Igor Wolfango Schiaroli

DARK WEB & BITCOIN

La nuova èra della rete

Il fenomeno WikiLeaks, la nascita di Anonymous, l'associarsi dei giovani protagonisti della Primavera araba, la creazione del Bitcoin: tutto ciò non sarebbe stato possibile se non esistesse un territorio libero come il dark web.

lantana

gazometro

collana
gazometro

Reporters sans frontières, *Gaza. Il libro nero*

Stefano Grazioli, *Gazprom. Il nuovo impero*

AA.VV. (a cura di Matteo Tacconi), *Narconomics* (Disponibile in e-book)

Renzo Leonardi, *L'abc dell'energia nucleare*

Franck Frommer, *Il pensiero PowerPoint.*

Il programma che ci rende stupidi

Paola Garieri, *L'insostenibile lentezza del processo*

Alessandro De Pascale, *Telecamorra*

Serge Quadruppani, *La politica della paura* (Disponibile in e-book)

ISBN 978-88-97012-76-4

www.lantanaeditore.com

Igor Wolfango
Schiaroli

DARK WEB & BITCOIN

La nuova èra della rete


lantana

Indice

a Monica

«Nessuna cosa in sé è una sola, né correttamente si potrebbe definire alcuna cosa, né si può definire la qualità di qualcosa, ma, se tu la proclami grande, appare anche piccola, e se tu dici che è pesante, può sembrare anche leggera, e così per tutte le altre, perché niente è uno, né determinato, né di una data qualità. Dallo spostarsi, dal muoversi, dal congiungersi delle cose fra di loro, deriva tutto ciò che noi chiamiamo esistente, esprimendoci in maniera non corretta. Infatti nulla è mai, ma sempre diviene».

Platone, *Teeteto 152d-e*

PREMESSA

Il mondo del web è affascinante. La rete è uno strumento incredibile, in cui all'utilità pratica dei contenuti si associa un territorio libero dove scambiarsi idee, condurre battaglie, cambiare il pianeta. È una creatura cangiante in continua crescita e costante mutamento, e per questo quando si trattano argomenti connessi alla rete sarebbe opportuno

parlare sempre all'imperfetto perché quello che è oggi, domani potrebbe essere cambiato, evoluto, diverso. Affronteremo dunque gli argomenti per come *erano* oggi.

Cercherò di evitare discorsi troppo tecnici, per addetti ai lavori, perché mi piacerebbe che questo libro venisse letto da un pubblico vario e curioso che durante la lettura si faccia delle proprie opinioni e poi possa proseguire con nuovi strumenti nella direzione che preferisce approfondire.

La scelta degli argomenti trattati non

è stata facile perché ci si muove in un universo in costante espansione, in cui ciclicamente avviene un'esplosione visibile da tutti, cosicché occorre scegliere un punto di osservazione e raccontare solo alcuni dei tanti punti luminosi. Dando per scontato ciò che è stato tra il «Big Bang» e la nostra osservazione, ossia l'origine della rete e oggi. Così farò.

Parleremo quindi di dark web, come luogo virtuale in perpetua trasformazione, esaminandone gli aspetti principali, permettendoci qualche riflessione sugli sviluppi attuali e

concedendoci un breve approfondimento su una delle conseguenze forse meno note, ma sicuramente tra le più positive, della sua esistenza: l'organizzarsi delle rivolte per la libertà durante la cosiddetta «Primavera araba». Aprirò il discorso affrontando il nascere della nuova moneta elettronica, il bitcoin, senza la quale molte delle attività economiche nel dark web non sarebbero possibili. Una moneta che sempre più sta risalendo dalle profondità della rete alla superficie degli scambi quotidiani, grazie alla sua indipendenza da autorità bancarie centrali, alla sua

«trasparenza» e, non ultimo, alla sua non tracciabilità. Considerato il particolare momento finanziario che il mondo occidentale sta attraversando, è un fenomeno che sta attirando l'attenzione di moltissimi, dai mass media agli economisti, dagli hacker ai sociologi.

Data l'ampiezza dei temi trattati, non pretendo di esaminare in un unico testo tutti i possibili risvolti, i particolari e le dinamiche. Voglio solo fornire uno spunto per chi vuole conoscere realtà che possono sembrare lontane e inaccessibili, mentre di fatto sono ormai consolidate e

ampiamente utilizzate. Voglio parlare di realtà che sono accomunate, tra l'altro, da uno spirito di libertà e sostanziale democrazia. Voglio farlo partendo da come oggi *erano* le cose.

NOTA AL TESTO

Nelle pagine che seguono troverete spesso il termine «internet» utilizzato in modo abbastanza inusuale rispetto a quello al quale siamo tutti ormai abituati. Non mi sentirete infatti parlare «di Internet», non leggerete «del dark net», «del deep net», «del net» (neanche fosse una partita a tennis). Mi sentirete invece parlare di «la internet». È di questo che

leggerete. Internet con l'articolo femminile, internet con l'iniziale minuscola. Anche se è più difficile da dire. Perché? Perché non condivido l'atteggiamento per cui, nel nostro Paese – e chissà perché –, la rete è diventata una sorta di mito, una vera e propria divinità. Non è internet ma Internet, e se va declinata, si declina al maschile. Come Dio.

Lo scrittore Stefano Diana, nel suo *Wc net*, ha esplorato diversi processi di personificazione e deificazione (quando, ad esempio, «il mare» diviene «Mare»),

operazioni che si sono ripetute in tutto il mondo, soprattutto nelle culture più arcaiche. A proposito della internet, Diana sostiene che «da quando ci è scivolata dentro, per "la internet" non vi è stato scampo: dal nome proprio alla personificazione, e da questa alla mitizzazione, il passo è stato brevissimo, il movimento praticamente automatico. In più, grazie alle moderne tecniche di comunicazione, stavolta la migrazione *oggetto-nome-dio* non ha avuto bisogno delle solite centinaia di anni per compiersi ma di uno solamente».

Gli americani, che l'hanno inventata, scrivono «The Internet», da «net» che significa «rete». Come avremmo dovuto tradurla noi? L'interrete. Termine che non sarebbe andato a genio a nessuno, suppongo. Ed eccoci a parlare di «internet». Ma trattandosi comunque di un ammasso di router, cavi, generatori e così via (ossia di una interrete) non è corretto eliminarne l'articolo. Quindi, la internet.

Il web invece è l'abbreviazione di World Wide Web (WWW), «grande ragnatela mondiale», che rappresenta quel

servizio della internet che permette di navigare e usufruire dell'insieme vastissimo di contenuti e di ulteriori servizi collegati tra loro attraverso legami (link). In inglese «web» è neutro. A noi va bene parlare «del web». Ecco tutto.

1. BITCOIN: MONETA E LIBERTÀ

La nuova moneta

È la nuova moneta elettronica, è indipendente dalle banche, garantisce l'anonimato nelle transazioni e la sicurezza negli scambi: tutto questo ha posto il bitcoin immediatamente sotto i riflettori non solo della stampa o degli «addetti ai lavori» (dagli hacker agli

economisti), ma anche di comuni cittadini sempre più interessati a investire in questa – ancora abbastanza misteriosa – nuova forma di moneta. Molti ne sono attratti e molti altri spaventati, in molti vi vedono il «futuro» dell'economia e molti ancora ne profetizzano la fine imminente.

Avremo modo di esaminare le diverse posizioni sull'argomento, quel che è certo, però, è che l'interesse per questa moneta è grande, accresciuto anche dal fatto che il modello teorico che ne è alla base si è evoluto al punto da far diventare il bitcoin la principale moneta di scambio

nel mercato, in gran parte nero, della dark net, e sta velocemente conquistando anche la rete internet che tutti conosciamo, attirando l'attenzione di alcune società che si occupano di carte di credito virtuali, che potrebbero farlo approdare definitivamente nel mercato reale.

Senz'altro, la moneta in sé e il sistema economico che le è connesso sono in grado di rivoluzionare l'economia globale, di creare cambiamenti epocali nello scambio di beni, servizi, moneta, modificando la concezione stessa di

libero mercato. Vediamo come.

Il sistema monetario in cui viviamo è un sistema monetario *globale*, che ci permette di scambiare moneta con beni e servizi, consentendoci di acquistare ciò che desideriamo effettuando pagamenti sia sotto forma di denaro contante, sia attraverso il trasferimento elettronico tra conti bancari.

Attraverso l'uso del denaro contante l'acquisto si conclude con il trasferimento del bene «carta moneta» in cambio del bene che abbiamo scelto. Quando utilizziamo bancomat, carte di credito,

assegni o predisponiamo un bonifico bancario, la transazione si conclude con un trasferimento virtuale a fronte del bene acquistato. Si tratta, in sostanza, di un processo di «informatizzazione» del concetto di moneta, che, come vedremo, può essere fonte di interessanti sviluppi e che, di fatto, ha reso possibile la nascita di monete elettroniche, del tutto virtuali, come il bitcoin.

Un altro fattore di indiscutibile importanza che ha permesso, e anzi stimolato, il sorgere di monete elettroniche è il fatto che il potere

d'acquisto di una qualunque moneta non è legato a un valore in senso fisico ormai da parecchio tempo. Se in origine, infatti, il valore della moneta era legato al valore di un determinato bene (l'oro), sono più di quarant'anni che questo non accade più, ossia da quando si è passati dal cosiddetto sistema aureo a un sistema di cambi flessibili. La quantità di moneta che circola oggi è dunque tutt'altro che facilmente deducibile. Come avremo modo di approfondire, il bitcoin, pur essendo un bene di scambio «virtuale», paradossalmente è ben più ancorato a un

valore reale di quanto non lo siano le altre monete.

Un po' di storia

Inizialmente esisteva il concetto di «cryptomoneta». Se ne parlò (era il 1998) per la prima volta nella mailing list dei Cypherpunks, un gruppo di *cryptographers* di grande influenza nel mondo digitale, noti per aver portato avanti battaglie che hanno permesso a noi di utilizzare tecnologie spesso malviste dai sistemi di

potere (come Skype) e anche per aver condotto attacchi alle autorità governative usando la rete. Tra questi, l'inventore di bitTorrent, quello del peer to peer (p2p) Bram Cohen, Julian Assange di WikiLeaks, e un certo Satoshi Nakamoto, il futuro creatore di Bitcoin, esperto di *cryptocurrency* e moneta elettronica. Il primo a parlare di cryptomoneta non fu però lui, ma il programmatore Wei Dai[1], che per facilitare l'*e-commerce* propose, in quel lontano 1998, una sorta di valuta digitale chiamata *b-money*. Alcune caratteristiche

di questa moneta, come la non tracciabilità e l'autonomia dall'autorità centrale, sarebbero stati elementi centrali nel Bitcoin, che della cryptomoneta è una delle prime implementazioni.

Satoshi Nakamoto iniziò a lavorare al progetto nel 2007, terminandolo due anni dopo e diventando ufficialmente il padre della nuova moneta digitale, il bitcoin, nonché dell'omonimo progetto software sviluppato per il suo uso (un progetto totalmente *open source*).

Di questo padre del Bitcoin si sa ben poco: Satoshi Nakamoto è uno

pseudonimo e si presume che, chiunque egli sia, possa essere di origine giapponese[2], anche se il primo software Bitcoin rilasciato al pubblico pare non avesse una versione giapponese. Altro non si sa sull'identità di Satoshi Nakamoto. Dal suo lavoro si deduce che sia un grande esperto di crittografia, ma non ci sono messaggi scritti da lui o su di lui sulle mailing list dedicate alla crittografia: per il suo lavoro sul Bitcoin infatti ha sempre utilizzato un indirizzo di posta elettronica registrato su un mail hosting anonimo (vistomail) e un account

di webmail gratuito (gmx.com), inviando posta elettronica solo quando connesso attraverso browser che garantiscono l'anonimato. Certo è che Satoshi non fa più parte dell'attuale progetto Bitcoin dalla fine del 2010, e i messaggi più recenti indicano che è «andato per sempre».

Molti hanno ipotizzato che quella di Satoshi (nome che può significare «saggezza» o «ragione») Nakamoto sia stata un'identità creata ad arte per nascondere il vero creatore – o il gruppo di creatori – di Bitcoin. Altri lo

considerano un individuo, anonimo e leggendario, «che utilizza le sue conoscenze per ispirare chi ha un'indole hacker» oppure «come Luther Blisset, un nome multiplo sotto il quale agisce programmaticamente un nucleo di destabilizzatori del senso comune»[3].

Online si trova di tutto sul nostro Satoshi, che è vivo e vuole distruggere il sistema bancario, che è stato anche un responsabile di Napster, che è morto, che è stato ucciso... Comunque siano andate le cose, nel 2009 nasce il Bitcoin[4], costruito sul concetto che la moneta è

ogni oggetto, e ogni sorta di dato, che sia accettato come pagamento per beni e servizi in un dato Paese o contesto socio-economico, e sviluppato attorno all'idea di utilizzare la crittografia per controllare la creazione e il trasferimento di moneta, invece di appoggiarsi ad autorità centrali. A ciò fa da corollario che nessuna autorità centrale può in alcun modo manipolare il valore del bitcoin.

Anzi, essendo il bitcoin creato attraverso un sistema peer to peer, quindi con architettura distribuita, non necessita di alcun ente centrale né per esistere né

per essere utilizzato. Scopriamo come.

Il bitcoin, la moneta fatta di bit

Con il termine generale di moneta elettronica (*digital currency*) si indica un tipo di «valuta» che viene scambiata elettronicamente sia tramite internet sia, più in generale, tramite una qualsiasi rete o apparecchi come smart card e card reader. In alcuni Paesi del mondo questa è già una realtà consolidata: a Hong Kong, in Belgio, nei Paesi Bassi, ad

esempio, esiste un sistema di transazioni tramite moneta elettronica largamente utilizzato che sta pian piano affiancando la moneta «tradizionale», soprattutto nelle spese quotidiane[5]. Ma il Bitcoin ha potenzialità ancora maggiori.

I bitcoin sono dei semplici file crittografati che contengono informazioni sul loro possessore[6]. Ogni importo bitcoin è legato infatti a una coppia di codici, le cosiddette «chiavi crittografiche»: una chiave è privata, la conosce solo il proprietario, ed è quella che gli permetterà di spendere la moneta;

un'altra invece è pubblica (viene anche definita come «indirizzo Bitcoin»), e permette di ricevere moneta (vedremo poi nella pratica come questo avvenga).

A differenza di quanto vale per le altre monete, complessi algoritmi provvedono a controllare la creazione dei bitcoin, i quali vengono generati tramite un procedimento chiamato *mining* (attività che ricorda il gergo dei cercatori d'oro) dove i partecipanti, i cosiddetti miners (una sorta di «minatori» digitali) eseguono un software, gratuito, chiamato Bitcoin Miner[7]. Quando il programma Bitcoin

Miner viene lanciato su un qualsiasi computer, esegue un algoritmo e inizia il processo di generazione di calcoli atti alla coniazione della moneta. L'algoritmo di creazione di nuova moneta bitcoin è basato su calcoli la cui velocità dipende dalla potenza dei computer che lo eseguono e dalla quantità dei bitcoin già emessi nel sistema. Con l'aumento del numero di bitcoin in circolazione, infatti, questa operazione richiede sempre più potenza di calcolo, e sempre più ne sarà richiesta, sino alla fine. Perché una fine esiste: il creatore dell'algoritmo ha

definito un limite massimo totale nel numero di bitcoin generabili, che è di circa 21 milioni.

A questo punto possiamo definire «rete Bitcoin» quella connessione formata tra tutti gli utenti (nodi) che hanno attivo il software di generazione di moneta.

La rete Bitcoin crea e distribuisce al suo interno, in maniera completamente casuale, un «blocco di monete» che deve essere «trovato» dagli utenti entro un determinato lasso di tempo, pena la sua definitiva eliminazione. La probabilità che un utente possa trovare e quindi ricevere

un blocco di monete dipende dalla potenza di calcolo che egli stesso aggiunge alla rete nella sua interezza. Approfondiremo in seguito l'attività di *mining*, quello che ci interessa capire ora è che il computer del «minatore», se vuole guadagnare monete, deve risolvere dei calcoli matematici per riuscire a trovare e ordinare in tempo questi blocchi come se fossero tessere di un puzzle. I computer di ogni nodo lavorano cercando di risolvere questi complessi problemi di calcolo e il nodo che riuscirà a trovare la soluzione in tempo riceverà come premio

un intero blocco di bitcoin[8]. Ogni blocco contiene una certa quantità di bitcoin, la *grandezza* del quale è un valore programmato che diminuisce nel tempo fino ad arrivare a zero. È in questo modo che non verranno creati nel sistema più di 21 milioni di bitcoin.

Stando all'attuale ritmo di produzione, si prevede che verrà raggiunto il traguardo di 21 milioni di bitcoin tra vent'anni, nel 2033.

Come già detto, i calcoli necessari per risolvere il blocco diventano sempre più complessi quanti più bitcoin sono stati

generati e quante più transazioni vengono eseguite dal sistema. Nelle prime settimane di vita del sistema, un gruppo di pochi computer poteva riuscire a trovare la soluzione in un'ora, mentre oggi è praticamente impossibile farlo in così poco tempo a meno di non far lavorare un vasto gruppo di supercomputer.

Il coefficiente di difficoltà computazionale aumenta col passare del tempo dunque, e gli utenti che vogliono coniare moneta, i *miners*, saranno costretti ad aumentare sempre più la potenza di

calcolo dei processori, avendo a che fare con una risorsa sempre più difficile da trovare e meno abbondante man mano che la creazione di bitcoin procede (proprio come avveniva ai tempi dell'estrazione dell'oro).

Oltre a creare nuova moneta, la cosiddetta «rete Bitcoin» memorizza costantemente tutte le operazioni di trasferimento di bitcoin.

L'intero sistema monetario Bitcoin viene gestito attraverso un database che risiede tra tutti i nodi e che memorizza tutti gli scambi monetari avvenuti

all'interno del network senza necessità di nessun tipo di regolamentazione da parte di un'autorità esterna o centrale.

I nodi della rete tengono traccia e controllano le informazioni di tutte le transazioni e svolgono la funzione di verificare la sicurezza, garantendo che il bitcoin venga speso da chi in quel momento ne è il legittimo proprietario. Il Bitcoin utilizza quindi un database distribuito tra i nodi della rete e utilizza la crittografia per evitare il cosiddetto *double-spending*, considerato in genere una delle maggiori criticità del concetto di

moneta digitale. Sappiamo infatti che quando si riproduce, ovvero si copia un file, è praticamente impossibile distinguere l'originale dalla copia, per la natura stessa in cui è costruito un file (è un insieme di bit). Si parla di *double-spending* quando si ha la possibilità di spendere un gettone digitale per due o più volte. Il problema è serio in quanto l'atto di spendere il denaro digitale non rimuove necessariamente i dati dalla proprietà del titolare originario, quindi è necessario usare dei mezzi che evitino una doppia spesa.

Di solito si usa un sistema centrale per verificare se il gettone sia stato speso, ma nel nostro caso vengono usati sistemi distribuiti per la prevenzione della doppia spesa.

Il software che permette di far funzionare il sistema, come abbiamo detto, è completamente *open source* e pertanto chiunque può condividere e verificare la consistenza del codice sorgente.

Come una qualsiasi moneta, i bitcoin permettono l'acquisto di beni e servizi, e ormai esistono anche diversi siti web

dove è possibile cambiare i propri bitcoin con dollari, euro, yen o altre valute.

I bitcoin possono essere accumulati (memorizzati) in un portafoglio elettronico nel proprio computer oppure affidati a server che offrono un servizio di custodia.

Grazie alla natura peer to peer di questo sistema monetario, è possibile creare moneta senza l'intervento – e il controllo – di una qualsiasi autorità esterna, come una banca centrale, e si possono effettuare transazioni in completo anonimato. La stabilità

economica del sistema è garantita dal coinvolgimento di ogni operatore sia nella costruzione sia nella verifica delle transazioni che regolano il funzionamento del sistema (non a caso è un sistema peer to peer, in cui tutti sono alla pari).

Il sistema monetario Bitcoin fornisce inoltre una particolare garanzia alle transazioni, dovuta a una verifica crittografica da parte dei nodi (che approfondiremo in seguito), che rende le transazioni monetarie, una volta avvenute, irreversibili.

Il sistema monetario Bitcoin

Come abbiamo detto, il sistema monetario Bitcoin è basato su comunicazioni peer to peer ed è studiato per mettere in contatto diretto le parti interessate a una transazione senza che sia necessaria la presenza di un intermediario bancario. Quindi, quando si acquista online con i bitcoin – ad esempio si paga l'abbonamento a un quotidiano elettronico, o si prenota un albergo – il pagamento avviene in maniera diretta tra l'abbonato e l'editore, tra il turista e

l'albergatore, senza la preventiva verifica da parte di una banca. In questo modo è possibile non solo restare anonimi durante la transazione, ma si elimineranno anche i costi di transazione. Come tutto questo avvenga, lo approfondiremo più avanti, quando ci saremo addentrati anche nei meandri del dark web.

Quello che ci interessa sottolineare adesso è che all'interno di questo sistema monetario è garantita sia la stabilità dei prezzi (perché l'offerta di moneta è calcolata da un algoritmo *open source*, non

da una banca) sia la regolarità delle transazioni (perché sono registrate in un database accessibile e verificabile da tutti).

Bitcoin: dove metterli, come spenderli?

Abbiamo detto che i bitcoin sono dei file crittografati: è arrivato il momento di capire come li si gestisce, e come è possibile procurarseli.

I bitcoin possono essere raccolti e gestiti attraverso un *wallet* online (un

portafoglio virtuale), oppure possono essere custoditi direttamente sul proprio computer. Per fare questo, per avere un vero e proprio conto Bitcoin, potete scaricare il software *open source*, il client Bitcoin. L'operazione è semplice, basta collegarsi al sito http://bitcoin.org/en, cliccare sull'opzione *choose your wallet* e selezionare il software: ce ne sono vari e potete sceglierli a seconda del sistema operativo che utilizzate (Windows, Mac OS, Linux, ma ne esistono anche per varie tipologie di smartphone)[9]. Una volta scaricato il file, procedete alla normale

installazione del software e apritelo. Vi apparirà una finestra introduttiva con il saldo dei vostri bitcoin e con le ultime transazioni effettuate (che all'inizio, ovviamente, sarà pari a zero)[10]. A questo punto siete a tutti gli effetti un nodo all'interno della rete peer to peer di Bitcoin (esattamente come lo è chi aderisce a reti per la condivisione di file con lo stesso genere di architettura, come Torrent).

La prima cosa da fare è proteggere il vostro *wallet* con una password[11]. A questo punto siete pronti, potete ricevere

e inviare bitcoin. Per riceverli, è indispensabile avere un indirizzo, che sarà l'indirizzo di riconoscimento per le transazioni Bitcoin (è un po' come un iban bancario). Per inviare bitcoin (quando ne avrete), basterà cliccare sul tasto *invia monete*: vi apparirà una schermata in cui scrivere l'indirizzo al quale volete inviare bitcoin e selezionare l'importo desiderato.

