchain.

Oppure possiamo anche immaginare distributori automatici che gestiscano direttamente il denaro in ingresso e facciano gli acquisti per rifornirsi dei prodotti in esaurimento con parte dei bitcoin incassati, continuando a *funzionare in autonomia* senza dipendere direttamente dall'azienda che li gestisce. Una macchina o un *software* non possono *aprire un conto* corrente tradizionale non essendo persone fisiche o giuridiche, ma possono scambiare bitcoin e comportarsi da agenti razionali in un mercato globale.

Gli *Smart contract* sulla *Blockchain* sono un componente ideale per qualsiasi tipo di *sistema elettorale* che voglia essere *non manipolabile* da nessuno, pur mantenendo la caratteristica indispensabile di garantire il voto segreto all'elettore. A Stalin hanno attribuito la frase: "la gente che vota non decide nulla, sono quelli che contano i voti a decidere tutto", fortunatamente ora c'è una soluzione tecnologica che può mettere a tacere per sempre le accuse mediatiche di brogli elettorali che avvengono spesso dopo le elezioni.³⁸

³⁷<http://bitcoin.stackexchange.com/questions/3718/what-are-multi-signature-transactions>

³⁸<http://motherboard.vice.com/read/bitcoin-could-change-voting-the-way-its-changed-money>

Per citare altre cose che bollono in pentola, IBM vuole basare “Adept”, il cuore del suo progetto per *Internet of Things*,³⁹ sulla Blockchain e sui protocolli Bitcoin e Bittorrent⁴⁰.

Uno sguardo al futuro

QUESTE APPLICAZIONI sopra elencate sono già possibili con la tecnologia attuale. Che cosa ci riserverà invece il futuro?

Probabilmente una vasta schiera di *crypto-currencies* tutte scambiabili con quella per eccellenza, il bitcoin, che saranno progettate per scopi specifici, anche complessi. Sto parlando di quelle che vengono attualmente chiamate *Appcoin*, come le attuali *Namecoin* che permette di decentralizzare un protocollo internet come il DNS o *Ethereum* che punta a divenire una piattaforma per gli *smart contract*.

Come *divertissement* conclusivo immaginiamo qualcosa ancora più in là nel futuro e proviamo ad intuire che, magari tra una ventina d’anni, le *smart-automobili*⁴¹ che guidano senza pilota *saranno le sole auto a poter circolare legalmente* nel traffico e immaginiamo di essere a bordo di una di queste e di avere fretta: bene, l’auto potrà pagare degli *Speedcoin* alle altre automobili attorno disposte ad accettarli per lasciarci passare, con il risultato che i viaggiatori con meno urgenza incasseranno da quelli frettolosi. Sì, saranno le auto stesse che pagheranno, non il passeggero, avranno la loro riserva digitale di diverse *Appcoin* per le varie funzioni, intercambiabili in bitcoin e si pagheranno anche la benzina e la manutenzione da sé. Se hai poca fretta ti sposterai gratis, altrimenti l’auto guadagnerà su di te che dovrai a suon di bitcoin sonanti, aumentare la riserva di *Speedcoin* della tua auto.

C’è già chi ha teorizzato⁴² che avverrà una *Singularità Commerciale*, una specie di punto critico di un sistema, quando il volume di denaro scambiato dalle “cose” (macchine o agenti software che siano) raggiungerà il volume dei commerci tra umani.

Le reali possibilità sono ancora al di là della nostra immaginazione, difficile immaginare cosa verrà; sempre che non si sia quel genere di persone che se fossero vissute negli anni ’60 sarebbero state in grado di immaginare, guardando armadi rumorosi pieni di lucine che un giorno qualcuno avrebbe giocato ad un gioco di guerra, contro un giocatore coreano, muovendo le dita su di un vetro sotto il quale appaiono delle immagini in movimento, ma senza che attori abbiano recitato la parte di quel film e senza che qualcuno abbia dipinto i fotogrammi.

Buona rivoluzione a tutti. E se non pensate di potervi *giocare un ruolo attivo*, preparatevi almeno i popcorn e *godetevi lo spettacolo*.

Marco Amadori <amadori@inbitcoin.it>

Imprenditore Bitcoin, già Tecnologo e Ricercatore presso la Fondazione Bruno Kessler (<https://fbk.eu>).

