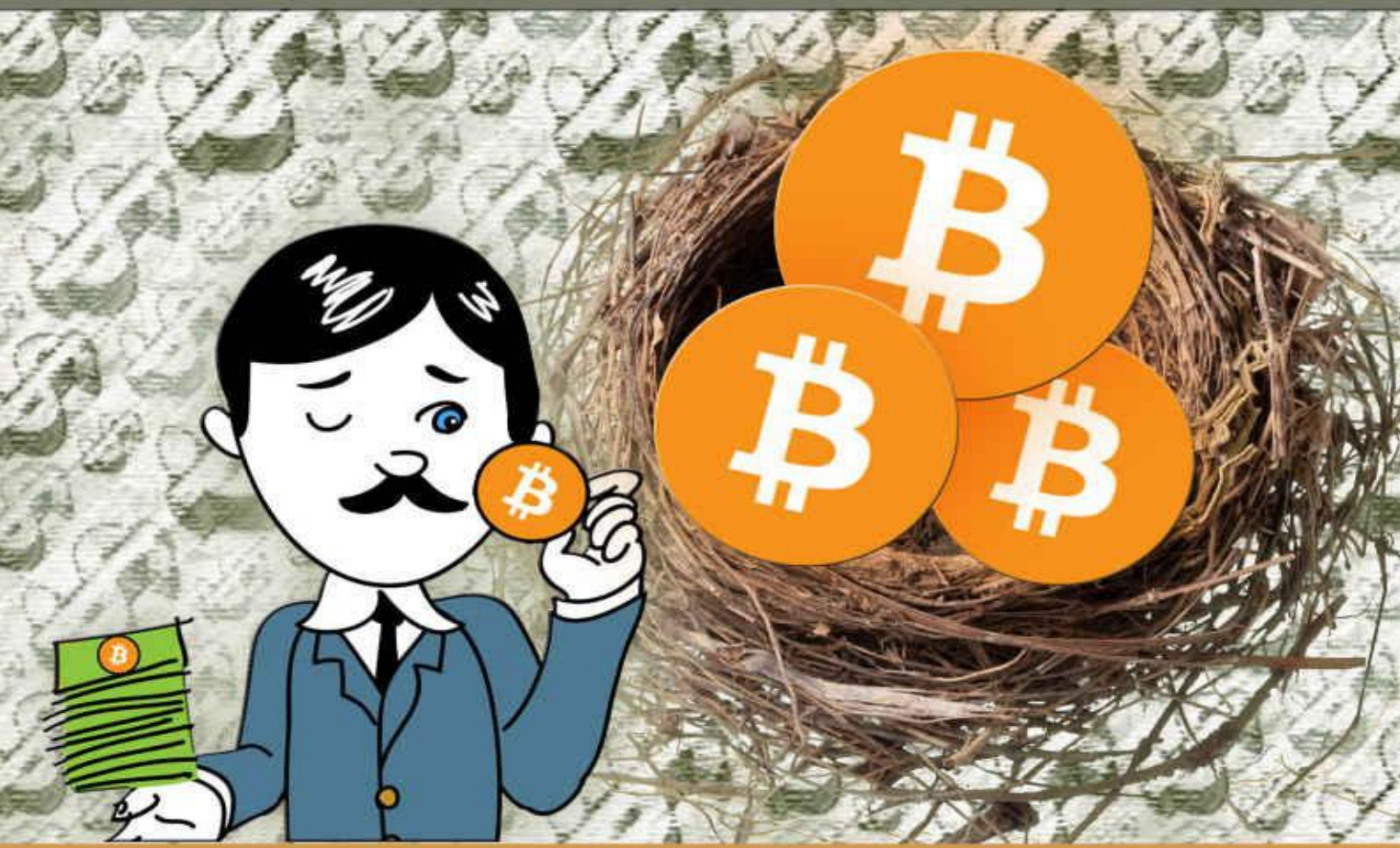
COME GUADAGNARE & GESTIRE BITCOIN



COME GUADAGNARE E GESTIRE BITCOIN

A.Bersia, G. Silano

INTRODUZIONE

Se stai leggendo questo e-book è perché hai intuito, o vuoi approfondire, le grandi potenzialità del mondo Bitcoin, e sei interessato a sfruttare in modo professionale la criptovaluta, operando ad un livello avanzato con la moneta elettronica.

L'e-book è stato attentamente studiato per essere la guida di riferimento, con un linguaggio chiaro e comprensibile, analizzando i migliori metodi per guadagnare, gestire e trarre vantaggio dai bitcoin. A questa trattazione pragmatica segue costantemente l'interpretazione del

contesto economico ed informatico che si fonde inevitabilmente con il mondo Bitcoin.

Gli autori hanno esperienza consolidata, e lavorano nel campo informatico e nel mondo dell'economia reale, binomio che è prerogativa essenziale per comprendere ed operare con una valuta digitale. Infatti, soltanto unendo nozioni economiche con strumenti informatici è stato possibile creare strategie e sviluppare sistemi per operare in questo business.

Con quest'opera saranno forniti gli strumenti per comprendere la fusione di questi due mondi. L'intento è quello di accompagnare il lettore nell'ottenere

una comprensione totale del fenomeno, con il fine ultimo di essere competitivo nell'utilizzo dei bitcoin, per arrivare a guadagnare, speculare, e gestire al meglio le proprie operazioni di compravendita con la valuta digitale, e creare un proprio business.