Ottenere e scambiare bitcoin

La diffusione del bitcoin come strumento di pagamento cresce quotidianamente. Dal gennaio 2011, giorno in cui ha iniziato a essere «spendibile», è stato utilizzato per un numero sempre crescente di transazioni, e si sono moltiplicati i siti web che ne hanno consentito l'uso per acquistare beni e servizi online. Nel tempo sono anche apparsi dei siti dove si possono cambiare i bitcoin con monete a corso legale come il dollaro e l'euro. La più grande «borsa» virtuale di Bitcoin è attualmente MtGox

(https://mtgox.com/) nel quale, previa registrazione, è possibile acquistare bitcoin e trasferirli su un proprio conto o sul proprio computer. Altri mercati attivi per la compravendita dei bitcoin sono Bitstamp (https://www.bitstamp.net/), BTCe (https://btc-e.com/) , BCchanger (http://bcchanger.com/), mentre Bitcoincharts (http://bitcoincharts.com/markets/) offre una buona panoramica sulle quotazioni del bitcoin sui vari mercati.

Anche se non siete interessati ad acquistarli (o ad acquistarli *ora*), è

comunque interessante andare a curiosare su questi siti per vedere quanto vale il bitcoin nel momento in cui tenete questo libro tra le mani, e le sue fluttuazioni.

Se invece siete interessati a procurarvi bitcoin, vedrete che il loro mercato funziona come qualunque altro: troverete offerte di bitcoin in vendita (*ask*) e offerte di acquisto (*bid*); se volete comprare bitcoin dovete dunque consultare la colonna *ask*, sotto la voce *best ask* (anche: *buy*) troverete la migliore offerta (ossia il minimo al quale qualcuno è disposto a scendere per vendervi bitcoin). Se invece

avete bitcoin da vendere, sotto la voce *best bid* (*sell*), troverete il prezzo massimo che qualcuno in quel momento è disposto a pagare per un bitcoin. Per esempio, nel momento in cui scriviamo (1 maggio 2013, ore 14,55) potremmo comprare 10 bitcoin su BTCe a 1292,50 USD (o a 1076 euro).

Esempio di quotazione del bitcoin, 1 maggio 2013 (BTCe)

Quanto vale un bitcoin

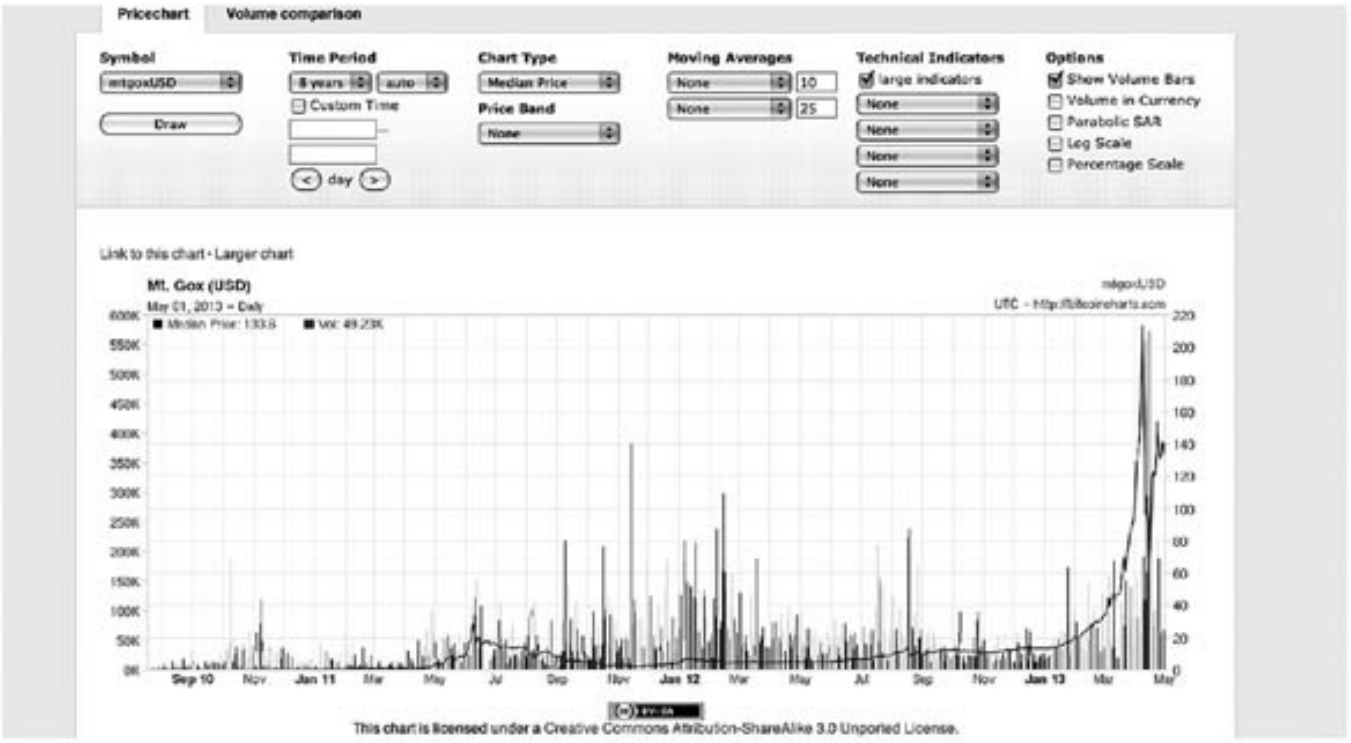
Quando è stato lanciato, un bitcoin si scambiava a 20 dollari americani, a metà del 2011 valeva 30 dollari, negli ultimi

mesi del 2011 è sceso a 2 dollari, e poi è risalito stabilendosi intorno ai 5 dollari, per risalire di nuovo. Negli ultimi anni, in ogni caso, si è sempre scambiato intorno ai 10 dollari. Nei primi mesi del 2013 ha subito un enorme balzo, prima è raddoppiato e poi è triplicato, e nell'arco di qualche settimana è arrivato a valere 240 dollari, raddoppiando il suo valore nella settimana dal 3 al 7 aprile 2013, durante la crisi di Cipro e il prelievo forzoso dai conti correnti dell'isola. Essendo Bitcoin un sistema in cui le transazioni sono completamente anonime

e non tracciabili, molte persone potrebbero aver pensato di convertire una parte del proprio capitale in bitcoin in modo da metterli al sicuro e utilizzarli come bene rifugio. Ma quando ha raggiunto il valore di 266 dollari, molti hanno venduto per incassare la differenza, ciò che, insieme a un problema dovuto a un attacco a MtGox, ne ha portato il valore, il 12 aprile, a 70 dollari.

Nel momento in cui scrivo, il valore medio del bitcoin è circa 115 dollari, potete verificarlo su diversi siti (un buon link è, ad esempio,

http://bitcoincharts.com/charts/).



Andamento del bitcoin da settembre 2010 a maggio 2013 (MtGox)

Dove spendere i bitcoin

I bitcoin sono creati da computer senza che l'uomo debba fare nessun lavoro fisico, tuttavia hanno valore per la

stessa identica ragione per cui diamo valore alle banconote che custodiamo nel nostro portafoglio. Come per ogni tipo di moneta, sono le persone che decidono se dare un valore a un oggetto o meno, e se accettare questo oggetto come mezzo di scambio. Una banconota da 100 euro non è altro che un pezzo di carta disegnato, ma diventa un mezzo con cui acquistare un bene o un servizio perché qualcun altro è disposto a prendere questo pezzo di carta in cambio di qualcosa di reale o che esprime un valore. Finora abbiamo parlato di bitcoin quasi fossero una merce

in sé, da generare o da barattare con altra moneta, ma il loro vero valore sta ovviamente nella spendibilità. Soprattutto considerando il fatto che pagando (e acquistando) in bitcoin si eliminano i costi per il trasferimento del denaro (niente più commissioni alle banche) e si può fare a meno delle carte di credito per i pagamenti in rete.

Uno dei luoghi in cui il bitcoin è più utilizzato è il dark web, ma avremo modo di parlarne in seguito: procurarsi bitcoin per spenderli nel «lato oscuro» della rete, infatti, non è esattamente la stessa cosa

che possederli per fare un investimento finanziario o per spenderli in acquisti di, mettiamo, libri. E l'argomento merita una trattazione a sé.

Nella rete di superficie, invece, esistono già molti siti in cui i bitcoin vengono accettati come moneta. Per alcuni sembra quasi un gioco: su Forbitcoin (http://forbitcoin.com/), ad esempio, si ironizza sul «Cosa fareste per un bitcoin?» («*for a bitcoin*»). Ed è tutto un proliferare di offerte di servizi in cambio di un bitcoin (o anche meno). Troverete ogni genere di proposta, dalle foto di

giovani ragazze che vi promettono l'amicizia su Facebook a improvvisati promotori musicali, da progetti di design e arredi personalizzati fino a offerte relativamente serie.

Ma le attività per le quali è più accettato il bitcoin come moneta di scambio sono la vendita e l'acquisto di oro e metalli preziosi su siti come BitAurum (https://www.bitaurum.eu/), Amagi Metals (http://www.amagimetals.com/) e BitSilver per l'argento (http://www.bitsilver.us/), l'offerta di

servizi per il web e di web hosting[12], nonché i molti servizi correlati alla rete (come servizi di email, di messaggistica, di file sharing e altro ancora). E poi, ovviamente, con i bitcoin si possono comprare dischi, libri, film, ad esempio su Bitcoinin (http://www.bitcoinin.com), abbigliamento, giochi, gadget su Bitcoin Market Place (http://bitcoinmarketplace.net/) e su Bitmit (http://www.bitmit.net/en/), e persino souvenir dalla Russia (http://rawrussia.com/souvenirs-from-russia/). Vedrete che non mancano

neanche i casinò! Il più grande attualmente è SatoshiDice (http://satoshidice.com), dedicato unicamente a scommesse effettuate con bitcoin.

E poi ristoranti, alberghi, negozi di alimentari, di elettronica, agenzie di viaggio... In molti hanno iniziato ad accettare il bitcoin come forma di pagamento. Una lista dettagliata e relativamente aggiornata la potete trovare sul wiki di Bitcoin (https://en.bitcoin.it/wiki/Trade#Curren e a questi due link:

http://www.bitcoiney.com/ e http://www.reddit.com/r/BitMarket.

Come è evidente però, lo scambio di bitcoin avviene ancora prevalentemente online, e le attività commerciali non online che accettano bitcoin sono poche e lo fanno spesso in via sperimentale (vedrete infatti che, anche se aggiornate, le liste citate vi rimanderanno spesso a realtà che magari non accettano più bitcoin). Al di là di soggettivi dubbi sull'effettivo valore di questa moneta e sulla sicurezza delle sue transazioni, uno dei maggiori ostacoli all'uso del bitcoin

nel commercio quotidiano è dato dal fatto, questo molto oggettivo, che non essendo una valuta a corso legale non può neanche essere legalmente contabilizzata...

Nonostante questo però, il bitcoin si sta rivelando ormai l'alternativa più valida per acquistare, vendere e scambiare beni al di fuori del sistema monetario convenzionale.

Procurarsi bitcoin dal vicino di casa (o quasi)

Se volete ottenere bitcoin in un modo, per così dire, più tradizionale, allora Localbitcoin è lo strumento che fa per voi (anche se di tradizionale, in effetti, ha molto poco). Il servizio vi permette infatti di comprare bitcoin in contanti direttamente dalle mani del venditore (oppure di venderli direttamente al compratore, in cambio di contante).

Il sistema è semplice. Basta registrarvi al sito e poi selezionare una delle due voci nel menu in alto, *sell bitcoins* o *buy bitcoins*, a seconda che siate interessati a vendere o a comprare. Poniamo che vogliate

comprare bitcoin: cliccando su *buy bitcoins* vi appariranno le prime offerte, ma scorrendo sulla pagina troverete lo spazio per inserire la località in cui vi trovate e la vostra offerta. Esistono anche delle opzioni ulteriori, ma già in questo modo vi sarà possibile sapere chi, vicino a voi, è interessato a vendere bitcoin. Una volta che avrete trovato un venditore vi organizzerete per il luogo e il momento dell'incontro (attraverso le coordinate di Google Maps). Quando vi troverete faccia a faccia, voi darete a lui il contante, e lui o vi verserà istantaneamente bitcoin sul

vostro portafoglio (Localbitcoin ha un *wallet* interno nel caso voi non abbiate già un vostro portafoglio) oppure potrete avvalervi del servizio di *escrow*, col quale il trasferimento di bitcoin viene verificato tramite un incrocio di messaggi sul cellulare[13].

Come abbiamo detto, dunque, è un modo abbastanza tradizionale per scambiare moneta, e alcuni utenti vi guardano con sdegno: che senso ha fare la fatica di spostarsi, andare a incontrare uno sconosciuto con in mano (talvolta parecchi) contanti, per ottenere qualcosa

che si può facilmente ottenere con un clic? La risposta è ancora una volta questa: la garanzia di non tracciabilità. Pagando bitcoin in questo modo non dovete passare per un conto bancario (anzi, non è neanche necessario che lo possediate), non dovete sperimentarvi in acquisti in borse di cui non avete esperienza, non dovete acquistare carte prepagate per poi con queste comprare bitcoin. Insomma, è più semplice, e più anonimo.

Sicurezza e privacy

Sappiamo che tutti i pagamenti elettronici sono facilmente tracciabili. È sempre possibile infatti risalire a chi ha versato e chi ha ricevuto il denaro se si utilizzano bancomat, assegni, carte di credito o quando si effettuano bonifici bancari; questo vale per tutte le forme di pagamento che abbiamo a disposizione, con la sola eccezione delle transazioni effettuate in contanti.

I pagamenti con i bitcoin, pur essendo eseguiti online, sono invece anonimi.

Restano nell'anonimato anche se per effettuare o ricevere bitcoin è necessario utilizzare un codice (la cosiddetta chiave pubblica), ma queste etichette o chiavi pubbliche si possono cambiare quante volte si vuole e non sono per forza collegate ad alcuna identità.

Sicurezza e anonimato delle transazioni sono dunque due delle caratteristiche principali di questo nuovo sistema monetario. Ma in pratica, vi starete chiedendo, come funziona?

I bitcoin sono come dei gettoni che si «trasferiscono» da un proprietario a un

altro. Quando avviene un trasferimento, dal punto di vista strettamente tecnico ogni proprietario trasferisce un bitcoin attraverso l'inserimento della propria firma digitale sull'*hash* della precedente transazione e sulla chiave pubblica del destinatario; tali informazioni vengono aggiunte in coda al bitcoin in fase di trasferimento. Chi riceve il bitcoin può verificare la transazione utilizzando la chiave pubblica del cliente per decriptare l'ultima transazione e verificare che oltre all'*hash* della transazione precedente vi sia anche la propria chiave pubblica.

In questo modo è semplice assicurarsi che la transazione sia stata correttamente eseguita, ma non si risolve il problema del *double-spending* a cui abbiamo fatto riferimento in precedenza, ossia non si ha la garanzia che quel bitcoin non sia stato già speso in precedenza. Vista la volontà di evitare i controlli centrali, si richiede allo stesso sistema di risolvere il problema, e quindi le transazioni devono necessariamente essere annunciate pubblicamente: in questo modo chi riceve il pagamento può verificare che i nodi della rete abbiano accettato la transazione

in questione (ossia che sia stato effettuato un controllo sulle ultime transazioni).

Sempre in materia di sicurezza e privacy, è utile sottolineare che il bitcoin, come il denaro contante, è totalmente anonimo, anche se questo non vuol dire che sia completamente impossibile risalire a chi l'ha speso. Si possono conoscere tutte le transazioni e gli indirizzi usati da chi ha trasferito dei bitcoin, ma non è possibile sapere con certezza a chi appartengano quegli indirizzi (se tutti a persone diverse, oppure a una singola persona, a gruppi...) Per saperlo occorre

investigare, e questo richiede molto tempo, molte risorse e in alcuni casi risulta essere un lavoro difficile se non impossibile.

La privacy viene garantita mantenendo le chiavi pubbliche in anonimato. Nel modello Bitcoin, infatti, tutti possono vedere che qualcuno sta inviando un pagamento a qualcun altro ma senza informazioni che mettano in relazione la chiave pubblica o l'indirizzo Bitcoin con l'identità di un determinato soggetto. In più, il sistema consente per ogni transazione la possibilità di

utilizzare chiavi differenti.

Per dirla in modo ancor più semplice: non si può sapere a chi appartiene esattamente un bitcoin, così come non si può sapere a chi apparteneva la carta moneta che ci viene data in resto acquistando qualcosa.

Come per ogni transazione in contanti, il bitcoin può essere utilizzato in qualsiasi attività, sia legale che illegale. Inoltre, come per il denaro contante, può essere sottratto o andare perduto (per il semplice fatto di presentarsi sotto forma di un file che può essere archiviato in un

computer o una chiavetta USB). I bitcoin si possono quindi distruggere se i file vengono perduti o se si rompono i dispositivi di archiviazione, oppure possono essere sottratti da un cyber-ladro che riesca a introdursi nel computer, allo stesso modo in cui il nostro denaro contante può essere sottratto dal portafoglio dalla mano abile di un borseggiatore. Proprio per questo sono nati molti servizi per garantire la custodia dei bitcoin e ridurne al minimo i rischi intrinsechi, quali la distruzione o il furto del file.

In ogni caso, si tratta di rischi non diversi da quelli impliciti nel conservare delle banconote sotto il materasso. Tra l'altro, lo schema Bitcoin, e quindi il protocollo che sta alla base del sistema, ha retto bene fino a ora qualsiasi attacco reale o simulato (molto più di quanto non abbiano saputo fare gli allarmi che installiamo previdentemente in casa).

Ovviamente, il fatto che chi paga in bitcoin lo possa fare in modo anonimo e senza controlli ha fatto sì che in molti l'abbiano considerato uno strumento pericoloso. Ne parleremo. Ma prima

vediamo di capire più a fondo come si generano i bitcoin, per poter fare poi le opportune considerazioni.

Mining: teoria e pratica

Per chi ha un po' di basi di informatica, una prima nota tecnica. Il *mining* consiste in una serie di operazioni computazionali il cui scopo è quello di trovare il numero che possa essere inserito correttamente all'interno dell'insieme di dati che costituiscono il

cosiddetto «*header* del blocco». Questo numero è quello giusto se il doppio *hash* SHA-256 di tali dati è un numero inferiore a un certo target (obiettivo), che viene calcolato sulla base del coefficiente di difficoltà: maggiore è la difficoltà, minore è il target. Come ogni algoritmo di *hash*, l'SHA produce un *message digest*, o «impronta del messaggio», di lunghezza fissa partendo da un messaggio di lunghezza variabile. La sicurezza di un algoritmo di *hash* risiede nel fatto che la funzione non è reversibile (non è cioè possibile risalire al messaggio originale

conoscendo solo questo dato) e che non deve essere mai possibile che si riescano a c r e a r e *intenzionalmente* due messaggi diversi con lo stesso *digest*.

In pratica, il computer che sta facendo *mining* riceve, generalmente da un server di *pool mining*, l'*header* del blocco che si sta cercando di chiudere. All'interno di questo *header* viene aggiunto un numero, il cosiddetto *nonce*, e viene calcolato l'*hash* doppio del tutto. Se tale *hash* è numericamente minore del target, l'*header* viene mandato al server per l'approvazione, altrimenti il *nonce* viene

incrementato e il controllo si ripete. Questa operazione viene effettuata diversi milioni di volte al secondo, tanti quanti sono i Mhash/sec possibili nel sistema in quel determinato periodo.

Il *mining* è un processo basato sulla pura statistica, infatti ogni tentativo di *hashing* che viene svolto ha la stessa probabilità di essere corretto, per questo motivo quando si parla di tempo o potenza necessari per chiudere un blocco si può esclusivamente parlare in termini di media.

La rete dei miners

Uno dei problemi fondamentali che i creatori del sistema Bitcoin si trovarono ad affrontare all'inizio fu quello di come emettere nuova moneta in un sistema autonomo e non centralizzato, che si distinguesse da tutti i sistemi monetari precedenti (quelli che emettono moneta attraverso degli organismi regolatori come le banche centrali).

Per creare un sistema decentralizzato e al tempo stesso credibile, fu necessario escogitare un metodo di generazione della

moneta altrettanto decentralizzato e soprattutto libero e autonomo.

La soluzione fu, come abbiamo visto, l'emissione di bitcoin a fronte di un lavoro atto alla conservazione del sistema stesso, sotto forma di premio a quelle componenti della rete che riuscivano a fornire quella potenza elaborativa necessaria a creare e a fortificare la rete stessa e in modo proporzionale alla potenza di calcolo fornita.

Inizialmente l'unico modo per produrre bitcoin era quello di «minare» utilizzando il software originale,

selezionando l'opzione *genera monete*. Questo dava al programma l'autorizzazione a utilizzare tutta la potenza di calcolo della CPU per cercare di risolvere operazioni che avrebbero potuto, casualmente, «chiudere i blocchi» e quindi generare bitcoin. Nel primo periodo di esistenza della rete Bitcoin, i partecipanti al sistema (i «minatori», i nodi) erano molto pochi, tanto che se un operatore lasciava un computer sempre attivo si potevano generare migliaia di bitcoin al giorno. Nella fase iniziale, di contro, il bitcoin non aveva alcun valore

reale o alcun tipo di liquidità, il *minig* era fatto per spirito scientifico da chi «credeva alla causa» e quindi metteva a disposizione risorse di calcolo come una sorta di donazione fatta per il bene del progetto.

Come abbiamo visto, il sistema prevede l'aumento della complessità dei calcoli che dovranno essere elaborati e risolti per creare moneta, in funzione del passare del tempo, dell'aumento della quantità di moneta generata e scambiata e della potenza di calcolo immessa nel sistema. La difficoltà di creazione è una

delle chiavi del funzionamento della rete Bitcoin. Il sistema riesce ad autoregolarsi attraverso la variazione della difficoltà del lavoro necessario a chiudere un blocco, in modo tale che in tutta la rete si possa generare una certa quantità di moneta. Per l'esattezza, il sistema è tarato per creare una media di sei nuovi blocchi ogni ora.

Col tempo, come sappiamo, il Bitcoin è divenuto un fenomeno globale, e molte persone si sono aggiunte a questo mondo, dedicandosi a creare moneta e quindi al *mining*, aggiungendo la propria potenza di

calcolo a tutta la rete. In altre parole, il successo stesso del Bitcoin ha fatto diminuire gradualmente il guadagno medio giornaliero per ogni partecipante.

Tuttavia, la diffusione del bitcoin ha consentito la nascita di una certa domanda e di un mercato, fornendogli quindi un valore tangibile. Questo ha comportato la nascita di vere e proprie organizzazioni che si dedicano al *mining*. È nato così il cosiddetto *professional mining*, persone che immettono in rete la potenza di calcolo di computer costruiti con il solo scopo di «minare» e di

rivendere il ricavato in bitcoin sul mercato. Inoltre il software è stato aggiornato con la possibilità di sfruttare più potenza di calcolo utilizzando anche il processore presente nelle schede grafiche (GPU), che è in grado di sviluppare una potenza matematica maggiore rispetto a una CPU. Questo aggiornamento di software, unitamente al sempre maggior numero di persone coinvolte nel progetto, ha causato un'impennata del livello di difficoltà e il risultato è stato che il singolo «minatore» (solo *mining*) poteva anche impiegare

settimane o addirittura mesi prima di riuscire a guadagnare dei bitcoin chiudendo un blocco. Attualmente chiunque voglia cercare di creare qualche bitcoin deve necessariamente entrare a far parte di una *minig* pool, un'associazioni di «minatori» che uniscono la propria potenza di calcolo per poi dividere tra loro i bitcoin trovati. Il *minig* viene quasi esclusivamente svolto tramite GPU e utilizzato solamente dalle *minig pools*, tanto che l'opzione *genera monete* presente nel software originale è stata rimossa a partire dalla versione 0.3.22.