³⁹http://it.wikipedia.org/wiki/Internet_delle_cose

⁴⁰<http://goo.gl/AXvA88>

⁴¹http://it.wikipedia.org/wiki/Google_driverless_car

⁴²<http://www.slideshare.net/winklevooscap/money-is-broken-its-future-is-not>

da un'idea di divulgazione della scienza, per il Blog di [ByoBlu](#). un ringraziamento agli amici e colleghi che hanno letto la bozza, nonostante non avessi inviato loro nessun *caviacoin*.

Questo articolo è distribuito con licenza “Creative Commons Attribution-ShareAlike 4.0 International Public License”, descritta all URL <http://creativecommons.org/licenses/by-sa/4.0/deed.it>. I sorgenti \LaTeX sono disponibili su: https://github.com/mammadori/bitcoin_divulgation/tree/master/rivoluzione_decentrata.

Aggiornamento

Oggi, alle porte di Marzo 2016, sono passati 15 mesi dalla prima stesura dell'articolo ed è stato necessario intervenire, visto l'uso che è stato fatto di questo documento, come una gentile introduzione al fenomeno nella sua complessità. Ho corretto qualche paragrafo per renderlo più scorrevole, ho aggiunto dei link in riferimento ad alcuni passaggi e ho cambiato la mia mail di riferimento, visto che ho seguito il mio stesso consiglio finale decidendo di fare la metamorfosi da Ricercatore ad Imprenditore del settore. Qui di seguito un piccolo aggiornamento sulla tematica Blockchain, l'idea è di tenere aggiornato questo documento finché avrà senso farlo. Di seguito un adattamento di un blog post con delle riflessioni su quanto accaduto in questi mesi e su come ho cambiato *accento* sulla Blockchain.

Bitcoin e Blockchain: Una Storia Zen

*Prima che una persona studi lo Zen,
i monti sono monti e le acque sono acque;
dopo una prima occhiata alla verità dello Zen,
i monti non sono più monti e le acque non sono più
acque.*

*Dopo l'illuminazione,
i monti tornano ad essere monti e le acque ad essere
acque.*

- Detto Zen

A fine 2014 **scrivevo**⁴³ che **il Bitcoin era rivoluzionario e dirompente, ma che la vera innovazione**, tecnologica, **era “La Blockchain”**, il registro permanente, inalterabile e ad accesso aperto che traccia ogni transazione di bitcoin fin dai tempi della creazione del suo primo blocco, biblicamente chiamato Blocco della Genesi, generato (“minato”) da **Satoshi Nakamoto**, pseudonimo del suo leggendario creatore.

Non è andata malissimo, la nuova *buzzword* “Blockchain” è stata abbracciata entusiasticamente dai media: l’Economist⁴⁴ ci ha dedicato una copertina e le grosse istituzioni Bancarie e Finanziarie hanno investito e stanno investendo in ricerca, seppur timidamente, nel settore. Questo accade perché la Blockchain ha applicazioni riguardanti i costi per stabilire e mantenere la fiducia (in inglese *Trust*, ovvero *il costo per stabilire e mantenere delle relazioni personali e/o di business* per potere effettuare le transazioni) che possono essere ridotti notevolmente in questo passaggio **da sistemi trusted a sistemi trustless** (ovvero senza necessità di doversi fidare di autorità centrali di garanzia).

La Blockchain come “il nuovo Bitcoin”

Come prevedibile, negli ambienti tradizionali del settore finanziario, il sogno sembra essere principalmente una **Blockchain Privata**, questo perché alcuni livelli di **disintermediazione del “Trust”** come definito fin qui, forniti da queste tecnologie, possono fare risparmiare tempo e denaro. La mia opinione personale è che questa delle **blockchain private** sia per lo più fumo negli occhi, quasi **un ossimoro**, come “acqua asciutta” o “scienze religiose”; per avere **una vera blockchain** e non un semplice database distribuito, **serve un gettone** (*token*) che possa avere valore economico, servono degli **incentivi corretti** (*mining*) ed è necessario un **accesso aperto** alla tecnologia, serve avere **Permissionless Innovation**, cioè poter provare ad innovare direttamente su una piattaforma aperta, senza necessità di ‘chiedere il permesso’ ad una Telco (Internet) o ad un Gruppo Bancario (Bitcoin). Ma tant’è, tanti auguri ad R3⁴⁵ nel vendere alle banche il suo *snake-oil*⁴⁶.