Gli autori hanno deciso di abbracciare una struttura simile alle pubblicazioni anglosassoni, le quali partendo dal mondo pragmatico e del "fare" giungono a spiegare la teoria sottostante. Ed è questa la chiave di lettura con cui si vuole accompagnare il lettore: nessuna superflua speculazione teorica, troppo spesso presente nel mondo accademico, ma concetti ed

esempi concreti, accompagnati da procedure sperimentate dagli autori.

L'e-book non lascia scoperto nessun argomento necessario per operare con la criptovaluta, ogni capitolo è stato strutturato per essere un tassello irrinunciabile alla conoscenza del mondo Bitcoin. Inoltre, siccome gli autori si rivolgono anche a lettori con conoscenze avanzate sul fenomeno, l'intera opera è composta in modo tale che gli argomenti siano efficacemente suddivisi in macro-aree, permettendo agevolmente di giungere direttamente ai capitoli più complicati e d'approfondimento.

Gli autori hanno riflettuto a

lungo per realizzare la migliore struttura possibile, che permetta al lettore una reale comprensione del fenomeno per poter operare concretamente, guadagnare, speculare e sfruttare i bitcoin a proprio vantaggio.

Gli autori hanno ritenuto necessario strutturare l'e-book come segue:

- In principio, verranno analizzate le implicazioni di carattere economico del protocollo Bitcoin. Troppo frequentemente si tende a sorvolare sulle nozioni economiche alla base di questa valuta digitale. Invero, comprenderle e sfruttarle, è l'unico

modo per poter speculare e quindi guadagnare grandi cifre, come già avvenuto nei casi celebri. Il lettore quindi scoprirà perché il valore dei bitcoin è aumentato considerevolmente, e cosa c'è da aspettarsi nello scenario economico futuro. In questa prima parte verranno evidenziati anche quali sono i reali vantaggi operativi dei bitcoin nelle transazioni di compravendita, e perché molte aziende, tra cui Microsoft, hanno già deciso di abbracciarla come forma di pagamento riconosciuta. Sarà accennata anche l'enorme vastità di beni, legali e non, acquistabili tramite bitcoin sul web.

2. In parole semplici quanto efficaci verrà spiegato il funzionamento del protocollo Bitcoin e le possibili remunerazioni derivanti dall'attività di *mining*. Non temete! Nessuna spiegazione noiosa o prolissa, il fine è rigorosamente quello di far capire ai lettori il funzionamento della cyber-moneta, in modo da poter operare con essa. Gli autori preferiscono lasciare le spiegazioni lunghe e fini a sé stesse ad altre pubblicazioni.

3. Conseguentemente, verrà sintetizzato lo studio degli autori riguardante il

portafoglio bitcoin (strumento di gestione degli stessi). Sulla base di quanto trattato il lettore sarà guidato verso la scelta migliore, con un occhio di riguardo alla sicurezza grazie ai backup ed i metodi di criptazione. Operazioni fondamentali per non avere "brutte sorprese" in seguito.

4. Comprese queste nozioni, si entrerà nel vivo dell'argomento "come guadagnare bitcoin", analizzando diverse metodologie, tra le quali il lettore potrà scegliere le più adatte alle sue esigenze e alle sue strategie. Ogni categoria è stata studiata

approfonditamente.

5. Una particolare attenzione sarà riservata ad un modello matematico basato su principi statistici, volto ad moltiplicare i profitti in bitcoin. Proprio a tal fine, il lettore potrà beneficiare di applicativi *ad hoc* in esclusiva per quest'opera.

6. Verranno trattati alcuni metodi per convertire i bitcoin guadagnati in moneta a corso legale (euro, dollari), ed il viceversa. Inoltre, sarà mostrato che è possibile sfruttare i bitcoin anche non avendone in portafoglio, potendo effettuare pagamenti in

bitcoin tramite euro, grazie ad appositi servizi.

7. In ultimo, gli autori proporranno delle conclusioni sul futuro di questa valuta e cosa attenderci, sempre al fine di ottenere il massimo profitto. L'attenzione sarà anche rivolta ad altre monete matematiche che si sono diffuse conseguentemente al successo dei bitcoin, spiegando come queste siano collegate ai bitcoin stessi.

Buona lettura.

3 Giugno 2015

Dopo 1 anno e 9 mesi dalla pubblicazione di questo e-Book, il valore di un bitcoin è aumentato da $225 (valore di riferimento alla pubblicazione) ad oltre $1'000.

Auguriamo a tutti i lettori di aver beneficiato delle informazioni contenute in quest'opera, che si sono dimostrate assolutamente esplicative del mondo Bitcoin e dell'incredibile trend rialzista che ha seguito la pubblicazione di "Come Guadagnare e Gestire Bitcoin".

Cogliamo l'occasione per ringraziare i nostri lettori per le numerossisime e-

mail di apprezzamento.

Per tutti i nuovi lettori, quest'opera vi permetterà di comprendere il mondo Bitcoin e la Blockchain Technology sottostante.

Marzo 2017

CAPITOLO 1.