Conviene «minare»?

Se si partecipa alle moltissime discussioni sull'argomento, ci si rende subito conto di come alcuni pensino che attraverso i bitcoin si possa diventare ricchi generando denaro dal nulla.

Queste convinzioni sono molto lontane dalla realtà, anche se è del tutto evidente che attraverso il *minig* si possano guadagnare bitcoin.

Generare bitcoin ha comunque un prezzo: il calcolo che viene effettuato dai computer ha dei costi, la generazione di

bitcoin attraverso il *minig* non può essere considerata gratuita.

I costi sono rappresentati principalmente dalla quantità di elettricità usata per permettere al computer di calcolare e dal costo di usura dall'hardware. Va anche tenuto conto l'impegno necessario a far funzionare tutto correttamente, e la manutenzione. La somma di queste componenti definisce il costo che dobbiamo sostenere per produrre bitcoin tramite il procedimento del *mining*. Se il risultato finale è svantaggioso, è consigliabile acquistare i

bitcoin direttamente sul mercato piuttosto che provare a generarli.

In questo momento, dato il valore del singolo bitcoin, non conviene eseguire il *minig* perché la potenza di calcolo computazionale necessaria per acquisire un blocco è molto elevata e si andrebbe a spendere più denaro per l'ammortamento del costo del computer e per l'uso dell'energia elettrica necessaria.

Costo del mining

Per vedere nella pratica quanto costi effettivamente l'attività di *mining*, proviamo ad analizzare la voce principale di spesa: la corrente elettrica.

Quel che ora andremo a calcolare è quindi la quantità di bitcoin che si genera con l'utilizzo di un kilowattora (kWh) di elettricità. Come sappiamo, ciò dipende dal tipo di hardware che utilizziamo e dal livello di difficoltà che il sistema ha raggiunto. Quest'ultimo fattore è facilmente recuperabile, dato che ci troviamo all'interno di un sistema trasparente. Il *livello di difficoltà* viene

espresso da un valore che è sempre consultabile, potete verificarlo ad esempio su questo link: http://blockexplorer.com/q/getdifficulty. Si aprirà una pagina bianca, con su scritta una lunga cifra. Due o tre giorni fa era 8974296.0148879, oggi (1 maggio 2013) 10076292.883419.

Questa cifra rappresenta l'indice di difficoltà nel risolvere i blocchi e varia nel tempo (generalmente, come per esempio in questi giorni, aumenta).

Conoscendo il valore del *coefficiente di difficoltà*, possiamo sempre sapere quanti

bitcoin per kilowattora si possono generare dato un determinato hardware, e questo calcolo può essere effettuato usando la seguente formula: BTC/kWh=41'911 MHJ/*difficulty* dove MHJ è il valore di MegaHashes/Joule, che è un valore che esprime la qualità di un certo tipo di hardware e può essere calcolato per ogni dispositivo usato per «minare». Attualmente è recuperabile sul sito wiki di Bitcoin nella sezione *Mining hardware comparison*[14].

Come per molti scenari matematici, la formula vale in un modello ideale, infatti

si esprime in un contesto in cui non esistono tasse di *pool* (ossia le commissioni che si devono lasciare alle *minig pools*: per partecipare al gruppo si lascia una percentuale a chi ha organizzato il gruppo di *mining*) e in cui si presume che il computer effettui calcoli per il 100 per cento del suo tempo-vita e senza che venga prevista alcuna inefficienza. Di fatto, la formula tiene conto esclusivamente della corrente consumata.

Come risulta evidente dalla tabella qui riportata, il *minig* è un'attività in perdita. Questa perdita sarebbe di gran lunga

maggiore se si andasse a calcolare anche l'usura e l'ammortamento degli elaboratori, visto che «minare» espone l'hardware a una probabilità di guasti e malfunzionamenti superiore a quella che si avrebbe in assenza del carico.

Al momento, generare bitcoin tramite il *minig* non è conveniente. A parità di denaro, è molto più conveniente acquistarli direttamente sul mercato piuttosto che produrli «minando».

Tipo	Descrizione	MHJ	BTC/KWh	Costo per 1 BTC	Guadagno per 1 BTC	Guadagno netto giornaliero
CPU Intel Core i5 650	Bassa potenza	0.1	0.0024	83.3 €	-79.3 €	-0.36 €
CPU Intel Core i7 950	Alta potenza	0.25	0.006	33.3 €	-29.3 €	-0.34 €
GPU NVIDIA GTX570		0.5	0.012	16.6 €	-12.6 €	-0.58 €
GPU ATI HD 4870	Ati datata	0.75	0.016	12.5 €	-8.5 €	-0.73 €
GPU ATI HD 6850	Ati recente bassa potenza	1.4	0.033	6.1 €	-2.1 €	-0.29 €
GPU ATI HD 6970	Ati recente elevata potenza	1.85	0.044	4.5 €	-0.5 €	-0.11 €

Costo del *mining* per tipo di CPU

Arricchirsi con i bitcoin

Se creare bitcoin, e quindi «minare», non è redditizio, è teoricamente possibile arricchirsi speculando sul valore dei bitcoin nel tempo.

Si stima infatti che molti dei bitcoin in circolazione siano dormienti, ovvero non vengano utilizzati da nessuno per effettuare transazioni ma siano stati acquistati o generati col solo scopo di attendere che il bitcoin prenda piede e che il suo valore progredisca considerevolmente.

Esistono numerose discussioni in rete su questo argomento, poiché sembra che i primi «minatori» siano riusciti ad accumulare delle cifre considerevoli, almeno se si tiene conto del valore attuale del bitcoin. È facile prevedere che, visto il

limite assoluto di soli 21 milioni di bitcoin, se questa moneta dovesse diventare un mezzo di scambio comune, ogni singolo bitcoin potrebbe arrivare a valere una fortuna (soprattutto se si pensa a quanta unità di moneta esiste in circolazione per esempio in dollari o in euro).

Un bitcoin è divisibile fino a otto decimali. Possono esistere massimo 2.099.999.997.690.000 (più di 2 quadrilioni) di possibili frazioni del bitcoin, così come è stato progettato. Il valore di 1 BTC rappresenta 100.000.000

di queste sotto-unità. Quindi ogni BTC è divisibile fino a 10^8, il che dovrebbe portare, in un prossimo futuro, a fare transazioni con unità più piccole come i milli-bitcoin o micro-bitcoin.

Bitcoin: una soluzione virtuale per l'economia reale

Dato che la quantità complessiva di bitcoin in circolazione è fissata da un algoritmo, alcuni hanno parlato di strette relazioni tra Bitcoin e *gold standard*, il

sistema monetario aureo nel quale la base monetaria è data da una quantità d'oro stabilita. Il *gold standard* venne abbandonato una prima volta nel 1914, durante la Prima guerra mondiale, quando tutti i Paesi entrati nel conflitto si trovarono a dover immettere denaro nelle loro economie per coprire le spese belliche. Tra il 1925 e il 1931 si ritornò a una forma di *gold standard* che dal 1947 fu riportato in vita dagli accordi di Bretton Woods, rimasti validi fino all'inizio della crisi petrolifera del 1971, anno in cui il crescente debito pubblico finì per

assottigliare le riserve auree degli Stati Uniti, portando il presidente Richard M. Nixon a decidere di smantellare il sistema. Il governo degli Stati Uniti d'America negò da quel momento la convertibilità in oro delle riserve in dollari di altri Paesi.

Iniziava l'èra, tuttora in corso, del denaro senza una base aurea, la cosiddetta *fiat money*, in cui le banche centrali regolano a loro discrezione la quantità di denaro circolante nel Paese e il suo costo attraverso il tasso di sconto. Il vantaggio del sistema *fiat money* è la flessibilità, che permette alla politica di gestire con

minore difficoltà periodi critici, come guerre o crisi petrolifere, attenuandone le conseguenze per la popolazione (quando invece vige il *gold standard* è molto più difficile la gestione sociale e impossibile combattere la disoccupazione aumentando la spesa pubblica).

Ma come abbiamo visto il sistema *fiat money* permette il verificarsi dei problemi che l'economia mondiale sta vivendo in questo ultimo periodo, ovvero la crescita considerevole della speculazione finanziaria sostenuta dall'incertezza che si ha nel calcolare gli spostamenti di

ricchezza delle diverse zone del mondo.

Il dibattito sulla questione è molto acceso: molti tra economisti e cittadini comuni credono che l'uscita dal *gold standard* abbia creato le basi per una situazione economico-finanziaria instabile che vede come conseguenza inevitabile un infinito succedersi di crisi economiche. Da quando l'oro non costituisce più la base dei sistemi monetari, e soprattutto dopo la grande crisi finanziaria dell'occidente iniziata nel 2008, i sostenitori dell'oro vedono nella sua riadozione il modo per stabilizzare il

sistema monetario. Ron Paul, uno dei leader del movimento per il restauro del *gold standard*, auspica addirittura l'abolizione della FED, la banca centrale americana, «il cui dirigismo distruttivo» è strettamente legato all'assenza del sistema autoregolatore dato dal sistema aureo.

Probabilmente la soluzione, ammesso che ce ne sia una definitiva, è più complessa: difficilmente risiede in sistemi del passato, che hanno già rivelato i propri limiti, e forse va cercata nelle innovazioni e nei cambiamenti che si profilano attualmente.

Al di là della valutazione delle diverse teorie economiche e delle opinioni sui sistemi monetari di riferimento, un sistema monetario costruito su denaro forte, internazionale e apolitico, stabilito in forma di sistema aureo o in forma di Bitcoin, potrebbe facilitare lo scambio libero e volontario tra soggetti privati e le imprese all'interno e al di là delle frontiere; un sistema che potrebbe rivelarsi stabile anche se totalmente fuori dal controllo politico.

Ci sarebbero molti vantaggi per «l'utente finale del denaro» e resterebbe

solo un piccolo ruolo per le banche.

Il bitcoin come l'oro?

Nei paragrafi precedenti abbiamo parlato di «parità aurea» e *gold standard*; vediamo adesso che tipo di analogia può esistere tra la moneta totalmente virtuale bitcoin e un metallo come l'oro, considerato bene prezioso fin dall'antichità.

Le proprietà che nel passato hanno fatto dell'oro la moneta di scambio per

eccellenza sono principalmente le seguenti:

- scarsità: di oro ce n'è poco, ed estrarne di nuovo è un'operazione molto costosa;
- durevolezza: l'oro è praticamente eterno, è un metallo nobile e uno degli elementi più stabili in natura;
- divisibilità: la capacità di potersi dividere in piccole quantità per essere impiegato come bene di scambio;
- riserva di valore: il potere di acquisto è mantenuto nel tempo.

Andando a confrontare queste qualità con quelle del Bitcoin, le somiglianze ci sembrano numerose. Riassumendo, il Bitcoin ha come caratteristiche:

- gestione peer to peer: un sistema distribuito tra tutti i nodi della rete e che non fa capo a nessun ente centrale;
- impossibilità (o estrema difficoltà) di falsificazione: la proprietà della crittografia garantisce che non sia possibile spendere una moneta per più di una volta, e quindi di truffare gli altri utilizzatori;
- scarsità: i bitcoin vengono «minati»

dagli utenti della rete, ma la capacità di trovare nuove monete decresce con il passare del tempo e con il numero di monete già scoperte. Si arriverà a un punto dove non sarà più possibile creare nuova moneta. Questo protegge tutti gli utenti dal rischio di inflazione una volta che il sistema sarà stabilizzato. (Anche se, ancora in questa fase, si sta assistendo a un processo inflazionistico a causa della speculazione di chi accumula bitcoin senza spenderli);

- facilità di scambio: i pagamenti, cioè il trasferimento di bitcoin da un utente

all'altro, avvengono in maniera diretta attraverso la rete senza la necessità di intermediari;

- facilità d'implementazione: il codice è *open source*, ed esistono numerose implementazioni gratuite in rete, un sito *e-commerce* che vuole adottare questo mezzo di pagamento può farlo senza grandi complicazioni tecniche, senza costi di licenza, e senza contratti più o meno vincolanti con gli istituti di credito che normalmente regolano le transazioni economiche;
- semplicità di custodia: è possibile

tenere «in casa» il proprio denaro senza doversi avvalere dei servizi di una banca (opzione che ovviamente rimane sempre disponibile).

L'attuale volume limitato di scambi rende il valore dei bitcoin molto volatile, ma se il suo uso continuasse ad aumentare, il suo valore si potrebbe stabilizzare notevolmente e soprattutto, analogamente a quanto avviene per l'oro, potrebbe aumentare con il tempo. Il teorico aumento di valore nel tempo andrebbe a compensare la perdita di

valore d'acquisto delle monete tradizionali dovuta all'inflazione, cioè alla continua emissione di nuova valuta sul mercato.

Dal punto di vista teorico questo sistema sembra in grado di poter cambiare l'economia monetaria mondiale sconvolgendo le attuali teorie monetariste e rendendo inutile la tecnica bancaria tradizionale.

Favorevoli e contrari

Probabilmente è ancora troppo presto per dare un giudizio definitivo sul Bitcoin. Sicuramente è un mezzo di scambio rivoluzionario e racchiude in sé profondi significati, oltre a un valore intrinseco come qualunque altra moneta.

Esso rappresenta, infatti, un vero e proprio attacco al controllo autoritario dello Stato sulle riserve monetarie: rende possibile un libero mercato, nonostante l'ostilità delle legislazioni. Governi e banche hanno espresso preoccupazione per l'indipendenza del bitcoin, e non ne siamo stupiti, scommetto.

Si tratta della prima moneta elettronica del tutto indipendente e libera, soggetta a convertibilità con altre unità attraverso il cambio di valuta, cosa da non sottovalutare.

Moneta molto «democratica» proprio perché basata sulla rete peer to peer e sull'indipendenza dai monopoli, che offre la possibilità di diversificare i metodi di pagamento.

Questa moneta elettronica è un ottimo strumento per i piccoli pagamenti. A rendere il bitcoin lo strumento ideale per il micropagamento è il fatto che

quando si tratta di piccole cifre, come per esempio una donazione, il dover passare attraverso una compagnia telefonica o una banca ha costi enormi. Con Paypal, ad esempio, su 1 euro quasi il 40 per cento andrebbe in commissione.

Il bitcoin invece è libero, spenderlo non implica alcun costo. Con i bitcoin si possono fare donazioni a WikiLeaks, per esempio, dopo che Visa, Mastercard e Bank of America gli hanno chiuso i conti[15].

Detto questo, è però necessario considerare le opinioni di tutte le persone

che affollano quei blog e forum nei quali si parla di bitcoin negativamente, come di una specie di truffa che porterà alla bancarotta chiunque vi si affiderà. In queste discussioni non mancano persino i teorici della cospirazione che finiscono anche per definire il sistema Bitcoin come uno strumento utile solo a terroristi, trafficanti di droga e, tra gli altri, a pedofili.

Gli argomenti contro il Bitcoin ricadono generalmente nelle seguenti categorie:

- Il sistema monetario Bitcoin non è

altro che uno schema Ponzi piramidale. Alcuni suoi detrattori sostengono infatti che le persone investono denaro e risorse del computer in un'impresa che non crea valore. Come in tutti gli schemi piramidali i primi investitori vengono ripagati con i soldi portati dagli investitori successivi e a un certo punto sarà impossibile trovare un altro gruppo di investitori e allora il tutto scoppierà come tante altre bolle.

- Il Bitcoin è vulnerabile alla speculazione e alle bolle di mercato. Molti sostengono che un bitcoin valga molto

meno di quanto quotato: è infatti un *asset* volatile il cui valore è in parte conseguenza della previsione di quanto esso potrà valere la settimana seguente, o l'anno dopo. Si comporta cioè come la moneta che utilizziamo già.

- Il Bitcoin non è sicuro. Mentre la crescita dei bitcoin in circolazione dovrebbe essere limitata a 21 milioni, è teoricamente possibile sovvertire questo limite se la maggioranza di quelli che forniscono potenza di calcolo al sistema *minig* acconsentono all'aumento[16].

Allo stesso modo si deve ammettere che, per quanto il protocollo Bitcoin venga garantito crittograficamente, non è comunque invulnerabile. La sicurezza del sistema è garantita dalla enorme quantità di potenza di calcolo necessaria alla falsificazione che renderebbe il tentativo, alle condizioni tecnologiche attuali, un'impresa titanica. Ma se la «ricompensa» fosse adeguata, un ente governativo, una società o persino un individuo particolarmente facoltoso, potrebbe acquistare potenza a sufficienza per attaccare la rete.

Una delle vulnerabilità, da alcuni considerata un collo di bottiglia, si può ricercare in alcuni mercati di scambio e nelle *minig pools*.

Nel giugno 2011 è stato attaccato MtGox, il più grande sito di *trading* di bitcoin, che è stato costretto a chiudere per una settimana per risolvere i problemi di sicurezza. Secondo un comunicato stampa di MtGox, un hacker ha sottratto bitcoin per un controvalore di circa 500.000 dollari dai conti di MtGox, li ha venduti tutti, e ha cercato quindi di ritirare i proventi. Il ladro era riuscito a

ottenere i privilegi di amministratore del sistema, e aveva semplicemente assegnato a sé stesso i bitcoin.

L'eccesso di bitcoin in vendita, creato dall'attacco a MtGox, ha fatto precipitare il loro prezzo da 17,50 dollari a un centesimo in meno di un'ora, causando panico e caos in tutto il mondo Bitcoin. MtGox riuscì a bloccare le vendite e a risistemare il problema. Quando riaprirono le negoziazioni, il mercato era apparentemente soddisfatto, poiché i prezzi erano tornati ai livelli precedenti l'attacco. Tuttavia, l'incidente ha messo

sotto i riflettori la falla, perché è stato dimostrato che attaccare l'ecosistema Bitcoin non richiede necessariamente la potenza dei supercomputer, si può fare con l'astuzia.

La stessa sorte può capitare alle *minig pools* e anche in questo caso dei pirati ne hanno attaccato alcune celebri con i famigerati attacchi DoS, riuscendo a bloccare la connessione dei *miners* con le loro *pools*.

Anche in questo caso, il bitcoin non si è rivelato inattaccabile.

A prova di censura

Una moneta digitale a prova di censura: così è stato definito il bitcoin dall'Electronic Frontier Foundation[17], in relazione al fatto che tutte le transazioni di bitcoin avvengono in modo anonimo e non sono dunque né tracciabili né censurabili.

Ed è proprio questo uno degli aspetti più discussi del sistema monetario Bitcoin. Da una parte c'è il dubbio sull'effettivo anonimato che lo caratterizza. Dall'altra ci si domanda, in

modo ancor più forte, se questo anonimato sia un bene o un male.

Riguardo al primo aspetto, possiamo dire questo. Sebbene a livello teorico sia impossibile collegare i titolari con il proprio codice di conto, nella pratica vengono lasciati degli indizi. È molto difficile non lasciare tracce riguardo l'identità nel momento in cui si negoziano transazioni, si inviano messaggi e si trasferiscono bitcoin in un *wallet*, e tutto questo è intercettabile attraverso l'uso di sistemi di tracciamento già utilizzati dall'FBI, dalla CIA e da altre agenzie

governative per individuare i flussi sospetti di denaro che stanno finendo nella rete Bitcoin e per risalire ai traffici illeciti che si servono dei vantaggi della struttura peer to peer.

In pratica, se in linea di massima si può parlare di anonimato per i pagamenti con bitcoin, in realtà il contante resta l'unica forma di scambio davvero anonima, perché nel mondo digitale la semplice raccolta storica di dati che resta in memoria può portare con discreto successo a un profilo univoco se la ricerca è condotta da esperti. Questo vale per i

bitcoin come per tutti quegli *anonymous data* che immettiamo in continuazione nella rete.

Per quanto riguarda il secondo aspetto, l'anonimato ha aspetti positivi e aspetti negativi. Ovviamente, potrebbe facilitare operazioni illegali, come la vendita di materiale contraffatto o, appunto, illegale; di contro, però, abbiamo degli aspetti positivi di grande portata: i cittadini onesti e rispettosi delle leggi possono portare avanti i loro affari senza che nessuno li debba necessariamente controllare. Si può

donare denaro a organizzazioni politicamente scomode, si può aggirare la censura di un regime violento e oppressivo e comprare libri o altri beni vietati in un Paese ma del tutto leciti nel resto del mondo. Inoltre, in Paesi con una forma di tassazione molto alta, o in cui il prelievo e l'uso dei contanti è sempre più ristretto, o dove il movimento limitato di capitali è tenuto sotto controllo, l'alternativa di un circuito monetario anonimo e gestibile da qualunque parte del mondo potrebbe allettare non solo i trafficanti e i grandi investitori, ma anche

i comuni e onesti cittadini.

Bitcoin deflazionista

Paul Krugman, editorialista ed economista premio Nobel, ha sostenuto nel suo blog sul «New York Times» che «quello che vogliamo da un sistema monetario non è di rendere ricche le persone che detengono denaro, ma che esso faciliti le transazioni e renda l'economia ricca nel suo insieme. E non è affatto quello che sta accadendo con

Bitcoin».

Krugman, ai tempi della bolla, ha sostenuto che il crescente valore in dollari dei bitcoin aveva fatto cadere il valore dei beni così prezzati; l'economia Bitcoin ha subito, in effetti, una massiccia deflazione.

La deflazione del sistema Bitcoin potrebbe essere considerata da un diverso punto di vista, e del resto gli argomenti di Krugman potrebbero applicarsi a qualsiasi tipo di moneta o titolo che vive con le tradizionali spinte inflazionistiche.

La nuova moneta anche in questo aspetto si comporta come l'oro,

continuando nell'analogia che abbiamo richiamato più volte nei paragrafi precedenti: è deflazionistica, costosa ed esiste in quantità limitata. Il bitcoin è progettato per rivalutarsi di continuo (il che spiega la deflazione), anche se i bitcoin potranno essere di taglio sempre minore. La quantità di bitcoin disponibili quindi diminuirà, mentre si potrà ottenere capitale solo a prezzi più alti. Se l'offerta di moneta cartacea aumenta costantemente, l'offerta di bitcoin è limitata, dunque il suo valore, in linea teorica, è destinato a salire nel tempo.

D'altra parte, però, questo sta portando gli utenti a fare incetta di bitcoin, depositandoli anziché spendendoli (bitcoin silenti), con la speranza che aumentino di valore, facendo diventare il bitcoin, di fatto, oggetto della speculazione e intralciandone il ruolo principale: facilitare gli scambi e il commercio.