⁴³Il riferimento è a questo documento, infatti questo aggiornamento è stato pubblicato anche in forma di blog post su www.byoblu.com con riferimento all’articolo originale di dicembre 2014.

⁴⁴<http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>

⁴⁵R3cev è una startup/consorzio di 42 banche globali e arcinote che promette loro strumenti per blockchain private.

⁴⁶I famigerati intrugli oleosi venduti nei secoli bui come elisir dalle proprietà taumaturgiche.

La Blockchain funzionava anche come ottimo dissimulatore: catalizzando su di sé tutta l'attenzione, il bitcoin come valuta – un potenziale nemico, anche se di dimensioni non ancora preoccupanti – veniva oscurato dalla tecnologia che serviva a realizzarlo. Secondo la propaganda dei fautori della Blockchain Privata (**Permissioned Blockchain**), si poteva tenere il buono che c'era nel Bitcoin, cioè tutte le Innovazioni della Blockchain, ma **senza il bitcoin come moneta**, troppo anarchica e senza (il loro) controllo.

Non mi sono del tutto sbagliato scrivendo quell'articolo in quel momento, **spostare l'interesse** che fino a quel momento i media e un po' tutti i bitcoiner avevano **per il prezzo del bitcoin**, cioè da bitcoin come asset speculativo e **puntare sull'incredibile tecnologia soggiacente**, dove si potevano trovare le gemme dagli usi concreti e di valore immediato, era necessario e urgente. **Necessario** perché dispiaceva che chi leggeva solo nella lingua di Dante non sapesse quali preziosi tesori nascondesse quello che i giornali al tempo dipingevano, quando andava bene, come uno schema Ponzi per fare arricchire nerd brufolosi. **Urgente** perché era il caso di non rimanere troppo indietro, come paese, quando le potenzialità italiane specifiche (creatività e diffusione della telefonia mobile) potevano determinare un ruolo importante in questa industria emergente.

Nel 2015 abbiamo assistito a quasi un **rebranding mediatico** (la strategia di marketing che consiste nel mutare stile, nome, design, terminologia a uno stesso prodotto per commercializzarlo meglio), simile ad un ipotetico *pivoting* per la reale "Startup Distribuita Autonoma" Bitcoin, per spostare l'attenzione da quello che sembrava ormai solo una semplice moneta digitale, anche se globale, anche se non controllabile da un singolo ente, anche se *non inflazionaria per design* **verso una tecnologia più rassicurante, più Bank-Friendly**, meno crypto e meno anarchica: La Blockchain.

Non mi sbagliavo dunque, visti i successi dell'idea, ma non vedevo correttamente quello che già era in evidenza e che lo era stato fin dall'inizio: la valuta, la moneta, la prima applicazione della Blockchain, era il luogo dove risiedeva la reale portata dirompente e rivoluzionaria di questa nuova tecnologia.

Store of Value. Bene rifugio.

La funzione più criticabile e più bistrattata da sempre del bitcoin è la sua vera **Killer Application**.

Perché sulle prime questa idea sembrava assurda?

Bitcoin: come comprenderlo al di là dei pregiudizi

A parte gli ovvi discorsi sul *bias cognitivo* e sulla paura dell'ignoto, **ci sono dei problemi reali ad affrontare intellettualmente il Bitcoin**.

Non i bitcoin rappresentino un grosso problema per chi non ne conosce la complessità sottostante: **siamo abituati ad usare diverse forme di denaro senza saperne troppo sul funzionamento**. Usiamo per esempio il contante senza sapere quanti euro ci siano in circolazione, quanti ce ne saranno tra dieci anni e in che percentuale esatta siano di carta e metallo, quanti siano fatti esclusivamente di numeri in un computer di una banca o se le banche ne presteranno più facilmente quest'anno rispetto all'anno precedente.

Così come si può guidare un'auto senza sapere la composizione chimica della miscela delle ruote, **si può comprare una birra al bar in bitcoin** premendo 'invia', **senza sapere come funziona** una Lightning Network⁴⁷.

Ma se invece vogliamo proprio capirlo, allora diventa un tantino complesso, anche se totalmente documentato e trasparente, trattandosi di informatica *Open Source*.