BITCOIN ED ECONOMIA: COSA C'È SOTTO

Non avrebbe alcun senso parlare di bitcoin, e strumenti ad essi associati, senza prima analizzare le implicazioni economiche.

In questo capitolo si indagherà sul perché nel mondo Bitcoin non esiste l'inflazione, e quali vantaggi operativi si ottengono utilizzandoli nella compravendita di merci reali. Verrà analizzato l'incremento straordinario di valore dei bitcoin sull'euro negli ultimi anni e come sia stato possibile, per molte persone, diventare milionari

grazie ad essi. L'indagine continuerà quindi al mercato di beni, legali e non, in vendita sul web proprio mediante bitcoin.

1.1. BITCOIN ED INFLAZIONE

Uno degli aspetti più peculiari dei Bitcoin è sicuramente legato all'inflazione. E' fondamentale capire questa implicazione, e le differenze con la moneta a corso legale con cui ogni giorno i lettori operano (euro, dollari, franchi, ...).

Il sistema economico contemporaneo è caratterizzato da un tasso di inflazione fisiologico, dovuto al fatto che la banca centrale – in questo esempio si parla dell'area euro e quindi Banca Centrale Europea – emette liquidità (moneta) in accordo con i cicli

economici, operazione che in gergo tecnico è chiamata *quantitative easing*.

Lasciando da parte i tecnicismi, è ragionevole aspettarsi che 100 euro nominali oggi abbiano più valore di 100 euro nominali tra un anno. Anche i lettori a digiuno di nozioni economiche possono facilmente intuire, con le dovute semplificazioni, che se la quantità nominale di moneta in circolazione cresce, e come visto la Banca Centrale Europea crea nuova moneta, il valore di un singolo euro si svaluta. Quindi, per comprare lo stesso bene tra un anno, occorrerà una quantità di euro superiore. Tale percentuale incrementale è definita, appunto,

inflazione.

Questa è, intuitivamente, la ragione per cui imprese e famiglie cercano di conservare i valore reali dei loro risparmi, investendo i propri soldi in titoli o altre attività, nella speranza di ottenere un interesse almeno pari al tasso d'inflazione e di mantenere lo stesso potere d'acquisto.

Sull'inflazione politici ed economisti spendono normalmente fiumi di parole, ognuno con opinioni e "rimedi" differenti. Lo scopo di questo capitolo esula dall'addentrarsi nel cuore della teoria economica, tuttavia gli autori hanno ritenuto opportuno, a beneficio dei lettori, riassumere alcuni

principi importanti inerenti al mondo dei Bitcoin. Se è vero che avere il controllo della politica monetaria può mitigare i periodi più duri di recessione e di disoccupazione, ogni persona sa bene, facendo i conti nel suo portafoglio, quanto gli effetti dell'inflazione siano disastrosi per il potere d'acquisto, che viene eroso anno dopo anno.

Inoltre, tutte le monete a corso legale (dollaro, franco, yen, …) sono accomunate dal fatto che esistono enti sovraordinati con lo scopo di controllarne quantità, tassi d'interesse, livello di inflazione. Nell'area euro, come visto, è la Banca Centrale Europea. Per il dollaro, la Federal

Reserve, e così via.

1.2. LA RIVOLUZIONE BITCOIN

Il protocollo Bitcoin, per sua natura stessa (Capitolo 2), non è affetto da questo problema. Al contrario, il numero di bitcoin è stabilito grazie ai suoi algoritmi e non può essere incrementato da nessun organismo di controllo esterno.

È stato toccato un punto saliente per la comprensione del mondo Bitcoin, ossia l'assoluta mancanza di controllo e di enti sovrastanti. In altre parole, non c'è nessun ente che può emettere bitcoin in accordo con i cicli economici e i livelli d'occupazione, creando

inflazione e, conseguentemente, perdita d'acquisto della moneta.

In seguito verrà analizzato come questo si ripercuote sulle transazioni e sulle preferenze dei venditori/compratori. In questa sede agli autori preme sottolineare e fissare il seguente concetto: dato un numero fisso di bitcoin disponibili, all'aumentare degli utilizzatori e delle transazioni, il valore degli stessi è destinato ad aumentare! In aggiunta, anche i bitcoin smarriti concorrono ad aumentare il valore dei bitcoin rimasti in circolazione (Tabella 1).