Nell'ottobre del 2012 la Banca Centrale Europea ha redatto un documento che analizza la nascita e la diffusione delle monete virtuali in cui vengono presentati come *case studies* il

lindendollar e il bitcoin (tra i due, il bitcoin è definito come la moneta più controversa e allo stesso tempo di maggior successo, con elementi di innovazione tali da essere molto più simile a una moneta convenzionale che a una virtuale)[18]. Uno degli aspetti più interessanti del documento – e che ha generato un considerevole dibattito tra gli economisti – è stato la considerazione della BCE che fa esplicitamente risalire le «radici teoriche» del bitcoin alla scuola austriaca di economia. In particolare, il documento cita «le critiche della scuola

austriaca sia al sistema monetario attuale, sia agli interventi istituzionali da parte di governi e altre agenzie che – secondo la scuola – non fanno che produrre inasprimenti del ciclo economico e inflazione sempre più elevata».

In effetti furono proprio alcuni esponenti della scuola austriaca ad accogliere con favore la nascita del bitcoin, collegandola al celebre pamphlet di Friedrich Hayek del 1976, *La denazionalizzazione della moneta*, in cui si proponeva di dare ai privati la possibilità di emettere moneta fiduciaria (*fiat*), anche

senza un legame intrinseco con delle *commodities* come l'oro (ossia senza che fosse necessaria la presenza di un bene, di una merce, il cui valore intrinseco garantisse valore al corrispettivo in moneta). Ciò che andava combattuto, secondo Hayek, era il potere delle banche centrali, che attraverso l'emissione monetaria e il credito manipolano i tassi di interesse e l'inflazione e provocano di conseguenza l'alterazione dei prezzi, causando inevitabili bolle finanziarie. «Ecco finalmente la nuova *moneta austriaca*!», acclamarono in molti. E invece

vennero presto altri a ricordare uno dei capisaldi del pensiero austriaco, come Ludwig von Mises[19], teorizzatore del cosiddetto «teorema della regressione». Semplificando il più possibile, si può dire che Mises abbia dimostrato come ogni moneta venga accettata non perché imposta dal governo né per mera «convenzione sociale», ma solo perché essa è in qualche modo rappresentata da un bene che ne determina il valore. Il bitcoin, invece, nasce e si propone unicamente come mezzo di scambio: ma non ha avuto alcun uso come merce, non

ha nessun valore intrinseco.

Come abbiamo visto, in molti tendono ad acquistare bitcoin e a tenerli sotto al materasso (o nel proprio *wallet*), e il valore della moneta oscilla vistosamente e imprevedibilmente. Ma se, e quando, il mercato si starà stabilizzato, allora potremo finalmente vedere che uso si può fare di questa moneta-non moneta che intanto sembra acquistare ogni giorno più valore.

Il bitcoin, per quel che possiamo dirne oggi, è dunque una moneta potenzialmente forte, con un'offerta

anelastica, liberista, capitalista, apolitica e internazionale, che ha valore solo nel momento in cui le persone sono disposte a utilizzarla.

Legalità

A questo punto molti potrebbero domandarsi: ma tutto ciò è legale? Le implicazioni legali in effetti sono numerose, e il più delle volte non esistono ancora normative facilmente applicabili a un fenomeno così nuovo.

Il Bitcoin non va facilmente d'accordo con la legislazione di molti Paesi, tra i quali gli Stati Uniti (ci sono leggi atte alla regolamentazione dei valori mobiliari e il monopolio del governo federale riguardo la creazione del denaro).

Il Social Science Reserch Network (SSRN), il 9 dicembre del 2011, ha pubblicato un lavoro di Reuben Grinberg della Yale Law School intitolato *Bitcoin: An Innovative Alternative Digital Currency*[20], in cui si analizzano le leggi federali in tema monetario.

Applicare le leggi esistenti al Bitcoin è

un'operazione tanto difficile quanto aleatoria. In linea con l'incertezza che ne consegue, la Electronic Frontier Foundation ha smesso di accettare donazioni in bitcoin, affermando che «non comprendono fino in fondo le complesse questioni giuridiche coinvolte nella creazione di un nuovo sistema valutario».

Come ha scritto Jason Calacanis, imprenditore e blogger, il Bitcoin è «il progetto più pericoloso che abbiamo mai visto» perché è tecnologicamente corretto, *open source* ed è destinato, come sostenuto

in una dichiarazione politica dei *technotarians*[21], a cambiare il mondo, a meno che i governi non esercitino una dura repressione.

Intanto, finché la normativa non si adegua – se mai questo accadrà – a fenomeni di monete esclusivamente digitali, l'uso del bitcoin in sé non è illegale. Certo, resta il fatto che è la moneta più utilizzata non solo per l'*e-commerce* in generale, ma anche per gli scambi di merce e attività illegali che si svolgono nel dark web, la parte oscura della rete che è giunto il momento di

iniziare ad affrontare.

1 Wei Dai è un programmatore abbastanza noto, ha creato diversi software e articoli di crittografia, ma si occupa anche di argomenti di altra natura, come il business e la meccanica quantistica.

2 Almeno è quanto viene detto nel profilo compilato dalla p2p Foundation: http://p2pfoundation.ning.com/profile/SatoshiI

3 Bitcointalk.org.

4 Quando Satoshi ha pubblicato il codice del Bitcoin ha inserito, come nota di testo nelle prime righe del programma (ossia in quelle

prime righe che sono il blocco di genesi), questa frase: «The Times 03/Jan/2009 Chancellor on brink of second bailout for banks». Oltre a fornire indirettamente la prova della prima data di rilascio del software (citando la data di un'articolo del «The Times»), fa anche riferimento alle difficoltà delle banche a causa della pratica del «*fractional reserve banking*» (riserva bancaria frazionaria).

5 Vedi, ad esempio, iDeal: www.ideal.nl

6 I bitcoin possono essere anche definiti come una catena di firme digitali, appartenenti agli utenti che hanno posseduto e successivamente speso quel gettone.

7 La sua ultima versione, 0.5.2, è disponibile dal 9 gennaio 2012 e si può scaricare all'indirizzo: http://bitcoin.org/en/download, anche se

ormai è un software poco utilizzato: come vedremo nella sezione dedicata ai *miners*, sono ormai altre le modalità per generare bitcoin, legate alle *pools* e ai software che queste fanno scaricare al *miner*.

8 Il numero di bitcoin creati per blocco era inizialmente di 50, tale quantità è programmata per diminuire nel tempo, con un dimezzamento ogni 4 anni circa, fino ad arrivare a zero, in modo che non verranno mai creati più di 21 milioni di bitcoin in totale. A partire dal 28 novembre 2012, la ricompensa è passata a 25 BTC per blocco, e così sarà per i successivi 4 anni, per poi diminuire ulteriormente.

9 Uno dei più diffusi è Bitcoin-Qt.

10 Nella parte bassa della pagina troverete una

serie di dati in continuo aggiornamento: lasciate al software il tempo di completare l'operazione, perché è la raccolta di informazioni di tutte le transazioni che sono state effettuate fino a quel momento.

11 In molti forum è consigliato anche di effettuarne una copia, sempre protetta da password, per tutelarvi nel caso di rottura del computer, smarrimento, virus, ecc.

12 Come Accelerated Global: http://acceleratedglobal.wordpress.com/

13 Per maggiori dettagli, vedi il sito di Bitcoin Italia: https://www.bitcoin-italia.org.

14 https://en.bitcoin.it/wiki/Mining_hardware_cor

15 http://www.wikileaks.org/Banking-

Blockade.html

16 Tutto ciò è molto improbabile poiché la modifica al protocollo non potrebbe in nessun caso essere fatta in segreto, anche se teoricamente i critici hanno ragione poiché la scarsità dei bitcoin non è realmente garantita.

17 È un'organizzazione internazionale no profit, con sede a San Francisco, attiva dal '90, che si occupa di tutela di diritti digitali e più in generale di libertà civili nel contesto digitale.

18 Il testo integrale del Virtual Currency Schemes è disponibile online sul sito della BCE: http://www.ecb.europa.eu/pub/pdf/other/virt

19 Economista austriaco naturalizzato statunitense, tra i più influenti della scuola austriaca, Mises dimostrò che, così come il

prezzo di ciascun bene era determinato dalla quantità disponibile e dall'intensità della domanda del consumatore per quel bene medesimo (domanda e offerta), così anche il «prezzo» o potere d'acquisto dell'unità di moneta veniva determinato dal mercato seguendo le stesse modalità. Mises diede spiegazione logica del prezzo del potere d'acquisto della moneta, ma questa, così fornita, aveva importanti implicazioni, prima fra tutte il fatto che la moneta potesse trarre origine in una sola maniera: grazie alla diretta domanda nel libero mercato come una utile e preziosa materia prima. In definitiva la scuola austriaca crede che una valuta debba innanzi tutto immagazzinare valore, e non che la moneta sia un mezzo di scambio e solo gli accordi che ne definiscono l'utilizzo le diano valore.

20 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857

21 Libertari tecnologici, cioè coloro che credono nel diritto fondamentale dell'individuo di essere libero, come WikiLeaks, Anonymous e Wikipedia.

2. IL LATO OSCURO DELLA RETE

Il web, un vasto mare in espansione

Nel romanzo *Solaris* di Stanislaw Lem, l'omonimo pianeta è ricoperto da un oceano, un unico enorme essere, una «macchina plasmatica [...] priva forse di vita secondo i nostri concetti ma capace di intraprendere attività utili su scala

astronomica», variabile nella forma, in costante autometamorfosi, in grado di intuire e modificare il pensiero degli uomini e materializzarne i pensieri; si tratta, insomma, di una sorta di oceano cosciente.

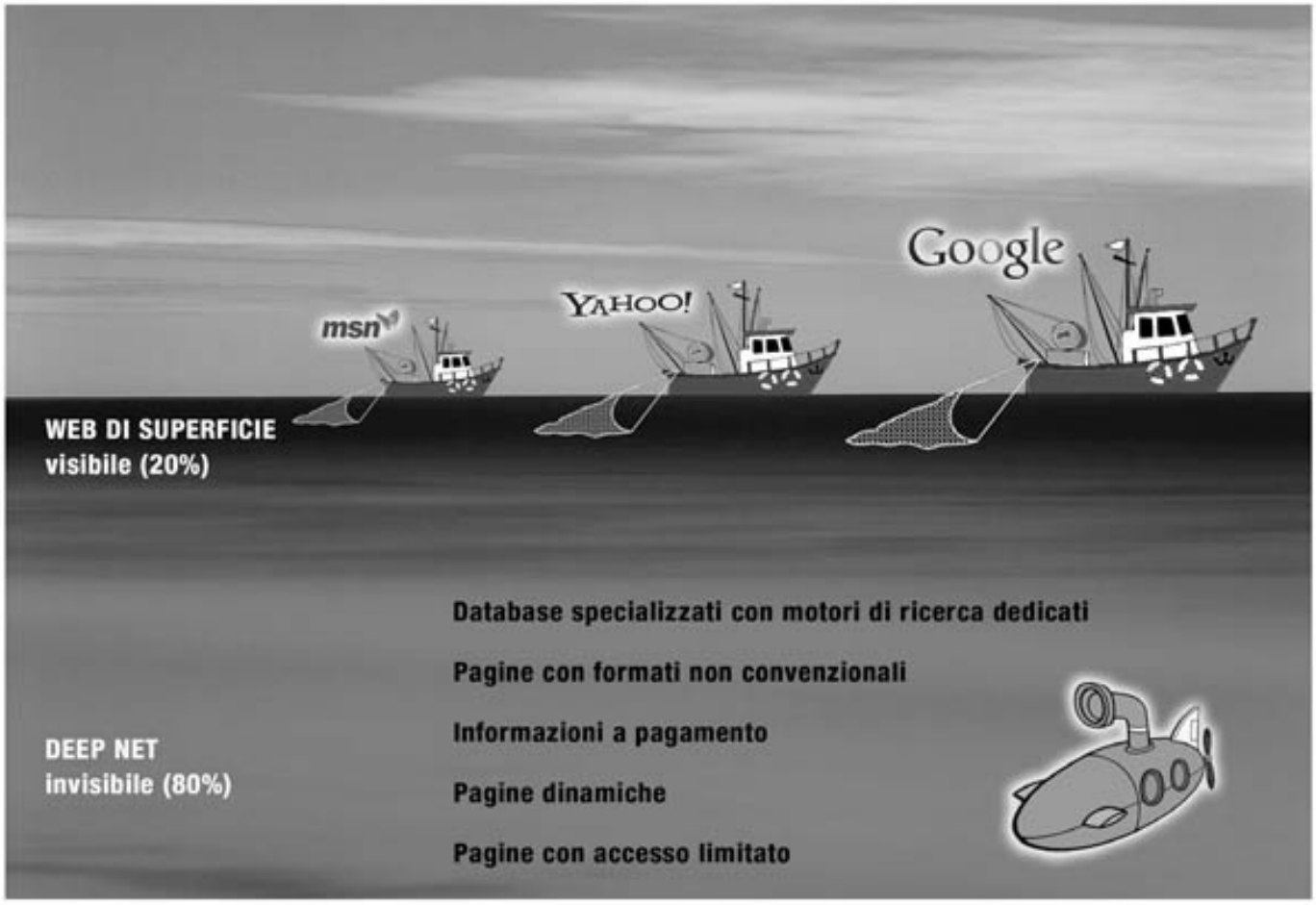
Immagine perfetta per descrivere il web: un vasto mare in espansione, esplorabile a diverse profondità, dotato di vita autonoma, capace di influenzare pensiero e comportamenti umani. Un luogo, dunque, e uno strumento, che a seconda di come viene utilizzato può assumere ruoli e finalità molto diverse.

Il web è l'insieme dei contenuti fruibili attraverso un *browser*, ossia tutto quel mondo esterno al vostro computer ma che potete raggiungere ed esplorare utilizzando determinati strumenti. Il fatto che vi muoviate in questo mondo come esploratori in terre selvagge viene ben rappresentato dai nomi dei browser: Explorer, Safari – ma anche Firefox, una volpe fiammante che avvolge il globo terrestre – e così via. Il web si «naviga», dunque, o meglio ancora, si «surfa» (*to surf* è il verbo originariamente scelto dalla lingua inglese per indicare il muoversi

nella rete). Nel web si avanza, dunque, in superficie. In che direzione? Come una bussola, i motori di ricerca ci aiutano a individuare dove sono raccolte le informazioni che stiamo cercando: se vogliamo saperne di più sulla fine del mondo, basterà collegarsi alle pagine di Google, Bing, Yahoo! (o alle pagine italiane di Virgilio e Arianna), scrivere nell'apposita finestra «fine del mondo» e scoprire in quali siti se ne parla, in quali libri, video o canzoni viene citata, e per quando è prevista. Insomma, tutto quello che sulla fine del mondo l'uomo ha

saputo ipotizzare, lo troverete. E tutto questo, solo rimanendo in superficie.

Il *deep web*, o web sommerso, è appena poco più sotto. Vi si trovano tutte quelle informazioni presenti nel web ma non segnalate dai normali motori di ricerca, perché questi non riescono a trovarle e quindi a catalogarle.



I motori di ricerca funzionano infatti così: utilizzano generalmente un software, chiamato *crawler* (una specie di sonda), che segue i link presenti nelle pagine web, li raccoglie, li analizza, e restituisce un indice dei contenuti disponibili. I motori di ricerca classificano i risultati in base ad

algoritmi che indicano il grado di rilevanza rispetto a una determinata chiave di ricerca.

Per raccogliere e analizzare dati, ossia per «indicizzarli», questi *crawler* possono accedere solo ai database relativi a pagine statiche, altrimenti il numero dei termini che potrebbero ricercare risulterebbe infinito. Tutto ciò che non è indicizzabile, dunque, è deep web. Ne fanno parte, ad esempio, tutte quelle pagine dinamiche che possono essere richiamate solamente eseguendo una specifica ricerca all'interno di un sito, così come quelle pagine web

che non sono collegate a nessun'altra pagina web. Sempre appartenenti al deep web sono le pagine il cui accesso è consentito solo attraverso l'inserimento di una password, come la nostra webmail oppure il profilo Facebook, o ancora siti web realizzati in tecnologia flash o con tecniche di programmazione diverse dall'uso dell'html (che è quello normalmente utilizzato per realizzare siti internet). Dunque, niente di segreto: deep web sono anche pagine di posta elettronica, messaggi di chat, reti aziendali, reti peer to peer, comunicazioni

via Skype, pagine protette da password, pagine che semplicemente non permettono l'accesso ai programmi dei motori di ricerca.

Gli studi che analizzano il web suggeriscono che solo una piccolissima quantità delle pagine web sia stata indicizzata. Data la sua vastità e l'interesse verso questa parte del web, numerosi programmatori e hacker ne seguono l'evoluzione e ne supportano gli avanzamenti.

Negli anni sono stati sviluppati anche dei motori di ricerca che tentano di

catalogare il deep web. Per farlo, questi devono utilizzare dei *crawler* più sofisticati che interrogano i database con termini specifici e riescono così ad accedere a maggiori informazioni (riescono, per così dire, a pescare più a fondo).

Siti come Deep Web Technologies (deepwebtech.com), accesso alla ricerca «profonda» su scienza, medicina e business, o il gigantesco database universitario The European Library (theeuropeanlibrary.org), TechXtra (techxtra.ac.uk), dedicato a ingegneria, matematica e informatica, e il ricchissimo

Complete Planet (aip.completeplanet.com), denominato infatti «front door to the deep web», rappresentano un buon punto di partenza se volete approfondire le vostre ricerche.

Il dark web

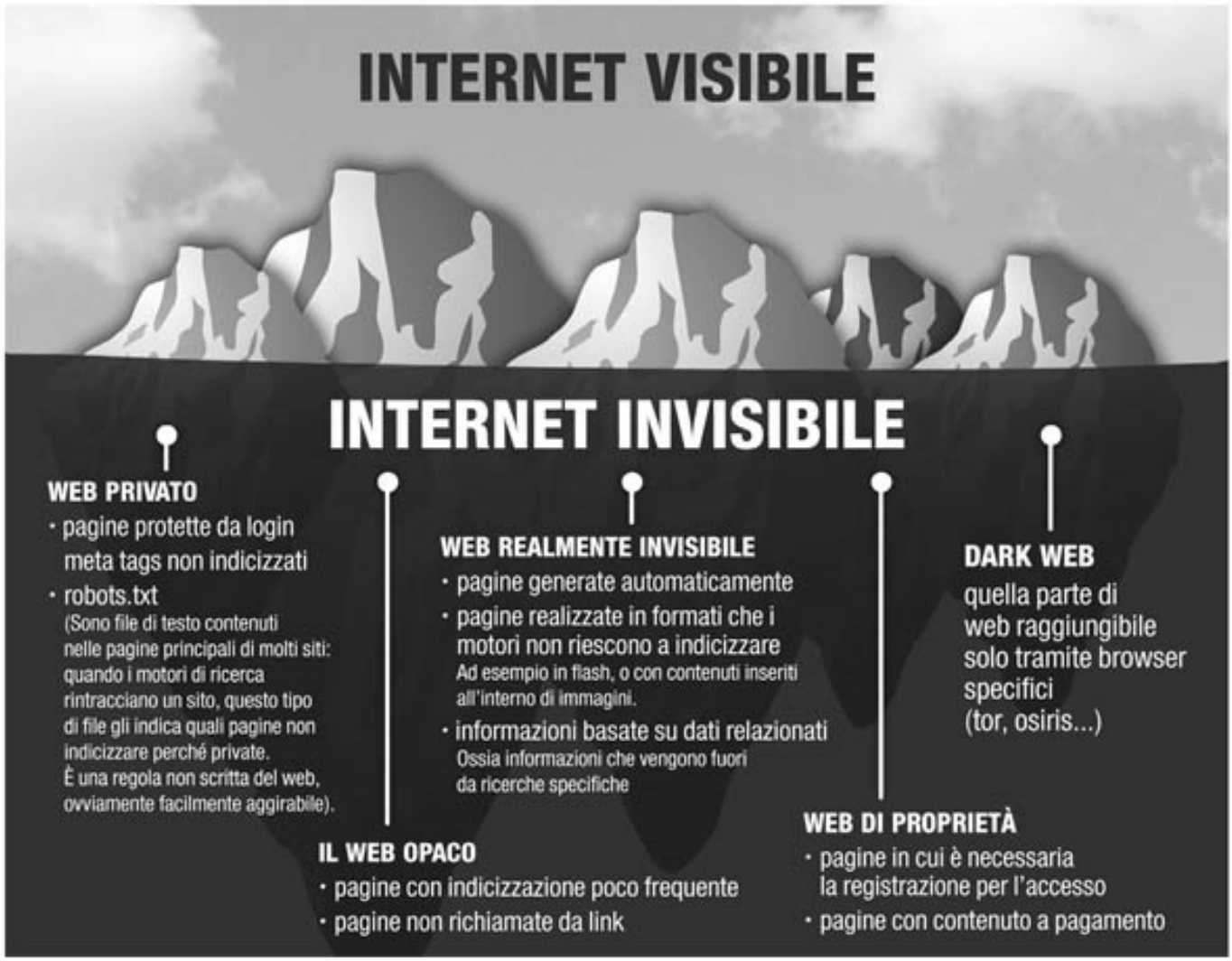
«The dark internet is any portion of the internet that can no longer be accessed through conventional means».

«La dark internet è qualsiasi parte di internet a cui non è più possibile accedere tramite mezzi convenzionali». (Wikipedia)

Esiste una porzione del deep web più complessa da esplorare. Si definisce *dark web*, e per accedervi è necessario utilizzare speciali software che permettono di raggiungere siti web anonimi e non rintracciabili. Tra questi software il più utilizzato è Tor, di cui faremo conoscenza tra poco.

Il dark web è dunque un'ulteriore dimensione della rete, uno strato ancor

più profondo, che non solo non viene indicizzato dai comuni motori di ricerca come avviene per il deep web, ma che non segue neppure le «regole» del web di superficie, essendo accessibile soltanto tramite specifiche applicazioni che rendono anonima ogni attività.



Il termine *dark web* deriva da *dark net*, cioè quel tipo di reti chiuse che necessitano di un software per l'accesso ai contenuti, reti caratterizzate da anonimato, riservatezza e altre qualità. Il termine fu originariamente coniato negli

anni Settanta per designare reti che erano isolate da Arpanet (la vecchia internet) per motivi di sicurezza.

Il fatto che ci si riferisca a questa parte della rete con il termine *dark* – «nero, oscuro» – fa pensare a molti che sia oscura anche la cosa in sé, che sia «roba da hacker» complicata, se non addirittura illecita e pericolosa.

Prima di inoltrarci nel dark web, allora, chiariamo questi due aspetti. Certo, per accedere al dark web si devono utilizzare alcuni browser specifici e la maggior parte dei siti al suo interno

richiedono login e altri mezzi per controllare l'accesso. Inoltre il dark web è sì colmo di pagine (ben più di quanto non lo sia il web di superficie), ma per raggiungerle bisogna conoscere l'indirizzo esatto, una specie di chiave, perché gli indirizzi (url) del dark web hanno nomi incomprensibili. Infine, molto più di quanto accada nel web tradizionale, qui i siti hanno vita variabile, a volte molto breve. Ma, a parte tutto questo, non è affatto difficile entrare nel dark web e fruire dei suoi contenuti. Come si fa, lo vedremo tra poco.