Se affrontassimo il Bitcoin con la lente di un economista monetario, subito ci faremmo distrarre dal fatto che **la moneta è volutamente progettata per divenire nel tempo deflattiva** ed evocheremmo subito la crisi del '29 e le persone sul baratro della rovina finanziaria grazie a debiti irripagabili. Se lo paragonassimo all'oro, peccherebbe di fisicità e storia millenaria nel suo utilizzo come bene rifugio. Se la si guardasse come un prodotto web, penseremmo che possa essere rimpiazzato, come Facebook fece con Myspace. Se la si osservasse come tecnologia potremmo pensare che verrà soppiantato da una tecnologia superiore. Se lo guardassimo come investimento lo troveremmo troppo rischioso e volatile.

Gli esperti solitamente non riescono a dipanare la matassa perché un po' tutti i modelli economici, monetari e finanziari, l'esperienza pregressa nel "settore" o la letteratura specifica, non ci aiutano molto a capire come questo curioso concetto possa funzionare o come possa non essere stato già soppiantato da un suo clone.

Il problema sta proprio nel **riuscire a vedere il fenomeno nella sua interezza**, senza osservarlo tramite modelli parziali. Certo, **la pratica val più della grammatica**: se ordinassimo un caffè pagandolo in bitcoin dal parcheggio di un bar, trovandoselo già servito con lo scontrino al nostro tavolino preferito, riusciremmo a mettere insieme i pezzi più facilmente.

La pratica dell'uso di bitcoin è infinitamente più semplice, già ora, della teoria. **Coi primi bitcoin ricevuti**, magari dallo smartphone di un amico, **si sente nel cervello un primo "click"**, con il primo acquisto in un negozio ne scatta un secondo ed i dubbi teorici svaniscono come neve al sole.

L'innovazione sconta il fatto che **non entra in nessuna categoria già conosciuta** e prevedibile e tutti gli esperti investigano il fenomeno con gli strumenti che il passato gli ha consegnato. Come quasi nessuno scrittore di fantascienza (salvo pochi e osannati 'guru') è mai riuscito a prevedere le innovazioni dirompenti che avrebbe portato il futuro (come Internet, gli Smartphone e il Bitcoin), pochissimi riescono oggi a vedere il fenomeno nel suo insieme. È come se si trovassero nella famigerata caverna di Platone e osservassero solo delle ombre, scambiandole per realtà.

Ma è più facile comprare da Amazon, godendo di uno sconto dal 15 al 50% solo per il privilegio di farlo in bitcoin (grazie a servizi come Purse.io) **che passare ore a studiare la Teoria dei Giochi**, imparare la Crittografia a Curva Ellittica o capire quando entrerà in gioco il **Lindy Effect**⁴⁸, la **legge di Thiers**⁴⁹ o di **Metcalfe**⁵⁰.

⁴⁷<https://lightning.network/lightning-network-technical-summary.pdf>

⁴⁸https://en.wikipedia.org/wiki/Lindy_effect

⁴⁹https://en.wikipedia.org/wiki/Thiers%27_law

⁵⁰https://it.wikipedia.org/wiki/Legge_di_Metcalfe

Il successore del Bitcoin è...il Bitcoin!

La demografia cambia.

Per un *millennial*⁵¹ **il fatto che alcuni di noi si rechino in banca** per prestare denaro ad un terzo, affinché questo terzo ci permetta in futuro di spenderlo (mentre il *millennial* preme solo 'invia' sul suo smartphone) è un po' come per noi vedere le file di anziani alla posta che ritirano la pensione in contanti. Sembra **una cosa inutilmente faticosa e per la quale ci sono metodi più rapidi**, grazie alla tecnologia.

In questi anni **molti hanno provato a dirottare** verso altre tecnologie, aziende o prodotti quello che mediaticamente fu **l'entusiasmo per il bitcoin**, lo *Hype* del 2013 per il quale sembravano tutti impazziti. Nel 2013 e nel 2014 molti sviluppatori/truffatori provarono a **sfruttare lo hype** per dire che la loro *Altcoin* (clone di bitcoin, come codice o funzionalità) era **"il nuovo bitcoin"**, *Ethereum* è il bitcoin del 2014, il *bitcoin 2.0* è il bitcoin del 2015, il *BitGold* è il nuovo bitcoin, la *Blockchain* è il nuovo bitcoin, e così via...