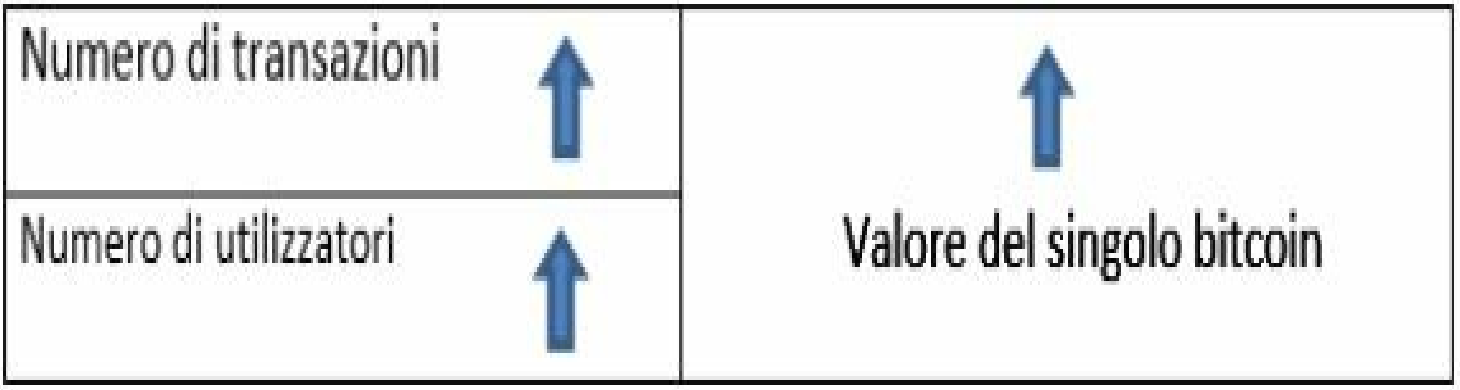


Tabella 1: Aumento del valore dei bitcoin.

Vale la pena soffermarsi su questo fondamentale concetto. Immaginate che Aldo, alla fine del 2010, avesse in portafoglio 100 bitcoin. In una economia reale, di norma, dopo 5 anni 100 euro valgono di meno. Di meno quanto? Il tasso di inflazione *r*, appunto, in questo caso su base quinquennale. Nell'economia dei bitcoin invece, l'inflazione non esiste, e non considerando momentaneamente

variazioni dovute alla speculazione, *il valore di 1 bitcoin è destinato ad aumentare nel tempo se le transazioni e gli utenti che utilizzano questa valuta aumentano*.

In questo esempio, Aldo, con 100 bitcoin alla fine del 2010, equivalenti all'epoca a circa 26€, si troverebbe all'inizio del 2015 con un controvalore di circa 27'685€.
In altre parole, il tasso di cambio è passato da 1BTC=0.3$ a fine 2010, a 1BTC=313.92$ a inizio 2015. Un incremento del 104'641% (per dare l'idea dei termini di grandezza, stiamo parlando di un incremento di oltre mille volte l'investimento iniziale!). Ecco

spiegato come, grazie ai bitcoin, siano nati nuovi milionari.

Aldo rappresenta un esempio di fantasia, ma ben poco di immaginario hanno gli 11 milioni di dollari accumulati dai gemelli Winklevoss, noti come i primi statunitensi ad essere entrati nel club dei “milionari bitcoin”, investendo nella criptovaluta ai suoi albori.