Secondo aspetto. Trattandosi di un territorio in cui ci si muove in completo anonimato, è ovvio che sia stato sfruttato anche per ogni genere di commercio illegale. Il rischio di imbattersi in pagine contenenti materiale pericoloso o illecito è alto anche per un semplice utente curioso soltanto di sapere cosa ci sia «là sotto». E non si tratta solo di indirizzi dove poter scaricare musica, videogiochi o film pirata, ma anche di siti che offrono droga, armi, killer a pagamento o pedopornografia. Questi servizi illegali e in grandissima parte immorali sono in

parte responsabili del timore che molti hanno di questo strumento, oscurandone in parte i contenuti più interessanti che invece vi si trovano. Perché materiale pericoloso ce n'è, ma ce n'è molto di più legale, più interessante e utile di quanto ci si possa aspettare. Vedremo insieme anche questo.

Fatta questa premessa, ricordiamo che nel dark web si possono trovare anche, oltre ai contenuti stessi del web tradizionale o di superficie, blog personali, siti scientifici, tecnici, siti-biblioteca, documenti contenenti preziose

informazioni riservate e molte offerte di servizi difficilmente presenti nel web tradizionale. Proprio perché l'accesso al dark web è criptato e anonimo, esso viene sfruttato anche da ricercatori, scienziati, attivisti politici e comuni cittadini che vogliono custodire e scambiare informazioni senza l'occhio del Grande Fratello sempre puntato addosso. Soprattutto in Paesi in cui il Grande Fratello è un regime che li minaccia di morte e censura le informazioni non allineate a quelle governative. Il fenomeno WikiLeaks, la nascita di gruppi

segreti come Anonymous, l'associarsi dei giovani ribelli protagonisti della Primavera araba, e persino la creazione di una nuova moneta tutta virtuale e sovranazionale non sarebbero stati possibili senza un territorio libero come è il dark web.

Il dark web dunque non è un pericolo di per sé, non va demonizzato, ma va innanzi tutto conosciuto e, nel caso, utilizzato. Ci sono già diversi forum dedicati a gruppi che cercano di approfondire la conoscenza del web profondo, con lo scopo non secondario di

cancellare l'immagine negativa che lo avvolge. Come qualunque altro strumento, se ne può infatti fare un uso buono o un uso cattivo. Scopriremo insieme come il dark web possa essere un importante mezzo per approfondire nuovi modi di condivisione della conoscenza, per accedere a contenuti inediti, per scoprire nuove funzionalità rispetto a quelle del web, per così dire, tradizionale.

Accedere al dark web

Come abbiamo detto, per navigare all'interno del dark web è necessario possedere dei software e browser specifici. Nel nostro caso analizzeremo Tor, che è il più conosciuto e utilizzato. Parleremo anche del progetto, per lo più italiano, noto come Rete Osiris, e dell'utilizzo di Psiphon, strumento che permette di oltrepassare i blocchi all'accesso della rete messi in atto dai Paesi in cui la censura è molto forte.

Tor: The Onion Router

Tor è un sistema di comunicazione anonima per internet[22] che permette di navigare – appunto in forma anonima – sia nel dark web sia nella rete tradizionale. Il suo funzionamento è (relativamente) semplice: fa viaggiare dati criptati attraverso diversi nodi, in modo da dissimulare l'identità della connessione sui siti visitati. Questo programma è *open source* e impedisce di fatto l'identificazione della propria posizione o della propria attività in rete: se un tecnico dovesse analizzare un computer in cui si usa solamente Tor per navigare, risulterà solo

il fatto che si è avuto accesso alla rete tramite Tor. A oggi è il software più utilizzato a questo scopo. Funziona con i browser, i sistemi di messaggistica istantanea, e più in generale può essere usato ogni volta che si accede a internet.

Quando si naviga o si invia un messaggio, dal proprio computer parte un pacchetto di informazioni a partire dal proprio indirizzo IP. Tor cripta questo pacchetto di dati, che invece di raggiungere direttamente il server relativo al sito visitato passa per stazioni intermedie fino alla destinazione, e queste

stazioni sono altri utenti che hanno scelto di far parte della rete Tor come *relay*. In pratica Tor protegge gli utenti dall'analisi del traffico attraverso una rete di *onion router* (i *relay*), gestiti da volontari, che permettono il traffico anonimo in uscita e la realizzazione di servizi web anonimi e nascosti. Nessuno sa da chi parte e a chi arriva il messaggio, si conosce solo chi ha fornito quel determinato pacchetto e a chi viene passato. I dati, nella rete Tor, non transitano unicamente tra client e server ma sono presenti all'interno di tutti o gran parte dei nodi della stessa rete Tor.

Questi nodi si comportano come router, reindirizzando casualmente i pacchetti di dati all'interno di un circuito crittografato. È un sistema costruito a strati, proprio come ricorda il termine inglese *onion* («cipolla»), da cui prende il nome.

I siti web creati per Tor non hanno le estensioni di dominio che conosciamo, ad esempio .com o .it, ma possiedono un'estensione chiamata .onion.

Il suffisso .onion è usato per i siti costruiti all'interno della rete Tor e questi sono, di fatto, ospitati sul computer del

loro creatore e possono essere trovati e raggiunti solo navigando attraverso Tor.

Questi siti sono anonimi e privi di un indirizzo pubblico vero e proprio (IP pubblico), e ciascun utente può fungere da *relay* prendendo parte attiva nella rete.

Un sito protetto da Tor può essere molto difficile da trovare, non si può visitare se non se ne conosce l'indirizzo esatto ed è consultabile solo attraverso l'installazione del browser Tor o usando un gateway come Tor2web[23]. A partire dal 2004, Tor ha consentito agli utenti di ospitare anche dei server, ma a differenza

dei server convenzionali, questi «servizi nascosti» di Tor non possono essere fatti risalire alla persona che li gestisce. Tutto questo garantisce all'utente un buon livello di anonimato.

Il software Tor permette di navigare e usufruire dei siti creati specificatamente per la rete Tor (i siti .onion), ma permette anche l'accesso a una grande quantità di servizi come chat, torrent, e alle tradizionali risorse sul web, sempre garantendo l'anonimato. Le considerazioni che si possono fare al riguardo sono dunque quelle fatte per il

dark web in generale. Grazie a Tor è possibile la navigazione sul web senza vincoli, e si rivela particolarmente prezioso in quei luoghi in cui sono in vigore restrizioni politiche o censure di vario genere. Giornalisti, poliziotti, fotografi, testimoni, blogger dissidenti, ricercatori «scomodi» e tutti coloro che vogliono navigare senza essere tracciati scelgono Tor. Lo scelgono dunque anche persone comuni, e anche solo per necessità quotidiane, come una semplice ricerca di file o per l'accesso ai social network. Molti utenti, per lo più

giovanissimi, lo utilizzano per guardare serie tv che non sono trasmesse al di fuori di un determinato Paese. Insomma, esiste un uso di Tor (e di strumenti simili che vedremo tra poco) assolutamente lecito. Se non addirittura «nobile», come accade quando diventa il mezzo per combattere battaglie civili per i diritti umani.

Osiris

Un altro sistema che permette di pubblicare siti internet difficilmente

censurabili e anonimi è il progetto, per lo più italiano, Osiris (http://osiris.kodeware.net), che tra gli altri vantaggi ha quello di poter essere utilizzato di concerto con Tor[24].

La definizione che ne dà Wikipedia è la seguente: «*Osiris Serverless Portal System* (solitamente abbreviato in Osiris sps o Osiris) è un programma gratuito per la creazione di portali web completamente distribuiti tramite p2p e autonomi dai comuni server per i sistemi operativi Microsoft Windows, GNU/Linux e Mac OS X».

L'obiettivo del progetto è quello di permettere a chiunque di creare e mantenere un sito internet p2p, senza ricorrere a un server centrale, senza pagare l'affitto a un gestore, senza bisogno di registrarsi come proprietari del sito. Non esistendo un server centrale su cui esso debba basarsi, non è facile censurare l'accesso al sito basato su Osiris.

In questo modo il sito è protetto da guasti, da attacchi diretti come i DDoS (che lo renderebbero inaccessibile) e da limitazioni imposte dagli Internet Service

Provider (*policy*, traffico, censura, ecc.) Dunque, si può realmente parlare di un portale *free* secondo le due accezioni della lingua inglese: *free* nel senso di «gratuito», ma anche «libero» da controlli esterni.

Il principio fondante di questo software è lo stesso su cui si basa il protocollo p2p: più copie esistono di uno stesso file e più sarà difficile un tentativo di farle sparire tutte. Ogni sito creato con Osiris viene distribuito via p2p tra i computer su cui è registrato lo stesso sito web. Quindi, se ci colleghiamo con Osiris, il nostro computer veicolerà

solamente i siti a cui siamo registrati.

La particolarità di questo sistema è che la navigazione nel sito avviene «in locale», ovvero sulla copia del sito stesso che viene trasferita sul nostro computer, poiché il protocollo p2p implementato in Osiris è concepito solamente per distribuire i diversi siti e non per inoltrare ricerche (come avviene in altri sistemi p2p).

Una fondamentale differenza, rispetto ad altri sistemi, è che in Osiris qualsiasi utente può vedere i dati presenti nel proprio computer («in locale») poiché

questi non sono criptati (a parte i messaggi privati). Se qualcuno reputa negativamente tali informazioni, potrà non contribuire alla loro diffusione. In pratica, è come se in Osiris esistesse la censura, ma fossero tutti gli utenti a determinarla. «Un portale Osiris è simile a un wiki», è scritto sul blog di Anonymous, «dato che non solo gli utenti sono liberi di aggiungere contributi, ma sono anche liberi di modificare i contributi altrui». In teoria il sistema fornisce anche la possibilità di distribuire indiscriminatamente tutti i contenuti, ma

ciò ne rallenterebbe il funzionamento.

I messaggi privati sono l'unica tipologia di dati che non sono leggibili da chiunque, ma solamente dal mittente e dal destinatario. Qualsiasi utente ha comunque la facoltà di disattivare il supporto ai messaggi privati: questo permette di non distribuire dati che non è possibile leggere, ma non permetterà né di inviare, né di ricevere messaggi privati.

Osiris, in maniera totalmente automatica, cerca continuamente di contattare altri nodi per poter scambiare e/o allineare i contenuti, e tiene traccia

dei computer con i quali ha potuto comunicare al meglio, generando una specie di classifica per stabilire i migliori «contatti».

Psiphon

Psiphon è un software canadese anti-censura che permette di aggirare i firewall, penetrando nelle falle presenti nei sistemi di sbarramento per la circolazione in rete dei documenti, delle immagini e dei video. Psiphon viene

principalmente utilizzato per accedere alle notizie e ai siti dei social network bloccati dalla censura di governi e regimi, per sapere cosa si dice al di fuori dei propri confini nazionali e dei canali ufficiali vigilati dagli organi governativi.

Psiphon, come altri software del genere, collega il proprio terminale a un proxy che consente di leggere la pagina che è stata bloccata. Per dirla con semplicità, alcuni computer (*psiphonodes*) funzionano da server, fungendo da collegamento alla rete libera, e a questi si collegano gli utenti (*psiphonites*) tramite

protocollo https, che essendo il protocollo utilizzato anche per le transazioni finanziarie è più difficilmente bloccato dai provider.

Rafal Rohozinski, sviluppatore del programma, lo definisce «un software per i diritti umani» nato a seguito della crescita del controllo della rete da parte dei governi. Proprio perché destinato alla gente comune, l'utilizzo di Psiphon non richiede alcuna competenza tecnica, si può utilizzare sia dal pc che dal cellulare.

Onionlanding

Pomeriggio di pioggia.
Istruzioni per l'uso.

Tanto per vedere insieme quanto sia semplice navigare per il dark web, ho approfittato di un pomeriggio di pioggia per esplorare alcuni siti .onion, sottogruppo di siti costruiti all'interno di Tor (dal quale, appunto, prendono il suffisso .onion).

Questi siti sono, di fatto, ospitati sul computer del loro creatore e possono essere trovati e raggiunti solo navigando

attraverso Tor, sia nella versione Tor Browser, sia nella sua versione completa.

Per accedere a questi siti ho dunque bisogno di Tor, perché i siti .onion non possiedono un nome e un indirizzo vero e proprio come quelli normali, ma un codice che serve a identificarli e localizzarli all'interno della stessa rete Tor: non sono collocati in un qualche punto della rete normale, ma sono come pagine realizzate e condivise all'interno di una rete criptata.

Il tipico indirizzo di questi siti è una successione di lettere e numeri, spesso

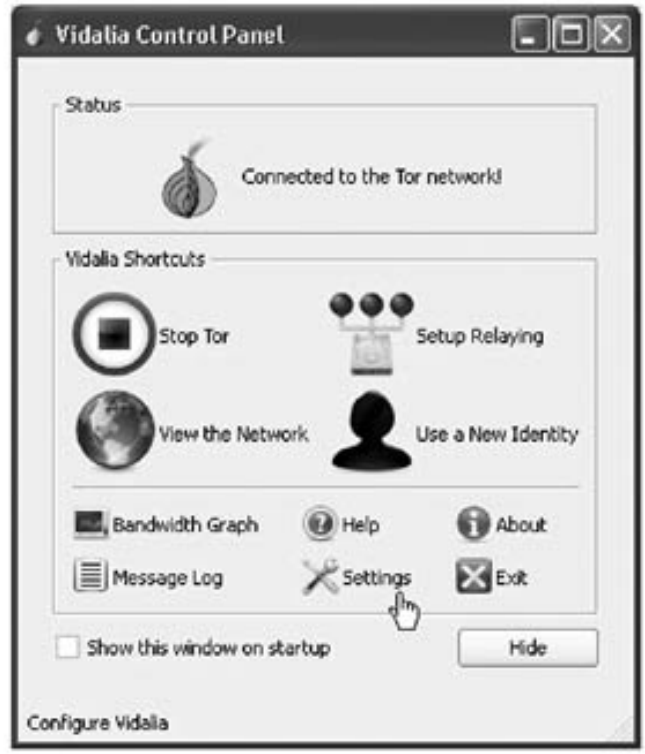
prive di significato apparente, dove la prima parte è un numero a 80 bit in base 32 e la seconda parte è lo pseudodominio di primo livello .onion, che ne identifica la natura.

Prima di iniziare la nostra esplorazione, un paio di avvertimenti. Innanzitutto, l'uso di Tor rallenta la navigazione, sia per la natura del processo di trasmissione sia perché non è ancora così diffuso. Per provarlo basta scaricare Tor Browser, una sorta di Firefox modificato che può essere usato senza necessità di installare nulla. Può essere

anche trasportato su chiave USB. Come per la normale navigazione, quando l'utente accede a una pagina per la prima volta, essa viene immagazzinata in memoria (*cache*), per cui diventa più veloce accedervi nuovamente. In secondo luogo, visto che la navigazione nel dark web può essere pericolosa, consiglio di utilizzare una macchina che abbia installato un buon anti-virus e un firewall. Terzo, ma lo sappiamo già, si corre il rischio di imbattersi in contenuti illegali inquietanti.

È arrivato il momento di procedere. Procuriamoci Tor. Puntiamo il browser

sulla pagina www.torproject.org e nella sezione download ci viene subito segnalato di scaricare la versione per il computer che stiamo utilizzando (nel mio caso, un Mac). Otteniamo dunque il file, e lo installiamo. Fatto questo, l'applicazione è pronta per essere utilizzata: ci apparirà l'icona di Tor, una piccola cipolla colorata, e cliccandoci sopra ne avvieremo l'apertura. È quello che faccio, e mi trovo davanti questa schermata, che avvia la fase di autenticazione:



Terminata l'autenticazione, siamo connessi alla rete Tor: si aprirà il browser e saremo liberi di navigare anonimamente.

Se ci fate caso, appena si apre, il Tor Browser segnala un indirizzo IP «fasullo» che ovviamente non è quello della vostra connessione adsl.

Dalla schermata «Vidalia control panel» mostrata sopra sarà possibile interrompere Tor, configurarlo solo per navigare o come *relay*, visualizzare la mappa degli utenti di Tor e cambiare identità, opzione utile se abbiamo appena visitato un sito di cui non ci fidiamo. Non scendo nel dettaglio di queste funzioni, ma Tor ha un buon wiki e ci sono ottime guide in giro per la rete.

Ora che mi trovo su Tor posso iniziare a esplorare il dark web. So già che non esiste, qui, un motore di ricerca efficiente come Google, e che dovrò

digitare nell'apposita barra l'indirizzo esatto del sito che voglio raggiungere (indirizzo, come abbiamo già detto, spesso incomprensibile e senz'altro difficile da memorizzare). Poiché non ricordo nessuno degli indecifrabili indirizzi .onion, decido di partire da Google e vedere se trovo qualche suggerimento sui forum. Quello che cerco è un indirizzo da copiare e incollare sulla barra degli indirizzi del Tor Browser: mi sento ispirato dalla ricerca «i migliori siti .onion» e trovo subito tra i risultati alcuni indirizzi, ma non mi fido molto visto che

alcuni provengono da forum poco edificanti.

Un buon sito da cui far partire le nostre ricerche mi sembra invece Search Onion Sites (https://ahmia.fi/address/): vi trovo una corposa lista di siti .onion: scoprirò che non tutti sono funzionanti ma è pur sempre una vasta mappa per raggiungere luoghi profondi. Decido infine di fidarmi di un blog, e seguo le indicazioni di un buon articolo che trovo sull'Antro del nerd (http://antrodelnerd.blogspot.com), che descrive e segnala alcuni indirizzi utili per

la nostra prima volta.

Seguendo i primi link segnalati, approdo sul più celebre motore di ricerca per la rete Tor, Torch, il cui indirizzo (http://xmh57jrzrnw6insl.onion) copio e incollo immediatamente sul browser Tor. La pagina si apre dopo un'attesa di qualche secondo: graficamente è molto spartano ma da quel che si legge dovrebbe aver indicizzato oltre un milione di pagine .onion. Inizio a smanettare per vedere come funziona e quanto è utile effettivamente. La navigazione con Tor è veramente molto

lenta ed essendo abituato alla risposta immediata di Google resto basito ad attendere mezzo minuto prima di vedere i sei risultati della ricerca delle parole *cold fusion*. E non trovo neppure nulla di interessante! Provo altre ricerche ma non mi sembra che si possa usare come Google e giocare con i termini per fare delle ricerche, il contenuto mostrato da Torch è prevalentemente fatto da documenti di testo.

Decido allora di passare a un altro sito per le ricerche chiamato Onion (http://dts563ge5y7c2ika.onion/Onionsea

che rispetto ad altri offre già una prima selezione di pagine utili (o potenzialmente utili) per un navigante di Onionland (cliccando su «How to start»).

Tra queste ho subito notato SilkRoad, «*marketplace with escrow (bitcoin)*», il bazar dove si vende di tutto e di cui la stampa ha parlato abbastanza, con articoli sensazionalistici e piuttosto imprecisi. A quanto pare, non è poi così difficile da raggiungere come lo descrivono i giornalisti, mi appunto l'indirizzo per arrivarci tra poco. Provo invece delle chiavi di ricerca ma non approdo a nulla.

Nel sito Antro del nerd avevo letto che in alternativa ai motori di ricerca esistono anche siti directory, dove i vari link sono raccolti e suddivisi per genere. Decido di puntare la prua su TorDir (http://dppmfxaacucguzpc.onion).

Attendo i soliti secondi utili ad allineare la rotta e mi compare un sito che sembra Yahoo! alla primissima versione. Spicca il banner di Black Market (http://5onwnspjvuk7cwvk.onion), un altro di quei luoghi dove si può vendere e comprare qualsiasi cosa anonimamente. Lo visiterò tra poco, perché ancora non

sono riuscito a farmi un'idea globale su cosa si possa effettivamente trovare nel dark web, e come.

Sempre grazie ai consigli sul web di superficie, arrivo finalmente a gettare le ancore sulla Hidden Wiki (http://7jguhsfwruviatqe.onion), che a Onionland rappresenta una sorta di guida alla navigazione nella rete Tor[25]. Soprattutto, come già abbiamo visto per TorDir, fornisce una lista di siti .onion a cui accedere, divisi per lingua e in parte per argomento, con diverse forme di classificazione e categorie: in sostanza, un

indice molto ampio dei contenuti che si trovano nel dark web e tutorial su come trovarne altri.

Quello che abbiamo detto circa l'incerta durata della vita di un sito .onion si applica anche alle altre risorse, compresi i motori di ricerca, se così li vogliamo chiamare. Scopro infatti che uno dei motori di cui più si parlava, Deep Search, sembra non funzionare più[26].

Come nel web «normale», poi, la maggior parte dei siti è ovviamente in inglese: vedrete però che esistono anche siti e forum in italiano dove trovare

commenti e proposte, e nel caso chiedere consigli a utenti più esperti per muovervi meglio all'interno della rete Tor.

Un blog tutto italiano molto utile, ad esempio, è Cipolla (http://x4tmhtkin4kumdvl.onion/forum). Arrivo sulla pagina e mi perdo tra diversi post di quelli che mi sembrano truffatori o contraffattori, non sono sicuro che ciò che scrivono sia vero ma perdo comunque molto tempo a scorrere tra domande e risposte su argomenti che sarebbero immediatamente censurati nei forum «normali».

Prima di andare a curiosare nei due grandi mercati neri del dark web di cui tanto si parla, do un'occhiata all'ampia scelta di libri della Tor Library (http://am4wuhz3zifexz5u.onion/) e al più celebre WikiLeaks (http://zbnnr7qzaxlk5tms.onion/), il grande contenitore di documenti riservati, che già ha messo in crisi parecchie aziende e governi.

Alla fine, eccomi al mercato nero, tra Black Market Reloaded (http://5onwnspjvuk7cwvk.onion/index.p e il già nominato SilkRoad, dove potete

fare qualunque tipo di acquisto nel più completo anonimato.

Tra i due, SilkRoad è probabilmente il sito più citato nella stragrande maggioranza degli articoli che le testate giornalistiche tradizionali hanno dedicato al fenomeno del dark web. Questo sito è un *e-commerce*, un negozio online all'interno del quale sono disponibili prodotti che di norma non possono essere commerciati legalmente: droga, armi, ogni tipo di medicinali, carte di credito anonime o clonate, materiale contraffatto e/o rubato e tanto altro.

Accedere a SilkRoad è fin troppo semplice (basta cercare su Google[27] e ne parlano più o meno tutti e soprattutto persone poco informate). Questo aspetto mi fa pensare che forse SilkRoad non sia altro che uno specchietto per le allodole, uno spaventapasseri che piace però molto agli uccelli. Non entrerò dunque nei dettagli, perché vi basterà cercare su YouTube e vi appariranno decine di video che lo illustrano e ne evidenziano le peculiarità illegali. Se i video non vi bastano, potete accedere direttamente al sito ed effettuare la registrazione tramite

il link «Click here to login»[28].

Nel mercato nero della rete, ovviamente, nessuno userebbe mai la propria carta di credito o una carta prepagata intestata a proprio nome: è per questo che gli inserzionisti accettano come pagamento solo i bitcoin.