Ma **gli utenti mondiali di una qualsiasi Altcoin sono meno dei nuovi utenti entrati in bitcoin questa settimana**, una blockchain alternativa (*Altchain*) è solo un registro, un database condiviso; la realtà è che *Bitgold* è centralizzato soffre di "rischio della controparte" (c'è un'unica controparte a conferirgli valore, e se questa lo abbandona, *BitGold* non vale più niente). Tutte queste cose **mancano o del network effect di bitcoin** (in senso ampio, VC money, sviluppatori, startup) **oppure mancano di decentralizzazione**, accesso aperto alla tecnologia ed ubiquità.

Bitcoin non è un titolo che rappresenta valore, **è valore, sono grammi di oro digitale** trasmissibili su un qualsiasi canale di comunicazione, ipersicuri, non censurabili, ad innovazione aperta, inclusivi, globali.

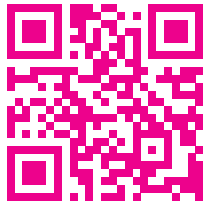
Concludendo, ringraziando gli amici revisori e Claudio Messori per aver semplificato l'accesso a questo *addendum* e abbracciando sia lo *Hype*, che lo *Zen*, vorrei veicolare questo meme⁵²:

È Bitcoin il nuovo Bitcoin.

Marco Amadori, Fondatore di inbitcoin.it e Ricercatore e Tecnologo presso Blockchainlab.

⁵¹I nati poco prima del cambio di millennio, da fine anni 80 a poco prima del 2000, nativi digitali, Internet per loro c'è sempre stata.

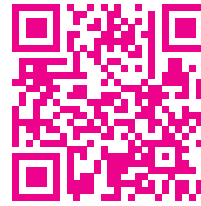
⁵²<https://it.wikipedia.org/wiki/Meme>



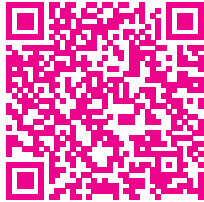
<https://bitcoin.org/it/>



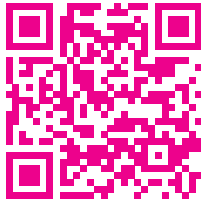
<https://bitcoin.org/bitcoin.pdf>



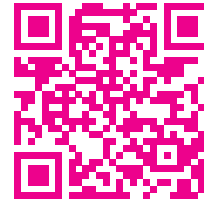
<http://youtu.be/YIVAluSL9SU>



<http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html>



<http://en.wikipedia.org/wiki/Hashcash>

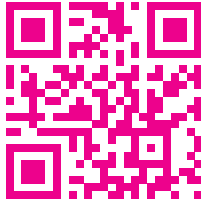


<http://it.wikipedia.org/wiki/Proof-of-work>

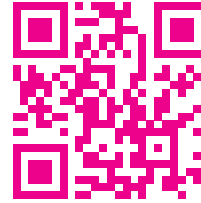
1



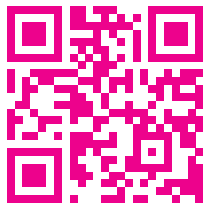
<https://bitcointalk.org/index.php?topic=583.msg11405#msg11405>



<https://inbitcoin.it/>



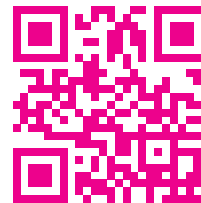
<https://electrum.org/>



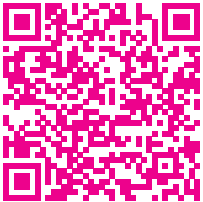
<https://www.bitpesa.co/>



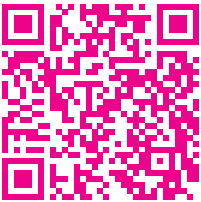
<http://motherboard.vice.com/read/bitcoin-could-change-voting-the-way-its-changed-money>



<http://goo.gl/AXvA88>



<http://www.slideshare.net/winklevosscap/money-is-broken-its-future-is-not>



http://it.wikipedia.org/wiki/Google_driverless_car



Ti è piaciuto questo articolo?
[1FBKmA3gFzuT28MpA4EfuqQ5kJEFS9owS](https://www.youtube.com/watch?v=1FBKmA3gFzuT28MpA4EfuqQ5kJEFS9owS)

Link principali, citati nell'articolo, in formato QRcode per la scansione con smartphone.