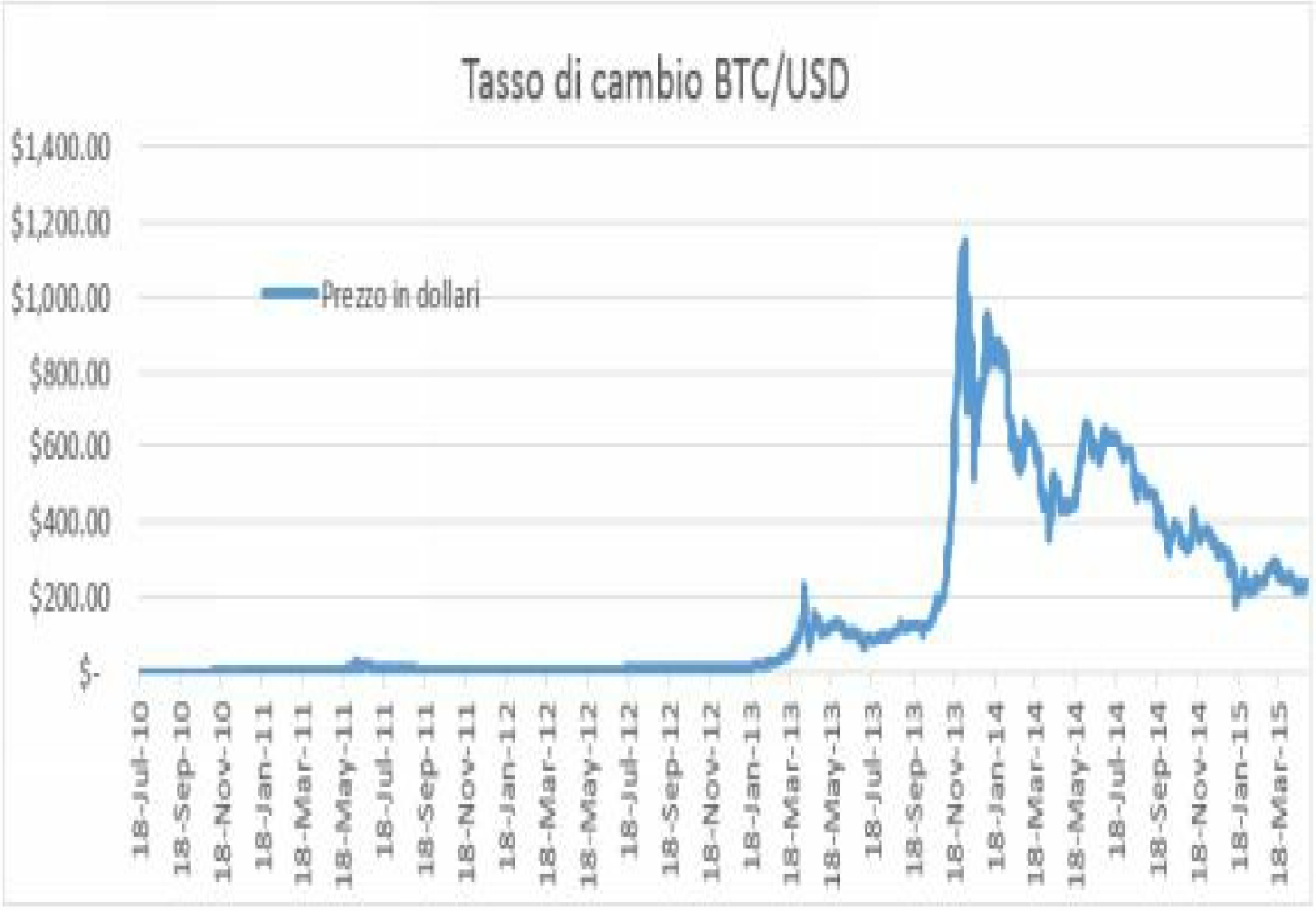


Figura 1: Serie storica BTC/USD. Fonte CoinDesk Bitcoin Price.

Il grafico (Figura 1) mostra l'incremento esponenziale del valore dei bitcoin a partire dal 2013. Non bisogna tuttavia cadere in errore valutando i dati "estremi" come indicativi del trend.

Infatti, sebbene sia stato toccato il valore record di 1147$ per un singolo bitcoin, è molto più significativo studiare l'andamento ripulito da movimenti meramente speculativi e dai valori estremi. Questo grafico evidenzia come gli internauti abbiano iniziato a riporre fiducia nella criptovaluta, aumentando le transizioni e la diffusione della stessa. Con un tasso di cambio di oltre 225$ per bitcoin a febbraio 2015, si può certamente affermare che la moneta elettronica ha ottenuto un successo strepitoso, ed il viaggio è appena cominciato!

Proseguendo nell'analisi, ai lettori più vivaci potrebbe essere sorto

il dubbio di come una economia caratterizzata da assenza d'inflazione, e quindi in gergo *deflazionistica*, possa essere adeguata ad una economia in crescita quale quella reale. È una osservazione sicuramente valida ma non così rilevante per i guadagni in bitcoin.

È opportuno introdurre il seguente ragionamento: per quanto esistano molti luminari o guru che descrivono il mondo del futuro dominato dai bitcoin, questo e-book utilizza un approccio pragmatico-razionale e supportato dai fatti, al fine di permettere al lettore di ottenere i massimi rendimenti dall'utilizzo dei bitcoin.
E' necessario sottolineare che,

nonostante le grandissime potenzialità di questa valuta, parlare di Bitcoin in quanto sostituti della moneta corrente è quantomeno prematuro. Anche per i più ottimisti, bisogna considerare il lunghissimo iter legislativo e culturale che è necessario percorrere per arrivare ad una tale diffusione, ed è mera speculazione verbale pensare il contrario. D'altronde, fu proprio il celebre economista J. M. Keynes ad affermare "*nel lungo periodo, siamo tutti morti*". Forti di questa verità, questo e-book si concentra su metodi validi oggi e nell'immediato futuro, non annoiando il lettore con ipotetici quanto remoti scenari troppo futuristici e fantasiosi.

A differenza di altre divulgazioni, gli autori vogliono mantenere un orizzonte temporale adeguato per investimenti ed operazioni che diano i loro frutti in un lasso ragionevole di tempo. I bitcoin hanno un grandissimo potenziale di crescita, indipendentemente dal fatto che un giorno remoto possano sostituire la moneta a corso legale. Questo perché coprono e servono una fascia d'utenza e di servizi che necessitano delle caratteristiche intrinseche della cripto-valuta, ossia *anonimato*, *assenza o bassissimi di costi di transazione, e velocità dei pagamenti*. Ed è questa la ragione per cui, entrare nel business dei

bitcoin è importante per il grandissimo potenziale di questo mercato, senza preoccuparsi troppo se in un ipotetico futuro il mondo utilizzerà all'unanimità la cripto-valuta.

Tuttavia, per ottenere guadagni, bisogna avere gli strumenti e le informazioni giuste, che verranno svelati nei seguenti capitoli.

1.3. I VANTAGGI DELLE TRANSAZIONI IN BITCOIN

Sia che i lettori siano interessati a commerciare tramite bitcoin, sia che vogliano semplicemente speculare sulla moneta, è fondamentale capire quali vantaggi e quali categorie di venditori/compratori hanno trovato nei bitcoin uno strumento perfetto. Senza analizzare questi elementi, non è possibile comprendere o fare previsioni verosimili e, conseguentemente, ottenere alcun utile dalla valuta digitale.

- *Certezza dei pagamenti.*
  Sembrerebbe scontato, e forse erroneamente molti credono che i sistemi più utilizzati (assegni, bonifici bancari, PayPal, e la lista può continuare ancora) forniscano la certezza al venditore di incassare il denaro. Non è così.
  Per restare in tema di "pagamenti digitali", un esempio esplicativo è rappresentato proprio da PayPal. Questo sistema, in realtà, offre ben poche garanzie al venditore di aver realmente a disposizione le cifre incassate dalle sue vendite. Infatti, è semplicemente possibile per l'acquirente aprire una contestazione,

per svariati motivi, e “congelare” i fondi del venditore. Lo stesso si può dire degli assegni (possono essere scoperti o bloccati *ex post*), e molte altre forme di pagamento bancarie ritenute erroneamente essere “certe”. Anche implicazioni di carattere giuridico possono compromettere il venditore, si pensi ad esempio ad un criminale che paghi con denaro frutto di illeciti: il venditore in buona fede, ignaro del fatto, può comunque trovarsi ad affrontare problemi e fastidi dovuti a provvedimenti giudiziari.