Questi mercati dark, infatti, non sarebbero mai potuti esistere senza un sistema di scambio ispirato alla stessa filosofia di libertà e anonimato. È un modello di libertà dagli enormi vantaggi, ma che può senza dubbio favorire gli individui e le organizzazioni con

tendenze criminali, basta vedere quanto sia facile acquistare o vendere qualsiasi prodotto in uno di questi mercati neri mantenendo l'anonimato.

Comprare e vendere nel dark web

Nel dark web si naviga a vista e spesso ci si imbatte in siti in cui si vendono oggetti e servizi di varia natura, i cosiddetti «market place». Cerchiamo di comprendere in che modo gli scambi di

merce, e quindi di denaro, siano possibili in questa porzione del web dove tutto avviene rigorosamente in maniera anonima. Come possono infatti avvenire scambi di merce in completo anonimato? Come fidarsi del venditore, come essere sicuri che il compratore effettivamente pagherà? Eppure, l'anonimato è necessario: in molti di questi «mercati» è possibile acquistare beni di cui, in alcuni Paesi, potrebbe essere vietata non solo la vendita ma anche lo stesso possesso. E poi, se si finisce a fare acquisti nel dark web, è perché non si vuol far sapere cosa

si sta comprando: l'uomo che prenota un viaggio con l'amante, l'ipocondriaco che si procura scorte di medicinali sufficienti per due vite, la donna che assolda un detective privato per seguire il marito... Non è detto che proprio tutti debbano fare acquisti illegali, ma è sicuro che non tutti vogliono avere le proprie spese ben memorizzate sul saldo della carta di credito.

L'anonimato, dunque, questo alleato. Una prima garanzia viene data dal fatto stesso che si naviga nel dark web, e che quindi sarebbe molto difficile risalire

all'identità di chi vende e di chi compra. Inoltre, tutti i siti «commerciali», nel dark web, accettano come moneta di scambio prevalente il bitcoin che, come abbiamo visto, può offrire un alto livello di anonimato. Se si vogliono fare acquisti, dunque, non si deve far altro che procurarsene una buona quantità. Abbiamo già parlato di come procurarsi bitcoin per scambi sul web di superficie ma in questo caso è necessario, ovviamente, procurarseli in modo anonimo. Un buon modo, suggerito anche in numerosi forum, è quello di

procurarsi una carta PaySafeCard (PSC), ossia uno strumento di pagamento prepagato spendibile online. Non è il solo strumento possibile ma è, almeno in Europa, il più diffuso. Si tratta di una carta – più che altro un pezzetto di carta – di valore compreso tra i dieci e i cento euro. La si compra in molti punti vendita (giornalai e tabaccherie compresi) e se ne possono acquistare – in una sola volta – fino a dieci, per un valore totale di mille euro. Funziona come un gratta e vinci: si gratta la parte argentata e ne esce un codice di svariate cifre che va poi inserito

come codice di pagamento quando si effettuano acquisti online. È un valido strumento per fare acquisti in rete in sicurezza: se viene smarrito o rubato, si perde solo il valore della singola carta. Poiché per acquistarla si paga in contanti, è anche un modo per fare acquisti online senza rivelare la propria identità. O per acquistare bitcoin. Ottenuta una PSC del valore desiderato, siamo pronti per scambiarla in bitcoin. Non è un'operazione a buon mercato ma si possono trovare diversi forum e siti attraverso i quali trovare informazioni,

uno dei più noti è bitcointalk.org. Ottenuti i bitcoin, l'acquirente che volesse continuare a restare anonimo cercherà di connettersi al servizio Bitcoin sfruttando una connessione sicura[29] e da questa usare Tor. Utilizzando Tor potrà scambiare i bitcoin per il codice della PSC. Una volta in possesso dei bitcoin potrà spenderli liberamente, senza che si possa risalire alla sua identità.

Un ipotetico venditore che, come l'acquirente, volesse rimanere anonimo, può operare gestendo un sito che sfrutta il servizio *hidden service* di Tor, attraverso

il quale può pubblicare anonimamente le proprie offerte. Connettendosi al servizio Bitcoin (anch'egli sfruttando connessioni sicure), una volta che il compratore ha pagato con bitcoin, il venditore porta la merce in un luogo segreto. E qui viene il bello: al compratore verrà dato il link delle coordinate di Google Maps tramite uno dei tanti sistemi di messaggistica anonima. A quel punto il compratore, verificata la merce, invierà un codice di sblocco che permetterà al venditore di incassare i bitcoin. Qualora il codice di sblocco non venisse fornito al venditore,

l'acquirente non potrà comunque riprendersi i bitcoin. In questo modo, sono tutelati entrambi: il compratore sulla disponibilità della merce, il venditore sul pagamento. E tutto questo senza incontrarsi mai.

Quant'è sicuro navigare nel dark web?

Navigando nel web profondo ci sono alcune precauzioni da prendere.

Tor è un software di navigazione

eccezionale, tuttavia ha alcuni limiti, essendo focalizzato principalmente sulla protezione dei dati che vengono trasportati. Innanzitutto è necessario installare l'ultimissima versione del pacchetto Vidalia-Tor, e per navigare si dovrebbe usare il pacchetto Tor Browser, la nuova versione del quale include una versione non sempre aggiornata di Firefox. Ma gli strumenti di anonimato divengono totalmente inefficaci se non si adotta un comportamento sufficientemente cautelativo.

Quando si naviga in profondità

bisogna essere, diciamo così, razionali: non dobbiamo mai inserire informazioni personali, in nessun luogo, anche se ci viene richiesto. Ricordate: Tor garantisce l'anonimato, ma sappiamo tutti che nessuno è infallibile e non c'è nulla che Tor possa fare per proteggervi da un sito di raccolta di informazioni se avete volutamente inserito le vostre.

Un'altra cosa di cui abbiamo accennato sono i servizi VPN. VPN è l'acronimo di «Virtual Private Network». L e VPN sono reti private che molte aziende utilizzano per mantenere la

sicurezza soprattutto per le loro transazioni finanziarie. Sono più difficili da «spiare» e offrono un livello di protezione soddisfacente. Quindi è consigliabile utilizzare uno di questi servizi. Ricordate che nessun software, nessun metodo è totalmente sicuro. Continuiamo quindi a tenerlo a mente. Se davvero volete fare in modo che si coprano le vostre tracce, allora provate ad adottare la mentalità di una persona che vuole scomparire totalmente. Come in ogni buon thriller l'agente segreto rompe ogni forma di routine, così l'internauta

del dark web, quando potrà, cambierà di certo il proprio IP.

Aprire il vostro sito e condividere documenti privati

I vantaggi di avere un sito .onion sono vari. Innanzi tutto, non dovete spendere nulla. Non c'è Icann da pagare né per registrare il dominio né per rinnovarlo. E il dominio viene generato automaticamente dal software Tor, che vi permette anche di modificarne in seguito

la posizione (a garanzia di un maggior anonimato).

Non entrerò nello specifico di come configurare un server e ottenere un dominio .onion attivo e funzionante, perché è una questione tecnica e ci sono molti siti che svolgono questo compito. Dirò solamente come iniziare.

Un dominio .onion è uno pseudo-dominio di primo livello che viene utilizzato per la navigazione anonima nel web profondo attraverso la rete Tor. Il dominio .onion è composto da una stringa (*hash*) semi-numerica di 16

caratteri e in nessun caso rappresenta aree geografiche. La procedura per impostare uno di questi domini .onion e il relativo sito è abbastanza semplice per chi mastica la tecnica e ha dimestichezza con la configurazione e registrazione di domini. Accenniamo solamente al fatto che è possibile offrire un server web senza rivelare il proprio indirizzo IP agli altri utenti. Non si utilizza un indirizzo IP pubblico.

Non spiegherò in questa sede come impostare un server web e rimando i più curiosi alla pagina del progetto Tor[30] in

cui viene spiegato in dettaglio come installare e configurare correttamente un server web anonimo con Tor. Se si seguono le istruzioni riportate, una volta installato il proprio server, Tor genera automaticamente l'indirizzo .onion.

A questo punto potete inserire le vostre pagine web, quelle il cui contenuto volete rimanga anonimo, e fornendo l'indirizzo di dominio, che si mostra come un testo alfanumerico più o meno incomprensibile, i vostri utenti potranno leggere ciò che avete deciso di pubblicare.

La biblioteca di Alessandria

Uno degli aspetti più interessanti del dark web è che le informazioni che vi si trovano non sono teoricamente censurabili e quindi non possono essere bloccate. Bisognerebbe aggiungere «facilmente», ossia lo sforzo, il tempo e le difficoltà intrinseche di ricerche mirate all'interno del dark web lo rendono di fatto un territorio libero. Nel dark web può risiedere qualsiasi cosa, senza che nessun organismo di polizia possa far molto per cancellare le informazioni

scomode. Il costo necessario per censurare il web segreto è immenso.

Sebbene, come abbiamo visto, esistano diversi contenuti estremamente interessanti come documenti di WikiLeaks, esperimenti di scienziati di tutte le nazionalità, informazioni dai Paesi che usano la censura per mascherare i crimini sull'umanità, del dark web emerge spesso solo l'aspetto più oscuro. Negli ultimi anni ho letto numerosi articoli e video-documenti online in cui si è parlato del dark web (molto spesso a sproposito) come di un porto franco in

cui delinquere dal salotto di casa, di un Far West dove non esiste alcuna legge, del regno della criminalità e delle più orride devianze.

C'è anche quello. Ed è esattamente ciò che viene sfruttato dai detrattori, che tentano di mostrare il dark web ai media come il sunto dei suoi lati oscuri e raccapriccianti, cercando di instillare l'idea che accedervi sia di per sé un crimine e che senza controllo la parte peggiore dell'uomo prevalga. Ma questo vale solo per alcuni, non per tutti.

Il sincero disgusto per certe immagini,

l'apprezzabile amore per la legalità, la lotta contro il crimine sono sicuramente alcune delle motivazioni di chi conduce questa battaglia contro i sistemi di anonimato (probabilmente persa in partenza). Ma la motivazione più profonda è un'altra: la paura. Uno strumento che fa dell'assenza del controllo la sua forza non può che incutere timore.

Più che un selvaggio Far West, dunque, il dark web è la «biblioteca di Alessandria»[31] aperta potenzialmente a tutti: chiunque può aggiungere

documenti, nessuno può cancellare o censurare le informazioni che vi sono contenute (questo può succedere in rari casi, e in modalità molto complesse, quando la maggior parte degli utenti è d'accordo e collabora per farlo: lo vedremo poco più avanti col caso Lolita). È per questo che l'impatto del dark web sulla vita reale, di superficie, potrebbe essere enorme: pensate a cosa accadrebbe nel mondo se fossero divulgate informazioni «protette» come formule scientifiche classificate o segreti industriali e militari... Pensate a cosa

accadrebbe se fosse possibile controllare chi fino a ieri ha solo controllato.

Anonimato, censura e qualche buona notizia

Nel 2010 Tor è stato premiato con il riconoscimento della fsf (Free Software Foundation), che gli ha assegnato il Free Software Award for Projects of Social Benefit, un premio conferito a team creatori di idee e progetti di software liberi da cui la società possa trarre

«significativi benefici».

Negli ultimi due anni il premio è stato conferito a progetti per sostenere gli aiuti sanitari nei Paesi in via di sviluppo o per le fasce di popolazione più svantaggiate[32], nel 2010 è andato a Tor, nel 2008 a Creative Commons e nel 2005 a Wikipedia. Tor è stato premiato perché, attraverso «il software libero», ha consentito a 36 milioni di persone in tutto il mondo di avere libertà di accesso e di espressione sul web.

Questo riconoscimento è dunque una buona notizia per il software Tor, ma

soprattutto lo è per la battaglia per la libertà di espressione, di accesso e riservatezza, tanto più importante e urgente dove la censura agisce ogni giorno. Tor ha già mostrato di poter avere un ruolo chiave per le rivoluzioni politiche e sociali nei regimi autoritari: ha permesso di «scavalcare» le barriere dei governi, di trasmettere, di criticare o difendere, facendo sentire la voce di chi non ne aveva, come è accaduto di recente in Iran e in Egitto.

Vale la pena di citare il portale di Reporters sans frontières, che pubblica

contenuti proibiti o punibili da regimi autoritari. Foto, video, articoli inviati da giornalisti o utenti comuni sono esaminati e poi inseriti con eventuali contestualizzazioni. Il tutto in modo che i contenuti possano essere facilmente duplicati e diffusi. I tentativi di bloccare il portale vengono aggirati attraverso la creazione di «siti specchio»: ogni documento che appare potrà essere duplicato e riprodotto, con l'invito a tutti gli internauti a contribuire ospitando sui loro server i contenuti specchio. Maggiore il tentativo di censura, maggiore

l'attenzione che riceve l'informazione, maggiore la diffusione mediatica, come previsto dal cosiddetto effetto Streisand[33]. Agli utenti viene garantito l'anonimato e viene consigliato l'accesso tramite reti virtuali private (VPNs), Tor, Psiphon, ecc. Lo scopo è ancora una volta impedire la censura e diffondere contenuti, attraverso la condivisione e la partecipazione.

La libertà è partecipazione, cantava Gaber. Mai stato più vero.

Autoregolazione

Anonymous, celebre gruppo hacker che raccoglie un numero imprecisato di simpatizzanti e sostenitori, ha realizzato un attacco mortale verso alcuni siti pedopornografici della dark net, il più celebre dei quali, chiamato Lolita City, raccoglieva più di 100 gigabyte di immagini pedopornografiche di ogni tipo.

L'attacco, come annunciato, è iniziato ufficialmente il 14 ottobre 2011. Anonymous ha dichiarato guerra sostenendo che «i proprietari e gli

operatori della rete libera che permettono ai pedofili di mostrare bambini innocenti [...] vengono considerati il nemico numero uno della Open dark net». Questa battaglia condotta da Anonymous ha portato alla chiusura di oltre 40 siti web accusati di scambio di pedopornografia, e ha permesso di pubblicare i dati di 1589 presunti pedofili che erano stati utilizzatori di questi siti.

Gli Anonymous hanno combattuto utilizzando armi hacker molto sofisticate ed efficaci che hanno permesso di «ripulire» in parte la rete Tor attraverso

un'ampia mobilitazione denominata «Operation DarkNet» o «OpDarkNet» e, in concerto con la comunità hacker mondiale, è riuscita a fornire protezione e controllo dove la polizia non era stata in grado di intervenire.

Il sito Lolita City era protetto dalla rete Tor. Questo sistema non è quindi infallibile.

Gli appartenenti al gruppo Anonymous, il cui motto è «Unity-Service-Recovery», sanno che, per mantenere in vita questo sistema, c'è bisogno di un forte controllo morale. Gli

hacker sanno che l'esistenza di queste devianze può contribuire a far accettare all'opinione pubblica il tentativo, portato ciclicamente avanti da alcuni Paesi democratici dell'occidente, di prendere provvedimenti per limitare la libertà nella rete.

Occorre davvero restare lucidi e non permettere che il dark web divenga sinonimo di pedofilia e crimine. Tutto quello che emerge sul dark web esisteva anche ieri, e forse proprio grazie alla sensazione, da parte di questo tipo di criminali, di poter operare indisturbati, si

possono tracciare contenuti che invece sarebbero scambiati nel sottobosco della società civile sfruttando, ad esempio, l'inviolabilità della corrispondenza postale presente in molte legislazioni dei Paesi più fortemente democratici.

Nel dark web prospera quello che non è accettato nella rete tradizionale, che sembrerà pulita in superficie, ma quanto maggiore sarà la censura tanto maggiore sarà lo sviluppo di questa parte franca. Un fenomeno evidente in questi ultimi anni è quello del trasferimento di siti di *file sharing* dal web tradizionale al dark

web, per aggirare le strette regole sul copyright. Più censura e repressione, più siti che si spostano e si sviluppano in questa Onionland.

Strumenti come Tor non solo sono utili ma sono necessari per permettere lo scambio di idee e di informazioni oltre le vie ufficiali.

Della parola *privacy* si fa un utilizzo quotidiano che a volte sembra ossessivo, in questo caso invece è davvero importante ricordare che abbiamo il diritto alla riservatezza delle nostre informazioni personali e del nostro

privato: qualora non si prefiguri un reato si tratta della forma più elementare di libertà. Siamo abituati a essere controllati e quindi siamo spaventati quando il controllo cessa e si entra in uno spazio veramente libero. Invece dovremmo essere spaventati dal controllo stesso, e non perché nascondiamo un peccato ma per l'uso immediato o futuro che altri possano fare delle nostre informazioni personali. Quando si naviga, si seminano informazioni sensibili su chi siamo, sull'orientamento sessuale, su cosa ci piace fare, e molte di queste informazioni,

più o meno coscientemente, le diamo noi stessi. L'informazione – e per estensione la conoscenza – è da sempre fonte di grande potere. Pensiamo per un attimo a cosa diventerebbe il mondo se la comunicazione diventasse anche solo per poco tempo veramente libera, gratuita e accessibile universalmente. Probabilmente era questa l'intenzione con cui è stato pensato l'intero sistema di cui abbiamo parlato. Ci si può chiedere se l'uomo sia pronto a gestire un'organizzazione anarchica totalmente libertaria, ma al momento attuale c'è uno strumento

importante che va difeso e utilizzato correttamente proprio per conservarlo, migliorarlo e preservarne lo spirito, portando avanti le battaglie contro chi lo sfrutta commettendo reati. Come per molti altri strumenti, il valore risiede nell'uso che si decide di farne.

22 Appartiene alla categoria pet (*Privacy Enhanced Technology*) ed è basato sulla seconda generazione del protocollo di *onion routing*. Il progetto Tor, nato grazie ai finanziamenti dello US Naval Research Laboratory con finalità essenzialmente militari nell'ambito di ricerca delle

comunicazioni protette, è stato un progetto della Electronic Frontier Foundation ed ora è gestito da The Tor Project, un'associazione senza scopo di lucro.

23 Per dirla semplicemente, è un sito nel quale c'è una specie di «interprete» che vi fa navigare nella rete Tor. In tal caso però la garanzia di anonimato è insufficiente, perché state comunque accedendo a quel sito in maniera tradizionale.

24 Per approfondirne i vantaggi, si veda anche l'articolo dedicato da Anonymous all'argomento: http://anon-news.blogspot.it/p/perche-osiris.html

25 Per la Hidden Wiki esistono diversi *mirror*, per essere sicuri che almeno uno sia accessibile.

26 Altri due motori di ricerca, per adesso attivi,

sono: http://zw3crggtadila2sg.onion/torgle/ e http://nstmo7lvh4l32epo.onion/

27 Attualmente mi appare questo link: http://silkroadvb5piz3r.onion/index.php/silkroad/home

28 Su SilkRoad, come su altri siti .onion, potete accedere anche senza installare nessun programma Tor. In questo caso basta andare all'indirizzo http://silkroadvb5piz3r.onion.to (che sfrutta il sito onion.to, una sorta di ponte per visualizzare pagine della rete Tor tramite un normale browser). Attenzione però, perché questa modalità di navigazione non è sicura, e potreste essere facilmente tracciati.

29 Il metodo più «corsaro» è quello di trovare una connessione wireless gratuita e da questa connettersi con un VPN che garantisca

l'anonimato.

30 https://www.torproject.org/docs/tor-hidden-service.html.en

31 La biblioteca di Alessandria venne fondata dalla dinastia greco-egizia dei Tolomei intorno al 300 a.C. Continuò a essere arricchita fino al I sec. a.C.

32 Nel 2012 è andato a Open MRS (http://openmrs.org/) e nel 2011 a GNU Health (http://health.gnu.org/).

33 Il fenomeno mediatico per il quale un tentativo di censurare o rimuovere una notizia provoca esattamente l'effetto opposto, ossia quello di pubblicizzarlo ancor più ampiamente.

3.TRA LIBERTÀ E CENSURA: L'ESEMPIO DELLA PRIMAVERA ARABA

I media e il NetActivism

Rivolte di piazza in regimi autocratici. La caduta di Ben Ali e di Mubarak, la guerra civile in Libia, le sommosse in Bahrein, Siria, Yemen, Giordania e Marocco. Regimi decennali, ingiustizia sociale, corruzione, iniqua distribuzione

della ricchezza, povertà e disoccupazione. Mancanza di libertà. Tutti fattori che hanno oppresso ed esasperato per anni, seppure con modi e tempi diversi, i popoli dell'area nordafricana e mediorientale. E ne hanno scatenato la ribellione. Le prime rivolte hanno fatto da miccia e l'esplosione si è diffusa da Paese a Paese, divenendo la lotta di una piazza lo *starter* per muovere le masse altrove, in un effetto domino in cui la rete e i social media hanno avuto un ruolo chiave. Durante la cosiddetta «Primavera araba» ci ha colpito proprio la velocità di

propagazione della rivolta nei diversi Paesi, dal Nordafrica al Medioriente, un'onda d'urto contagiosa.

Prima ancora del web, un effetto propulsivo l'ha avuto la televisione. Le immagini delle prime rivolte fornite dalle tv satellitari arabe (in particolar modo Al Jazeera[34] e Al Arabiya) sono state d'ispirazione per quei popoli che ancora non avevano scelto di manifestare e ribellarsi, hanno acceso i loro animi e hanno sicuramente contribuito a creare una sorta di coscienza comune tra i vari Paesi, pur con connotazioni diverse a

seconda del contesto.

Ha dichiarato Barbara Serra, giornalista e conduttrice di Al Jazeera English: «La gente non scende in piazza Tahrir perché lo dice la tv, ma è lì perché sa esattamente che qualcosa non funziona nel suo Paese. Stessa cosa in Libia e in Tunisia. Detto ciò, credo che Al Jazeera abbia giocato un ruolo chiave, tant'è vero che sempre in piazza Tahrir, al Cairo, c'era uno schermo enorme che mandava in onda Al Jazeera araba»[35].

Come Al Jazeera anche altre emittenti arabe si sono rivelate decisive nella

diffusione delle rivolte, potendo raggiungere persino le regioni più isolate grazie al satellite. Queste televisioni, sebbene non sempre siano libere da influenze politiche (più o meno evidenti), condividono cultura e lingua dei popoli della zona, e spesso hanno accesso a informazioni e fonti difficili da raggiungere per le televisioni occidentali. Fornendo prospettive diverse da quelle offerte da emittenti straniere come la Cnn o la Bbc, si sono conquistate negli anni anche l'interesse del telespettatore occidentale alla ricerca di una propria

opinione critica e informata.

Uno strumento indispensabile però, non solo per la circolazione di informazioni, immagini, video, ma soprattutto per la collaborazione e il coordinamento delle piazze in rivolta, è stato il web. Come? Tramite le piattaforme di scambio di filmati e immagini, tramite i social network, e non ultimo sfruttando le possibilità che la rete offre di rendere anonima la comunicazione.

Twitter e Facebook hanno sicuramente accelerato la diffusione di

notizie che avrebbero altrimenti impiegato molto tempo prima di «approdare» sui media tradizionali (e forse alcune volte non vi sarebbero arrivate mai). Nel momento in cui una notizia era online, o le immagini su YouTube, i media dovevano per forza «essere sul pezzo». La mole di documenti scritti, audio e video pubblicata in rete è stata enorme.