Con i bitcoin, questi problemi non esistono. Un pagamento quando

inviato è irreversibile ed incontestabile, assicurando al venditore la certezza assoluta di aver la somma disponibile.

- *Anonimato*
  Tutti i comuni sistemi di pagamento basati su internet hanno una caratteristica comune: la totale assenza di anonimato. In altre parole, la transazione dell'utente che effettua/riceve un pagamento rimane inesorabilmente salvata e a disposizione dei fruitori del servizio, per un lasso di tempo potenzialmente infinito. Gli autori non vogliono affermare che ciò sia

necessariamente allarmante, ma è pur vero che molti utenti preferirebbero un sistema anonimo di pagamento, riconducibile al cash, però su internet. I bitcoin rispondono totalmente a questa esigenza, nessuna informazione personale è diffusa oppure ottenibile nell'invio o ricezione di un pagamento, ed è uno tra i tanti motivi per cui sempre più persone utilizzano la cripto-valuta. Indubbiamente, questa caratteristica può incentivare l'utilizzo dei bitcoin anche per la vendita di prodotti e servizi non propriamente legali. Agli scopi di questo e-book, ciò è completamente irrilevante, poiché in questa sede parliamo del valore della

cripto-valuta, ed al crescere degli utilizzatori, è destinato ad aumentare. L'utilizzo, da parte di alcuni utenti, del protocollo Bitcoin per fini illegali costituisce un fallimento degli organismi volti a garantire la legalità, e non della valuta digitale. Proprio come avviene per il cash, non avrebbe senso colpevolizzare lo strumento (la banconota), se tramite essa sono stati pagati servizi illeciti.

- *Pagamenti in tempo reale e riducendo al minimo le commissioni*
  Un altro limite di molte forme di pagamento sono i tempi d'attesa tra l'invio e l'effettiva ricezione del

denaro. Ad esempio, i bonifici bancari: non possono avvenire in tempo reale ma necessitano, di norma, minimo un giorno lavorativo, sino ad oltre cinque per i bonifici internazionali! Come se non bastasse, è preclusa la possibilità di inviare celermente denaro nei giorni festivi o weekend. Ed il tutto, a fronte di commissioni variabili da banca a banca. Molte altre forme di pagamento digitale sono anch'esse affette da questa asincronia temporale tra l'invio e l'effettiva ricezione del denaro, ed in aggiunta soggette a cospicue commissioni. Per non parlare delle spese di tenuta conto, più o meno presenti in forma diversa

nella totalità dei sistemi di pagamento informatici.[1]
Con i bitcoin questi problemi non esistono, i pagamenti avvengono in tempo reale (per approfondimenti, si rimanda il lettore al paragrafo 2.5.2) e le commissioni sono soltanto facoltative, e oltretutto irrisorie se paragonate ad altri servizi.
Qual è lo scopo delle commissioni all'interno del network?
Semplicemente quello di "compensare" il lavoro svolto dai nodi, cioè altri utenti bitcoin, che utilizzano la potenza di calcolo dei loro PC per trasmettere più velocemente il pagamento al

destinatario (per approfondimenti, Capitolo 2). Queste commissioni sono, tuttavia, molto inferiori ai costi applicati da qualsiasi altro tipo di servizio, oltre che essere a discrezione dell'utente che le sceglie in base alla priorità e all'ammontare del pagamento stesso.
Tirando le somme, non solo i bitcoin permettono trasferimenti immediati di somme di denaro, ma addirittura a costo zero o irrisorio

Ancora una volta gli autori intendono precisare che in alcun modo si cerca di mistificare il protocollo Bitcoin come la migliore forma di pagamento in

assoluto. L'inerente, ai fini di questa trattazione, è ribadire l'equazione "più utenti bitcoin = maggiore valore dei bitcoin". Questi notevoli vantaggi, propri della cripto-valuta, fanno sì che il suo utilizzo sia abbracciato da una grande quantità di utenti. Il lettore dovrebbe aver già compreso che ciò si traduce immediatamente in grandi possibilità di business.

1.4. GLI "EARLIER ADOPTER": MULTINAZIONALI E COMMERCIANTI DI PAESE

Le premesse sul mondo dei Bitcoin non sarebbero complete senza prestare attenzione a come il fenomeno sia già iniziato ad essere realtà, a partire da diverse multinazionali sino ad arrivare ad esercizi commerciali di piccole dimensioni.

A fine 2014, nell'elenco delle grandi società che accettano pagamenti in bitcoin compaiono, tra le altre:

Microsoft (terza società al mondo per capitalizzazione nel settore tecnologico), Atomic Mall, Clearly Canadian, Dell, Dish Network, Expedia, Newegg, PrivateFly, Overstock.com, TigerDirect, Time Inc., Virgin Galactic, e Zynga (la famosa società di giochi su Facebook).

Ancora non si annoverano grandi compagnie italiane, ma poco male. Anzi, questo dimostra come il percorso dei bitcoin sia ancora agli inizi e quanto grandi siano le possibilità di sfruttarli a proprio vantaggio, cercando di anticipare il trend proprio come stanno facendo gli statunitensi.

Inoltre, anche celebri organizzazioni no-profit accettano

donazioni in bitcoin: Greenpeace, The Mozilla Foundation, e The Wikimedia Foundation sono solo alcune delle tante.

E' evidente che grandi colossi operanti a livello internazionale stanno investendo nel futuro di questa valuta, e se lo fanno è perché questo business offre delle grandi potenzialità di guadagni e di crescita.

Tuttavia, non serve essere una multinazionale per conquistarsi la propria fetta all'interno di questo mercato, ed iniziare ad operare con i bitcoin.

In Olanda, per esempio, esistono locali (Figura 2) che accettano la cripto-valuta come regolare mezzo di

pagamento.


DE WAAG
BETALEN MET
"BITCOINS"
MOGELIJK!

Figura 2: Esempio di locale olandese che accetta bitcoin come forma di pagamento

In futuro, anche situazioni di questo tipo potranno diventare più comuni, ma ancora una volta gli autori preferiscono non occuparsi di un futuro troppo remoto, e concentrarsi sullo studio delle possibilità attuali.

Il fine di questo paragrafo non è affermare che sia sufficiente emulare l'esempio di un negozio che accetta pagamenti in bitcoin, per ottenere guadagni. Molto più lungimirante è conoscere perfettamente il protocollo Bitcoin per poterne comprendere le potenzialità e, successivamente,

sfruttarlo nel proprio business.

Inoltre, riteniamo che avere a disposizione bitcoin sia importante quantomeno per poter iniziare speculare con la criptomoneta.

1.5. Il DEEP WEB ED I BITCOIN

A conclusione di questo capitolo iniziale, è stato ritenuto rilevante introdurre una piccola digressione sul fenomeno del “deep web”, “Web sommerso” tradotto in italiano, e di come sia legato al mondo dei bitcoin.
Per chi non sapesse cosa sia il “deep web”, non è altro che la porzione del World Wide Web non indicizzata dai motori di ricerca, e quindi, in altre parole, impossibile da trovare mediante una ricerca con Google. Per rendersi conto della vastità del “deep web”, basti

pensare che soltanto l'1% del World Wide Web risulta indicizzato tramite motori di ricerca, tutto il resto è, appunto, nascosto. Volendo fare un paragone, proprio come l'universo, di cui conosciamo solo una piccolissima parte.

Il motivo per cui si parla del "Web sommerso" risiede nel fatto che al suo interno esistono dei veri e propri siti di e-commerce, anche se la maggior parte di essi illegali, e per questa ragione tenuti nascosti agli organismi di controllo. Tra le altre cose, vengono vendute armi, sostanze stupefacenti, prodotti illeciti e altri servizi.
Non sarà sfuggito al lettore attento che

tutti questi beni non potrebbero essere acquistati tramite consuete forme di pagamento, e fu questo il motivo per cui il protocollo Bitcoin prese rapidamente piede in questa ambiente "*underground*" di internet.

È innegabile affermare, sotto un certo punto di vista, che una spinta iniziale alla diffusione dei bitcoin sia stata proprio la possibilità di fare acquisti (illegali) nel deep web. Questa informazione è necessaria per comprendere il fenomeno nella sua totalità, e quindi non tralasciata dagli autori.

Non è tuttavia motivo per rimanere scandalizzati né sconvolti. Come visto in

precedenza, i bitcoin sono abbracciati da alcune tra le più grandi multinazionali al mondo, con fatturato di miliardi di dollari e non certo operanti nell'ombra o illegalità!

Con questa divulgazione si vuole anche spazzare via una certa ignoranza che aleggia sulla cripto-valuta. Infatti, non avrebbe alcun senso discreditare il protocollo Bitcoin, o ancora peggio sottostimarne le sue potenzialità, conseguentemente al fatto che esistono persone che ne fanno lo strumento per attività illecite. Sarebbe come rifiutare di detenere euro perché alcune organizzazioni criminali operano con essi. Assurdo.

Dopo questa panoramica, sufficientemente ampia e volutamente mai prolissa o superflua, ci si avvia quindi a trattare gli strumenti con cui gestire e capire il protocollo Bitcoin nel dettaglio.

CAPITOLO 2.

PROTOCOLLO BITCON

Nel pieno rispetto dei presupposti in cui si colloca l'e-book, verrà affrontato dapprima il *mining*: letteralmente minare, pratica che utilizza la capacità di calcolo (di un personal computer) per estrarre BTC[2] dalla rete. Gli autori entreranno nei dettagli del *mining*, capendo cosa sia, perché oggi non è più conveniente per i privati, e quali sono i metodi alternativi a tale strategia per guadagnare BTC.

Per i lettori più curiosi, nella parte finale di questo capitolo, verranno affrontati gli aspetti fondamentali che regolano il funzionamento del protocollo

Bitcoin.