Le innovazioni tecnologiche nella telecomunicazione sono state così rapide da cogliere impreparati molti regimi rispetto alle effettive conseguenze che

l'uso di tali tecnologie poteva portare. Questa inadeguatezza ha indotto alcuni governi, abituati ad avere il pieno controllo del flusso di informazione, a reagire in modi estremi, spesso ottenendo l'effetto contrario di moltiplicare l'attenzione mediatica su tali Paesi e il sostegno internazionale verso i popoli oppressi.

Le restrizioni sul web e la censura, come limitazioni gravissime della libertà individuale, e la dura repressione esercitata dalle autorità governative, sono andate a unirsi alle altre cause di lotta,

perché, sebbene non si tratti di rivolte di internauti ma di persone comuni, la maggior parte dei ribelli sa che cedere vuol dire chiudere la finestra del mondo sulla protesta, soffocando la voce di tutti.

All'interno del NetActivism (forma di attivismo che sfrutta la tecnologia della comunicazione elettronica), diverse comunità hanno prestato collaborazione alla causa dei popoli in rivolta. Tra queste Avaaz (il cui nome significa all'incirca «il suono che rompe il silenzio»), organizzazione non governativa internazionale nata nel 2007, tra le più

grandi e potenti, che si occupa di attivismo in diversi ambiti, dai cambiamenti climatici globali ai diritti umani, dal problema della povertà ai conflitti sociali, ai diritti degli animali. Avaaz ha espresso solidarietà al popolo egiziano, organizzando campagne di sensibilizzazione e lanciando una petizione online nel gennaio 2011, sostenendone di fatto la lotta per la democrazia.

We Rebuild e Telecomix si sono invece mobilitate principalmente fornendo strumenti per aggirare la

censura e i blocchi di rete offrendo proxy internet anonimi, distribuendo vecchi modem per tentare di superare i blocchi di banda, e creando un database, modificabile dagli utenti, sugli episodi di censura.

Hacker attivisti offrono poi da tutto il mondo la loro esperienza tecnica ai cittadini imprigionati nel sistema di segregazione dovuto alla censura, di filtraggio e sospensione dei servizi.

La comunità Anonymous ha fatto la sua parte nell'ambito della contro-censura, in difesa della libertà di

espressione ha diffuso informazioni compromettenti sui regimi e ha contribuito a diffondere messaggi e consigli pratici ai rivoltosi. In Tunisia e in Egitto, in risposta alle limitazioni di rete, alla censura e al black-out della rete imposto dal regime, il collettivo Anonymous ha oscurato i siti governativi, utilizzandoli talora per veicolare messaggi e immagini. Con videomessaggi online letti da persone che indossano la ormai celebre maschera di Guy Fawkes, gli Anonymous dichiarano guerra ai regimi, ribadendo di essere contro ogni tipo di

censura sulla internet, spronando i cittadini a combattere per la libertà.

La risonanza mediatica

La morte del giovane tunisino Mohamed Bouazizi, conseguenza delle ferite riportate dopo essersi dato fuoco protestando contro le autorità di Tunisi, è stata uno degli eventi simbolo della Primavera araba. Da quel momento le manifestazioni sono cresciute di numero e di forza, fino a portare alla caduta del

presidente Ben Ali e facendo di Mohamed Bouazizi un «martire» della rivoluzione.

I media occidentali hanno dato poca rilevanza a questo evento, il governo tunisino ha sottovalutato la possibilità che potesse essere un innesco, l'inizio di qualcosa di molto più grande, i Paesi vicini non hanno creduto che questa rivolta potesse contagiare l'intera area.

Le informazioni di questa prima fase della ribellione popolare hanno circolato soprattutto via Twitter, che ha svolto il ruolo di diffusore ancora prima che le altre vie di comunicazione svelassero la

portata del momento storico. Anche Facebook ha avuto un certo peso, se pur decisamente minore. Questa comunicazione multimediale si è andata ad aggiungere e non ha sostituito, ovviamente, la rete d'incontri tra le persone nelle piazze, nelle moschee e nei mercati. E questo è avvenuto non solo in Tunisia, ma in tutti i Paesi coinvolti nella Primavera araba.

Il traffico di immagini, video, messaggi ha sfruttato i social network e gli altri canali del web. Dalle piazze in rivolta, immagini e notizie in tempo reale

sono arrivate grazie a telefoni cellulari e satellitari direttamente sul web. Da qui direttamente sui media tradizionali. E indietro, verso le singole persone, magari in un altro Paese, nonostante gli strumenti utilizzati dalla polizia informatica fossero in vigore anche precedentemente agli scontri.

I governi dei Paesi in sommossa hanno iniziato a prendere in seria considerazione l'impatto di tale fenomeno.

Le autorità del Cairo, compresa la portata e il pericolo di destabilizzazione

del regime per questo passaggio velocissimo di informazioni, oltre a esercitare una pesante attività di controllo e repressione, hanno optato per la radicale decisione di spegnere la rete per cinque giorni. Il conseguente blocco delle attività economico-finanziarie, secondo i calcoli dell'Ocse, ha determinato una perdita di circa 13 milioni di euro al giorno, per un totale di circa 65 milioni di euro. Il tentativo di isolamento si è rivelato immediatamente inattuabile e sostanzialmente inutile, le manifestazioni sono proseguite, la gente ha continuato a

comunicare sfruttando telefoni satellitari e linee telefoniche. Agli egiziani sono stati offerti numerosi servizi di *dial-up*, e Google e Twitter hanno proposto un sistema per cui, digitando un numero telefonico, si poteva lasciare un messaggio *voicemail* che in automatico inviava il messaggio su Twitter al tag identificativo #egypt. E Anonymous ha vendicato l'atto bloccando i siti governativi.

In tutti i Paesi interessati dalla Primavera araba la polizia informatica ha rafforzato la sua attività repressiva di controllo. I social network e i blog sono

stati utilizzati essi stessi dalle autorità governative nella gestione del monitoraggio della situazione sociale e nella ricerca dei cyber-attivisti, di cui si sono moltiplicati gli arresti.

Un esempio è il caso di Wael Ghonim, membro del team Google in Medio Oriente e web-attivista della protesta contro Mubarak, arrestato il 28 gennaio 2011 durante le manifestazioni anti-governative al Cairo, tre giorni dopo la prima manifestazione di massa in piazza Tahrir. Ghonim aveva postato da poco sulla pagina Twitter: «*Pray for*

#Egypt. Very worried as it seems that government is planning a war crime tomorrow against people. We are all ready to die #Jan25» («Pregate per l'Egitto. Molto preoccupato perché sembra che per domani il governo stia programmando crimini di guerra contro la popolazione. Siamo pronti a morire, 25 gen.») Il suo arresto è stato reso noto da Amnesty International, allarmando i media per il rischio di maltrattamenti e torture.

Ghonim, inserito dalla rivista «Time» nella lista delle cento persone più influenti del 2011, è diventato un simbolo

della protesta egiziana in qualità di portavoce del Movimento 6 Aprile[36], rispondendo all'esigenza di un movimento apolitico e non ideologico privo di leader di averne uno.

In Siria la stretta censura del regime nell'ambito del controllo delle informazioni esercitato da Assad ha impedito a televisioni satellitari, come Al Jazeera, di fare da cassa di risonanza per le proteste, facendo di siti come YouTube il principale mezzo di condivisione tra la popolazione e di informazione per gli altri Paesi. Nonostante l'oppressiva

censura e i ripetuti blackout del web.

Concludendo, per quanto i regimi abbiano tentato strenuamente di arginare il passaggio di informazioni tra i ribelli e verso il mondo esterno, tra il web e le televisioni si è instaurata una sorta di «risonanza massmediatica» che ha moltiplicato le possibilità di aggirare i controlli governativi e ha dato a queste rivolte (in molti Paesi ancora in corso) la visibilità di cui adesso godono. Il tutto grazie a semplici cittadini che hanno rischiato la vita per denunciare la drammatica realtà che stavano vivendo,

per far circolare le informazioni e ottenere che la repressione non avvenisse nel totale silenzio mediatico e a «porte chiuse». Cittadini che hanno avuto il coraggio di denunciare, per non rimanere segregati.

Sarà molto interessante osservare il ruolo che questi strumenti avranno successivamente, durante la riorganizzazione verso la democratizzazione e la presa di coscienza dei diritti civili, se è vero, come sembra emergere da recenti ricerche, che coloro i quali fanno uso di social media appaiono

«più aperti e tolleranti rispetto alle opinioni di altre persone»[37].

Combattere la censura

Nel 2010, l'organizzazione Reporters sans frontières aveva classificato una serie di Paesi dell'area nordafricana e mediorientale come «nemici di internet». Tra questi, Egitto, Libia, Siria, Tunisia e Arabia Saudita.

Sono «nemici di internet» i Paesi che esercitano, anche in assenza di evidenti

moti insurrezionali, misure pratiche e psicologiche per limitare di fatto la libertà di informazione sul web. Connessioni internet difficoltose, liste crescenti di siti resi inaccessibili, filtraggio dei contenuti (mediante software spesso acquistati dall'Occidente), propaganda online più o meno mascherata, controlli e arresti per i dissidenti, compresi gli attivisti difensori dei diritti umani, persecuzioni e campagne diffamatorie (in alcuni Paesi i gestori di internet cafè sono soggetti a controlli governativi e si assiste a perquisizioni e arresti arbitrari tra la

comunità di blogger e di cyber-attivisti), strategia della paura. I Servizi di sicurezza informatica dei regimi arabi limitano così il flusso di informazioni in entrata e in uscita.

Mappa di Rsf, in occasione della giornata mondiale contro la cyber-censura del 12 marzo 2012

Ogni anno Reporters sans frontières

pubblica un nuovo elenco di «nemici di internet» e di Paesi «sotto sorveglianza».

Quella qui riportata è la mappa più aggiornata reperibile online, risalente al 2012, e riflette un mondo in continua evoluzione: ad esempio, il Bahrein e la Bielorussia sono passati dalla categoria «Paesi sotto sorveglianza» a quella di «nemici di internet». In Bielorussia la sorveglianza e il controllo hanno infatti raggiunto livelli elevatissimi, per i cyber-crimini esiste la possibilità dell'arresto preventivo e il presidente Loukachenko ha imposto dei blocchi al web dopo aver

istituito una black list di siti in continua crescita. Nel Bahrein vige la messa al bando di media stranieri, con arresti e persecuzioni per i cyber-attivisti, per i promotori di diritti civili e della libertà di espressione.

Nel rapporto sui «nemici di internet» di quest'anno, Rsf ha individuato cinque «Paesi nemici», classificati come «Paesi spia», Paesi che alla censura esplicita aggiungono anche una sistematica sorveglianza online, sabotaggi all'accesso, e forme di violazione di alcuni diritti umani fondamentali: Siria, Cina, Iran,

Bahrain e Vietnam.

La Cina rappresenta, com'è noto, il sistema di censura più sofisticato al mondo (non a caso si parla di una vera e propria «grande muraglia digitale»), e sempre più sta intensificando la guerra contro gli strumenti per l'anonimato sulla internet, reclutando servizi privati per tenere sotto controllo gli utenti della internet nel proprio Paese. L'Iran ha portato la sorveglianza elettronica a un livello ancora mai raggiunto, con la creazione di una vera e propria internet nazionale, la «Halal Internet». Per quanto

riguarda la Siria, Rsf ha trovatc documenti che dimostrano come sin dall'inizio la rete sia stata equipaggiata con filtri e strumenti per il monitoraggio elettronico[38].

Per la prima volta Rsf ha incluso nel suo elenco anche cinque aziende «nemiche di internet» (Gamma, Trovicor, Hacking Team, Amesys e Blue Coat): sono i cosiddetti «mercenari digitali» accusati di fiancheggiare i regimi nell'attività censoria e di sorveglianza tramite la fornitura di sofisticate tecnologie.

Secondo Rsf escono dalla lista «Paesi sotto sorveglianza» Venezuela e Libia, ma vi entrano India e Kazakistan, mentre la Thailandia rischia di essere inserita nella lista dei «Paesi nemici».

Durante la Primavera araba i social media sono stati il primo bersaglio delle contromisure informatiche delle autorità governative, che hanno utilizzato gli stessi come strumenti di controspionaggio per scoprire e infiltrarsi nel vivo dei movimenti di protesta, individuare gli attivisti, fare propaganda.

In una prima fase sono stati chiusi alcuni nodi di smistamento (*hub*) della rete telefonica per isolare determinate aree. Nella fase successiva, come già visto, le autorità governative sono giunte allo spegnimento dei server centrali e a veri e propri blackout della rete.

Tuttavia i dissidenti sono riusciti ad aggirare queste restrizioni grazie a sistemi diversi. Per ovviare alla censura chiunque riuscisse ad avere una connessione internet poteva scegliere di fungere da proxy, anche dall'esterno dei confini nazionali, permettendo agli altri Paesi una

connessione temporanea.

C'è stato inoltre un ampio utilizzo di comunicazioni telefoniche e internet via satellite che ha permesso ai rivoltosi di continuare tramite smartphone a utilizzare i social network, per comunicare tra loro e inviare video e resoconti degli scontri di piazza in tutto il mondo.

Esistono alcuni programmi per aggirare i blocchi e le censure permettendo un collegamento internet tramite accesso criptato, pur non garantendo sempre l'accesso a tutti i siti

censurati. Tra questi i più utilizzati sono stati Hotspot Shield, Ultrasurf, Psiphon e Alkasir, e funzionano in modi abbastanza simili.

Hotspot Shield (www.hotspotshield.com/en) crea una VPN, una rete privata virtuale, tra il proprio computer e il VPN server di AnchorFree, produttore del programma.

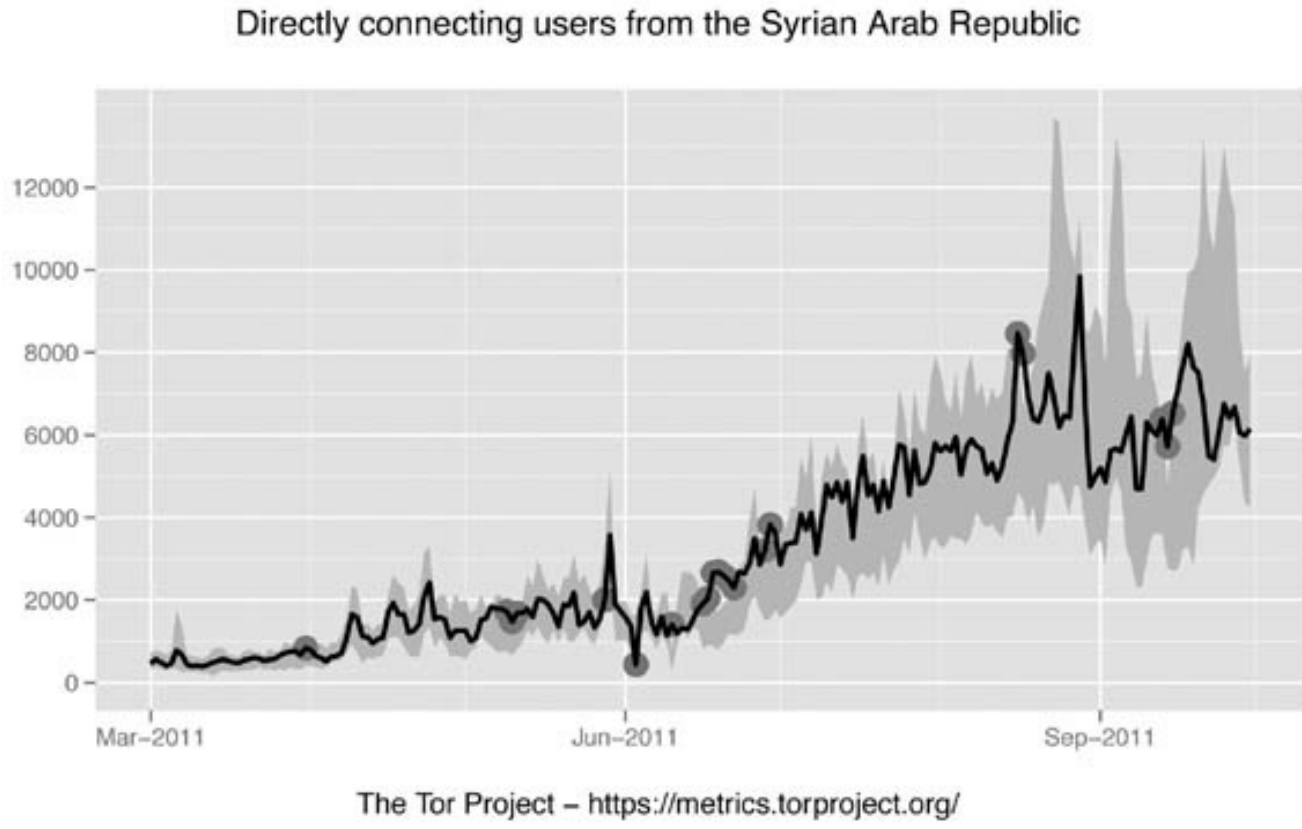
Ultrasurf (https://ultrasurf.us/) è un freeware creato dalla Ultrareach Internet Corporation che permette di aggirare la censura e i blocchi usando un http proxy e protocolli criptati. Fu inizialmente

creato per aiutare i dissidenti cinesi a eludere la censura governativa e la tracciabilità dei propri movimenti online. Ora vanta circa 11 milioni di utilizzatori. Durante gli scontri in Tunisia ha visto gli utenti tunisini aumentare del 700 per cento.

Alkasir (https://alkasir.com), creato dal giornalista e programmatore yemenita Walid al-Saqaf, è molto usato nei Paesi arabi perché ha un'interfaccia sia in inglese sia in lingua araba.

Di Psiphon, invece, abbiamo già parlato in precedenza.

Un altro strumento largamente utilizzato durante le proteste per ovviare al controllo imposto dai regimi è stato, ovviamente, il software Tor. Per capire l'ampiezza con cui è stato utilizzato, basti osservare il grafico seguente, che mostra il numero di utenti direttamente connessi alla rete Tor durante le proteste in Siria.



Utenti direttamente connessi a Tor dalla Siria da marzo 2011 a settembre 2011

Reporters sans frontières, in occasione della Giornata internazionale contro la cyber-censura, ha pubblicato la *Guida pratica del blogger e del cyber-dissidente*, un manuale che spiega come creare e gestire un blog proteggendolo della censura, in

cui tra i vari consigli pratici insegna ad adoperare il software Tor.

Alcuni hacker attivisti tengono spesso dei seminari sull'«alfabetizzazione digitale per insegnare agli attivisti politici l'uso di Tor». Nel prossimo futuro i dissidenti e i blogger sotto regimi che applicano censura e restrizioni potrebbero inoltre sfruttare la tecnologia «Internet in a Suitcase», un progetto sviluppato dalla New America Foundation e finanziato dal Dipartimento della Difesa statunitense (Dod).

Si tratta di un kit facilmente

trasportabile in una piccola valigia che sfrutta la trasmissione GSM per permettere comunicazione e condivisione di dati: un telefono satellitare, un ripetitore wireless per il segnale, un computer portatile, cd e chiavette usb per i drive.

È probabile che alcuni prototipi di «Internet in a Suitcase» e di altri sistemi simili sviluppati dal DoD siano stati forniti a dissidenti in Iran, Siria e Cina.

Una rivoluzione del popolo

Come abbiamo visto, i «nuovi media» e i social network sono stati molto efficaci nel processo di mobilitazione delle masse, nel supporto morale e pratico offerto ai manifestanti e per la mole di informazioni che hanno veicolato, permettendo ad altri media di amplificare le notizie e diffonderle a livello internazionale.

Il loro ruolo nelle rivolte arabe è tuttora argomento di confronto e dibattito. Da una parte viene ricordata la loro indubbia utilità per la popolazione, soprattutto per i giovani, tra i quali è prevedibile che continui a crescere

l'utilizzo degli strumenti offerti dal web. Dall'altro lato, c'è però il rischio che gli stessi strumenti digitali possano essere sfruttati dai regimi autoritari proprio per fini di repressione e propaganda. Una guerra nella guerra, insomma: quanto più le tecnologie si sviluppano tanto più si raffina la strategia per bloccarne l'utilizzo o per trasformarle in una risorsa per il regime.

I media hanno parlato con enfasi di «internet revolution» o di «twitter revolution», con titoli sensazionalistici che sembrano guardare con smisurato

ottimismo al web come alla panacea contro ogni sopruso dei regimi, come la terra promessa, virtuale, in cui si organizza la lotta finale per il riscatto di tutti i popoli. Molto più probabilmente il web è stato un alleato per i popoli in lotta, ma si tratta pur sempre di rivoluzioni popolari.

L'argomento è complesso e occorre analizzarlo da più punti di vista. È vero che internet e social network hanno già cambiato drasticamente la comunicazione e il modo in cui le persone interagiscono tra loro. Ma nei Paesi coinvolti nella

Primavera araba il numero di utenti della internet era piuttosto esiguo e la sua stessa penetrazione non era particolarmente alta. Questo è dimostrato dal fatto che la maggior parte dei contenuti postati sui social network provenivano dalle città principali e da coloro che potevano permettersi uno smartphone, un computer e un collegamento. Cioè da una fascia elitaria della popolazione ricca e alfabetizzata.

Senza dubbio c'è stata una correlazione tra la mobilitazione online e quella di piazza. I social media hanno

«funzionato» assieme a forme più tradizionali di attivismo e mobilitazione. E oltre al ruolo associativo e organizzativo si è aggiunto, come abbiamo visto, quello di «generatore di contenuti in tempo reale», contenuti che le televisioni satellitari rilanciavano poi in tutto il mondo. Da questo punto di vista, l'aspetto più interessante del fenomeno è stato il fatto che la maggior parte delle informazioni e delle immagini che si vedevano scorrere nei tg proveniva dai manifestanti, dalle piazze, e non da inviati esterni. Questo nuovo modello di

comunicazione ha reso possibile avere informazioni – e punti di vista – che altrimenti sarebbe stato impossibile ottenere (a costi, tra l'altro, irrisori per le emittenti).

Molto interessante è l'opinione di Evgenij Morozov, sociologo e giornalista bielorusso, autore del saggio *The Net Delusion: The Dark Side of Internet Freedom*, ed ex-collaboratore di Transitions Online (Tol), organizzazione non governativa che si occupa di sviluppo dei media[39].

Morozov si dichiara scettico nei confronti dell'opinione secondo la quale

internet stia favorendo la reale democratizzazione nei Paesi con regimi autoritari che esercitano uno stretto controllo sulle informazioni, pensiero maturato durante l'esperienza di collaborazione con Transitions Online. La rete può cioè rivelarsi uno strumento potente anche per gli stessi governi, per il controllo sociale e la propaganda. Questo risulta evidente anche osservando le risorse e le energie che i regimi dedicano allo studio delle tecnologie informatiche, all'acquisizione del *know-how* per comprendere i meccanismi alla base della

circolazione delle informazioni sia pubbliche che private. Più sono in grado di padroneggiare gli strumenti informatici, più facilmente possono svolgere al meglio la loro azione politica e repressiva. Questi sistemi di sorveglianza, di censura e, non ultimo, di propaganda sono molto evidenti nei Paesi «nemici di internet» in cui censura e *filtering* limitano di fatto la libertà. La protezione della privacy è falsata poiché le società che la «garantiscono» sono le stesse che vendono ai governi i mezzi informatici per violarla.

Questi governi, infatti, hanno spesso

partecipato al processo di collegamento del loro Paese alla rete globale e hanno investito nella creazione di siti nazionali. Internet è uno strumento lowcost sia per comunicare sia per controllare le comunicazioni, ad esempio analizzando il traffico di email attraverso sistemi di *sniffing*.

Morozov non muove affatto una critica generalizzata a internet, piuttosto vuole mettere in guardia da quello che definisce «cyber-utopismo», nel cui pensiero ottimista potrebbero di fatto essere offuscate alcune criticità come

quelle sopra citate, e dalla fin troppo facile equazione «più tecnologia più democrazia». Inoltre, pur rimanendo la rete e i social network uno strumento potente di divulgazione e diffusione, come è avvenuto nella cosiddetta Primavera araba, analizzare ed elaborare situazioni così complesse esclusivamente sotto la lente potenzialmente distorta della internet («cyber-centrismo»), potrebbe portare a una lettura superficiale o addirittura non corretta della realtà. I mass media occidentali potrebbero dare una lettura dei fatti falsata e giungere a

vedere negli scontri della Primavera araba, in modo semplicistico, una *internet revolution*.

A mio parere, anche senza l'uso del web le rivoluzioni avrebbero avuto luogo comunque, forse non subito, forse con maggiori violenze, sicuramente sarebbero state più lunghe. Certo, i social network hanno coinvolto più velocemente il resto del mondo permettendo a tutti di sapere cosa stava succedendo: Twitter, più di Facebook, nei fatti che hanno coinvolto l'Egitto, ha permesso lo scambio di informazioni trasformandosi in una sorta

di strumento giornalistico: «Twitter ha per la sua natura conquistato un posto indiscusso nell'economia dell'informazione», per citare le parole della giornalista Giovanna Loccatelli[40].

Chiunque può divenire un reporter. Nei Paesi interessati dagli scontri della Primavera araba i social media hanno avuto un effetto moltiplicatore ma non hanno causato la rivoluzione.

«*It's not a Twitter or Facebook revolution... It's an Egyptian revolution*» è anche quanto ha dichiarato Mohamed Nanabhay, 31 anni, origini indiane, nato in Scozia,

cresciuto in Sudafrica, ex-hacker, nel 2011 direttore del sito inglese dell'emittente Al Jazeera. Come già detto, Al Jazeera ha seguito da vicino i recenti eventi del mondo arabo. Alcuni sostengono che l'emittente satellitare che fa base nel Qatar possa aver avuto un ruolo attivo in essi pur dichiarandosi neutrale, anche se su questo aspetto non tutti concordano. Alcuni osservatori credono che Al Jazeera abbia alimentato in qualche modo la rivoluzione, altri che ne abbia alterato alcuni aspetti nel modo in cui ha offerto al mondo i contenuti. È comunque

indiscutibile il ruolo che ha avuto con una copertura degli eventi eccezionale. Torniamo ancora a Mohamed Nanabhay, per evidenziare un aspetto molto interessante che riguarda il modo di dare, e condividere, le informazioni giornalistiche. Il 27 dicembre 2008, iniziò il bombardamento israeliano sulla striscia di Gaza, l'operazione Piombo fuso. Nello stesso momento, negli uffici di Al Jazeera a Doha (Qatar), l'unica emittente tv presente a Gaza, Mohamed Nanabhay stava per prendere una decisione che avrebbe cambiato il modo di condividere

le notizie: Nanabhay propose la sua iniziativa ai vertici dell'azienda: mettere tutto il materiale riguardante il bombardamento online con licenza Creative Commons. Spiega Nanabhay a «Wired»: «La mia posizione era: queste sono notizie, e le notizie non appartengono a nessuno, sono di tutti, di chi è sul terreno sotto le bombe e di chi è lì che le guarda»[41]. Tutti i contenuti della tv – la prima al mondo – sono infatti rilasciati in Creative Commons, disponibili in download, in diretta streaming sul sito, sull'applicazione per

smartphone. Anche questo ha avuto un peso.

Guardando ancora una volta il quadro nel suo insieme: il web ha rappresentato, anche prima degli scontri di piazza, uno spazio alternativo in cui la gente ha potuto parlare e discutere di cose non permesse dai regimi, grazie all'anonimato. È stato un fattore chiave nell'organizzazione, una piattaforma per chiamare gente alla rivolta. E ancora un luogo dove scambiarsi informazioni e consigli per ingannare le forze di polizia, la censura, ecc. Il web ha costretto i media

tradizionali a dare a loro volta le notizie e a passare le immagini che sono così arrivate in tutto il resto del mondo. E il resto del mondo non può rimanere indifferente. Le associazioni per la difesa dei diritti umani, frequentemente con sede nei Paesi occidentali i cui governi hanno appoggiato i regimi che il popolo sta cercando di abbattere, contribuiscono sia sensibilizzando l'opinione pubblica in luoghi lontani da dove si verificano gli scontri di piazza, sia educando alla consapevolezza dei propri diritti i popoli in difficoltà, così che, dopo gli scontri, la

ricostruzione e la riorganizzazione possano fondarsi anche sulla cultura dei diritti umani.

Democrazia in democrazia

Io vivo in un Paese democratico e ho la percezione di essere libero (per così dire). Ma internet, la realtà in cui «vivo» per molte ore al giorno, si sta veramente sviluppando in modo democratico? Mentre scrivo, censura e controllo sul web sono esercitati in una lunga lista di

Paesi. Mi tranquillizza pensare che vivo fortunatamente in una democrazia occidentale? Se ci penso bene neanche tanto. E se domani le mie informazioni, tutto quello che di mio è passato sui social media, venisse usato per il controllo, la censura, la repressione governativa? Chi mi garantisce che le aziende che gestiscono tali servizi non siano pronte a vendere tutti i miei dati al miglior offerente? Facebook e Google che rapporti hanno con agenzie ed enti statali?

Il fatto che l'iscrizione a un servizio o

a un social network sia «gratis» spesso dà all'utente la sensazione di trovarsi in uno spazio libero, mentre in realtà la piattaforma appartiene comunque a un privato, a qualcuno con cui si è stipulato un contratto. Quando si utilizzano strumenti come un social network si ha l'illusione di usufruirne gratuitamente, in realtà il prezzo che si paga è ben alto: si rinuncia di fatto a una parte della propria privacy, si subisce la pubblicità, si regalano informazioni che potrebbero magari un domani essere utilizzate per fini che non conosciamo ancora.

In effetti anche sotto i governi definiti democratici il pericolo di permettere ad altri di invadere la propria sfera personale è poco percepito.

Ciò che è accaduto nei Paesi della Primavera araba ci dovrebbe portare a riflettere sul potere del web, sull'utilizzo che le parti possono farne, sulla privacy che dovremmo proteggere e sulla necessità di lottare ad armi pari sul terreno del flusso delle informazioni. Il web si è dimostrato un potente mezzo di informazione e divulgazione che, come abbiamo visto, può trasformarsi nelle

mani di un regime in un altrettanto potente strumento di persecuzione. In molti Paesi la pressione della censura è divenuta molto forte. Ma recentemente anche nei Paesi «democratici» sono aumentate le censure sotto la bandiera della pubblica sicurezza o della difesa dei diritti d'autore.

Che la libertà del web sia in pericolo lo pensano in molti. Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn e Jèrèmie Zimmermann hanno fatto il punto sullo stato attuale delle cose nel libro *Cypherpunks, freedom and the future o*

the Internet[42].

Come sottolineano gli autori, l'utilizzo della internet, a qualsiasi livello, espone potenzialmente ciascuno degli utenti a un rischio quando da strumento di comunicazione si trasforma in strumento di controllo. E perché ci sia controllo non è necessario vivere sotto un regime. Parte della libertà di cui si godeva sulla internet nei decenni scorsi è ormai un ricordo. Continuamente il cyber-utente viene tracciato e semina un numero enorme di informazioni personali. Lo smartphone di oggi, a detta

di Assange, sarebbe «un *device* di tracciamento che fa anche telefonate».

Sta, molto semplicemente, aumentando la sorveglianza digitale esercitata dai governi «democratici». Una sorveglianza che non si manifesta in modo palese, una sorta di «sorveglianza strategica» che accumula una mole incredibile di dati sensibili, i nostri: chi siamo, dove ci spostiamo, cosa ci piace, cosa pensiamo. Cediamo la proprietà intellettuale delle nostre immagini e delle nostre vite. E l'aumento del controllo è la strada intrapresa da molti governi, spesso

in accordo con le *corporations*. Invece resta a livelli bassissimi la consapevolezza degli utenti e la stessa conoscenza di base degli strumenti che utilizzano quotidianamente. Questo è ciò che abbiamo accettato. Ma forse questo è il momento per riscrivere le regole.

La soluzione proposta nel libro citato è quella che appartiene da sempre alla filosofia cypherpunk: crittografia dei linguaggi informatici che permettono l'anonimato, software libero e peer to peer. Ma ciò che occorre, per prima cosa, è l'acquisizione della consapevolezza che

un problema c'è. La libertà e la democrazia sulla internet sono una necessità e un diritto, così come il rispetto della privacy; e tutti, dagli hacker ai semplici utenti, dovrebbero reagire.

Nel suo libro *Consent of the Networked The Worldwide Struggle for Internet Freedom*, Rebecca MacKinnon fa riflettere il cittadino della internet su cosa sia realmente accettabile e lo spinge a lottare per i propri diritti nel mondo virtuale così come in quello reale.

Spesso come utenti di un servizio non abbiamo la capacità di controllare in

modo critico e responsabile che coloro ai quali accordiamo la nostra fiducia stiano davvero operando come dovrebbero. Chi ha conoscenza ha potere, e occorre monitorare costantemente affinché non vi siano abusi.

Francamente, l'esistenza di uno spazio in cui ci si possa muovere anonimamente mi rassicura. Non si sa mai.

34 Al Jazeera nasce nel 1996, è stato il primo canale del mondo arabo a fornire notizie 24 ore su 24, con notiziari, dibattiti e interventi in

diretta. Il fondatore, Hamad bin Khalifa al-Thani, emiro del Qatar, ha fatto un investimento rivelatosi molto redditizio, nel desiderio di trasformare il suo Paese nel centro culturale della regione e ottenere maggiore importanza nel panorama politico.

35 http://www.meridianionline.org/2011/10/09/al-jazeera-ha-giocato-ruolo-chiave-intervista-barbara-serra/

36 Il movimento giovanile egiziano, nato nel 2008, che ha portato alla caduta di Mubarak.

37 Dall'ultimo *Arab Social Media Report*, diffuso dalla Dubai School of Government.

38 http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html

39 Fondata nel 1999, Tol è un'organizzazione di sviluppo dei media (*media development organization*), con un suo giornale online, che si occupa di news ed eventi nella macro-zona dei 29 Paesi post-comunisti dell'Europa dell'Est, dell'Europa Centrale, del sud-est europeo, della Russia, dei Paesi Balcanici, della zona del Caucaso e dell'Asia Centrale. Evgenij Morozov è intervenuto come speaker della Conferenza Ted nel 2009 analizzando i modi attraverso i quali il web influenza l'impegno civico e la stabilità politica dei regimi nelle società autoritarie e chiuse, o nei Paesi «in transizione». Nel novembre 2011 ha tenuto una Lectio magistralis al Festival della Scienza di Genova dal titolo *L'ingenuità della Rete. Perché Twitter non può scatenare una rivoluzione*, affrontando i temi del suo primo saggio, *The Net Delusion*, pubblicato nel 2011.

40 http://twitter.com/gioloc28

41
http://tv.wired.it/news/2011/04/06/mohamednanabhay-con-creative-commons-ho-rivoluzionato-al-jazeera.html

42
http://daily.wired.it/news/internet/2012/12/07assange-cypherpunks-wikileaks-323446.html

GLOSSARIO

Browser: è un programma che consente di usufruire dei servizi di connettività in rete e di navigare sul World Wide Web, appoggiandosi sui protocolli di rete forniti dal sistema operativo (a partire da quelli di livello applicativo come HTTP, FTP, ecc.) attraverso opportune API (*Application Programming Interface*), permettendo di

visualizzare i contenuti delle pagine dei siti web, specificandone l'URL, e di interagire con essi.

CPU (Central Processing Unit): è l'unità centrale di elaborazione di un computer (detta anche processore centrale) e ne rappresenta uno dei componenti principali. È una tipologia di processore digitale *general purpose* che si contraddistingue per sovrintendere a tutte le funzionalità del computer basate sull'architettura di von Neumann o

sull'architettura Harvard. Al circuito integrato della CPU è affidato il compito di leggere i dati in memoria, di elaborare le istruzioni e i calcoli matematici, di organizzare i flussi di dati da e verso dispositivi esterni. La sua velocità di calcolo si misura in MHZ, ed è uno dei principali fattori che determinano la velocità di esecuzione dei programmi.

DoS: nella sicurezza informatica DoS (scritto con la maiuscola al primo e terzo posto) è la sigla di Denial of Service

letteralmente: «negazione del servizio». Si tratta di un malfunzionamento dovuto a un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, ad esempio un sito web, fino a renderlo non più in grado di operare.

Fiat money: la *fiat money* nasce nel 1971 quando il presidente americano Nixon decise che il dollaro, prima ancorato all'oro (*gold standard*), dovesse abbandonare la convertibilità.

GNU: è un sistema operativo distribuito come software libero. Il progetto GNU supporta la missione della Free Software Foundation di preservare, proteggere e promuovere la libertà di utilizzare, studiare, copiare, modificare e distribuire software e di difendere i diritti di chi usa software liberi.

GPU (Graphics Processing Unit): l'unità di elaborazione grafica o unità di elaborazione visiva (comunemente abbreviata in VPU), è una tipologia

particolare di coprocessore che si contraddistingue per essere specializzata nel *rendering* di immagini grafiche. Il suo tipico utilizzo è come co-processore della CPU e da alcuni anni viene anche utilizzata in generiche elaborazioni dati.

Hash: una funzione crittografica di *hash* trasforma dei dati di lunghezza arbitraria (un messaggio) in una stringa di dimensione fissa chiamata «valore di *hash*», «impronta del messaggio» o «somma di controllo». Le applicazioni

pratiche dello *hash* includono i controlli sull'integrità dei dati mediante somme di controllo, le firme digitali semplici, l'autenticazione e varie applicazioni nella sicurezza informatica.

Header: nella commutazione di pacchetto, viene denominata *header* quella parte del pacchetto, o più in generale della PDU, che contiene informazioni di controllo necessarie al funzionamento della rete, cioè le informazioni di protocollo (PCI) aggiunte di strato in

strato, in opposizione al carico pagante (SDU), ovvero ai dati utili che vengono trasportati tra gli utilizzatori della rete.

Hosting: in informatica si definisce *hosting* (dall'inglese *to host*, «ospitare») un servizio di rete che consiste nell'allocare su un server le pagine di un sito web, rendendolo così accessibile dalla rete internet e ai suoi utenti.

Hub: in informatica, nelle telecomunicazioni, nella tecnologia delle reti informatiche, un *hub* (dall'inglese

«fulcro», «mozzo», «elemento centrale») rappresenta un concentratore, ovvero un dispositivo di rete che funge da nodo di smistamento dati di una rete, organizzata prevalentemente con una tipologia a stella.

Escrow: è il cosiddetto «acconto di garanzia», molto utilizzato nelle transazioni via internet tra Paesi distanti tra loro. Un acconto di garanzia è un accordo legale nel quale un bene (denaro o qualunque bene tangibile) è depositato

sul conto di una terza parte neutrale (agente), fino all'adempimento delle clausole contrattuali dell'altra parte. All'adempimento delle clausole, l'agente consegnerà alla seconda parte il bene depositato.

Extranet: è l'estensione di una rete privata (intranet, o LAN) che permette anche a soggetti non operanti all'interno della suddetta rete di accedere a informazioni, servizi e consultare o immettere dati. Ad esempio, per

un'azienda dotata di una rete intranet, essa rappresenta il sistema di comunicazione pubblico che consente la condivisione sicura di dati e informazioni con clienti, soci, fornitori, partner commerciali. Le sue caratteristiche sono dunque simili a quelle della rete intranet, ma può essere estesa anche a utenti esterni (sono previste forme di autenticazione utente e di sicurezza nello scambio dei dati).

IP (Internet Protocol address): un

indirizzo IP è un'etichetta numerica che identifica univocamente un dispositivo (*host*) collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di comunicazione. Un indirizzo IP assolve essenzialmente a due funzioni: identificare un dispositivo sulla rete e fornirne il percorso per la sua raggiungibilità da un altro terminale o dispositivo di rete in una comunicazione dati a pacchetto.

Lindendollar: Il Dollaro Linden, o

Linden Dollar, è la moneta di scambio usata nell'economia del mondo virtuale di Second Life. Con i Dollari Linden in Second Life si possono acquistare e vendere terreni e oggetti; in seguito possono essere riconvertiti in denaro reale. Alcune persone si sono arricchite costruendo e vendendo oggetti nel mondo virtuale di Second Life.

Message digest: l'acronimo MD5 (Message Digest algorithm 5) indica un algoritmo crittografico di *hashing*

realizzato da Ronald Rivest nel 1991 e standardizzato con la RFC 1321. Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit. La codifica avviene molto velocemente e l'output (noto anche come «MD5 Checksum» o «MD5 Hash») restituito è tale per cui è altamente improbabile ottenere con due diverse stringhe in input uno stesso valore hash in output. A oggi sono disponibili molte risorse online che riescono a decriptarla in pochi secondi.

Mining: indica l'attività di generazione di bitcoin, in analogia al *gold minig* («estrazione dell'oro»).

Nonce: in crittografia il termine *nonce* indica un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico. *Nonce* è infatti la contrazione delle parole inglesi *number used once*, che significano appunto «numero usato solo una volta».

Open source: in informatica, indica un software i cui autori (più precisamente

i detentori dei diritti) ne permettono, anzi ne favoriscono il libero studio e l'apporto di modifiche da parte di altri programmatori indipendenti. Ciò è possibile mediante l'applicazione di apposite licenze d'uso. Il fenomeno ha tratto grande beneficio dalla internet, perché esso permette a programmatori geograficamente distanti di coordinarsi e lavorare allo stesso progetto.

Peer to peer: abbreviato in p2p, letteralmente significa «da pari a pari», è

un modello di comunicazione nel quale ciascuna delle parti ha le stesse funzionalità e può iniziare la sessione di comunicazione. In alcuni casi, la comunicazione p2p viene implementata dando a ognuno dei nodi di comunicazione le funzionalità sia di server che di client. È un modello dunque radicalmente opposto a quelli basati sul rapporto *server/client* o *master/slave*. Nel linguaggio corrente l'espressione «peer to peer» viene usata per descrivere le applicazioni con le quali gli utenti

possono, attraverso internet, scambiare direttamente file con altri utenti. In particolare, per quanto riguarda proprio internet, il p2p è una tipologia di network che permette alle persone che utilizzano lo stesso tipo di programma di connettersi e accedere direttamente alle risorse condivise. Napster, Gnutella, Kazaa, eMule ne sono gli esempi più noti e utilizzati.

Provider: è il termine più comunemente usato per indicare un ISP, o

Internet Service Provider («fornitore di servizi internet»). È una struttura commerciale o un'organizzazione che offre agli utenti (residenziali o imprese), dietro la stipulazione di un contratto di fornitura, servizi inerenti alla internet, i principali dei quali sono l'accesso alla rete, la posta elettronica, gli spazi web personali.

Riserva frazionaria bancaria: è la percentuale dei depositi bancari che per legge la banca è tenuta a detenere sotto

forma di contanti o di attività facilmente liquidabili. Attraverso la pratica del «fractional reserve banking» (della «riserva frazionaria bancaria »), il denaro vero si trasforma in credito e si moltiplica, in forma di prestiti o di fondi, secondo uno schema da molti ritenuto dannoso.

Schema Ponzi piramidale: spesso confuso con il marketing piramidale o il marketing multilivello, uno schema Ponzi piramidale è un modello economico di vendita che promette forti guadagni a

patto che le parti coinvolte reclutino nuovi «investitori», a loro volta vittime di quella che può considerarsi una truffa.

Server/client: un sistema *server-client* (letteralmente «servente/cliente») è un'architettura di rete nella quale un computer client istanzia l'interfaccia utente di un'applicazione connettendosi a una *server application* o a un sistema di database. Più semplicemente, i sistemi *server-client* sono un'evoluzione dei sistemi basati sulla condivisione semplice delle

risorse.

Sniffing: si definisce *sniffing* (dall'inglese, «odorare»), in informatica e nelle telecomunicazioni, l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password

o altre informazioni sensibili).

VPN (Virtual Private Network): reti virtuali private chiamate anche «extranet» (vedi relativa voce del glossario).

Ringrazio Fabrizio Ruggirello per la fiducia accordata

e Michela Carpi per la pazienza

collana le stelle

Alicia Steimberg, *Musica e orologi*

Federica Tuzi, *Non ci lasceremo mai*

Principessa Saffo, *Il tutù*

Peter Weissman, *Penso, dunque chi sono? Memorie di un anno psichedelico*

Stig Dalager, *Quei due giorni di luglio*

Gretelise Holm, *Spiriti ribelli*

Maurizio Cotrona, *Malafede*

Marie-Hélène Ferrari, *Il destino non*

c'entra. Le inchieste del commissario Pierucci

Marco Bigi, *Sei bellissima*

Giovanni Dozzini, *L'uomo che manca*

Patrick Modiano, *Riduzione di pena*

Tarif Khalidi (a cura di), *Un musulmano di nome Gesù*

Janina Katz, *Desiderio su ordinazione*

Lü Tiancheng, *Il copriletto intrecciato di storie segrete*

Stig Dalager, *Il libro di David*

Jerzy Pilch, *L'amante in carica*

Lucette Destouches,Véronique Robert, *Céline segreto*

Marco Di Porto, *Nessuna notte è infinita*

Patrick Modiano, *Fiori di rovina*

Gretelise Holm, *Bastarde*

Rafael Argullol, *Lampedusa*

Erskine Childers, *L'enigma delle sabbie*

Tom Antongini, *Vita segreta di Gabriele d'Annunzio. Parte prima*

collana il raggio verde

Charles Stanley Nott, *Insegnamenti di Gurdjieff. Diario di un allievo*

Migi Autore (a cura di), *Le dieci icone del bue*

collana lantana.doc (libro e dvd)

Una storia da ridere. Breve biografia di Mario Monicelli

Il secolo lungo. Breve biografia di Margherita Hack

collana lantana
jr

Colin Thompson, *I Floods 1. Vicini di casa*

Colin Thompson, *I Floods 2. A scuola di magia*

Colin Thompson, *I Floods 3. Il mondo è casa nostra!*

Colin Thompson, *I Floods 4. Ossi duri*

Colin Thompson, *I Floods 5. Sotto accusa*

Colin Thompson, *I Floods 6. Un mare di guai*

fuori collana

Patricia Mazy, *Mirabelle, cane marinaio*

Massimo Duranti (a cura di), *Dottori futurista. Sei opere «riscoperte» degli anni romani*