2.1. IL *MINING*

Il termine "*mining*" è stato volutamente scelto, dal protocollo Bitcoin, per creare una sorta di analogia con il processo di estrazione dell'oro: come i minatori "reali" estraggono l'oro dalle miniere, così i minatori "virtuali" estraggono BTC. Dunque, si tratta di un meccanismo temporaneo (si capirà a breve il perché) per l'emissione di nuovi BTC.

A differenza dell'estrazione dell'oro, la produzione di bitcoin riconosce un premio sia per la creazione di nuova moneta, sia in cambio di servizi utili al funzionamento della rete.

Infatti, il *mining* è responsabile dell'intero sistema dei trasferimenti (da un conto ad un altro) della criptomoneta, e ciò lo rende necessario anche quando sarà estratto l'ultimo bitcoin. Il tutto viene gestito attraverso il sistema delle conferme, sistema semplice ma che merita un approfondimento al riguardo e per questo trattato nei paragrafi successivi.

A questo punto, il lettore più attento, potrebbe pensare che attraverso questo sistema è possibile produrre un numero teoricamente infinito di BTC, ma non è così. Il numero di BTC presenti in rete è stato già fissato, dunque non è possibile produrne a caso. Sarà più

chiaro – nel corso di questo capitolo – il motivo per il quale, anche se volessimo farlo, non potremmo.

Il premio elargito per l'attività di *mining* è in BTC, dato dalla somma di una componente **aleatoria** più una **deterministica**. Chiariamo questi termini. La prima componente è la somma delle commissioni pagate per il trasferimento di BTC, per questo aleatoria: non è possibile conoscere in maniera esatta l'ammontare di questa cifra, perché è funzione del numero di transazioni che avvengono in quell'intervallo temporale[3]. La seconda, al contrario, è definita dal tasso di produzione annuale della

moneta, e per questa ragione è conosciuta a priori e quindi deterministica.

La prima componente resterà sempre parte attiva dei guadagni dei miner anche quando sarà estratto l'ultimo BTC, mentre la componente deterministica è destinata ad annullarsi al raggiungimento del numero massimo di BTC previsti dal protocollo stesso.

Il premio pagato per il lavoro svolto dai minatori è piuttosto cospicuo, basti pensare che un solo BTC vale circa 212 €, e che le transazione avvengono ogni 10 minuti.

In sintesi, il *mining* si può considerare come il centro dati dei

Bitcoin, ad accezione del fatto che è stato progettato per l'esatto opposto: i minatori sono presenti in tutta la rete ma nessuno di essi ne ha il controllo.

2.2. COME DIVENTARE MINATORI

Per poter far *mining* è necessario disporre di strumenti hardware e software adeguati. Mentre in passato, si parla del non troppo lontano 2009, era sufficiente un normale personal computer, oggi non è più così. Il *mining* era un'attività a cui prendevano parte tutti gli utilizzatori della valuta digitale, che cercavano di contribuire attivamente in questo modo al suo funzionamento, oltre che guadagnarci un po'. Tutto questo aiuta a capire l'enorme espansione che la

criptovaluta ha avuto in questi anni.

Oggi, è necessario acquistare un ASIC (*Application-Specific Integrated Circuit*, Circuiti Integrati per Specifiche Applicazioni) che consente di ottenere prestazioni 100 volte superiori rispetto alle normali CPU General Purpose, nell'elaborazione degli algoritmi Bitcoin.

A titolo meramente informativo, si elencano alcuni sistemi dalle prestazioni tutt'oggi affidabili, capaci di dissipare in maniera adeguata l'enorme calore generato durante l'attività di calcolo. Sono prodotti dalla **Butterfly Labs**, dalla **Antminer**, **Bit-Furry** e **KNC**.

Ordinato e ricevuto l'hardware, è necessario scaricare uno speciale software per i minatori. In rete, sono disponibili molti programmi utili allo scopo ma i più popolari sono **CGminer** a linea di comando e **EasyMiner** a interfaccia grafica, disponibile per le piattaforme Windows, Linux ed Android.

Installato l'hardware ed il sistema software, non resta altro da fare che unirsi a club dei minatori, in gergo *mining pool*, come ad esempio "**eclipsemc**". I gruppi lavorano tutti uniti per risolvere i blocchi; senza un gruppo di minatori ben assortito per risolvere un solo blocco ci vorrebbero anni!

L’ultimo passo, ma non meno importante, è aprire un portafoglio (vedi Paragrafo 3.2) all’interno del quale fluiranno tutti i BTC derivanti dall’attività di *mining*. La procedura per l’inserimento dell’indirizzo Bitcoin è abbastanza semplice, ne viene richiesto l’inserimento durante il processo di installazione del software. Lo stesso software procederà all’accredito dei BTC sul wallet (portamonete, vedi Paragrafo 3.2.2), il tutto in maniera completamente automatica.

In Figura 3 e 4 sono riportati due esempi di sistemi hardware casalinghi utilizzati per effettuare *mining* di Bitcoin. La presenza di unità

dedite al raffreddamento fa percepire il fatto che si tratta di dispositivi che posso raggiungere temperature di funzionamento molto elevate. È dunque necessario monitorare la temperatura, che deve rimanere all'interno di un certo *range* di esercizio, per evitare danni permanenti ai dispositivi stessi. Il tutto fa presagire elevati i consumi energetici.

Figura 3: Esempio sistema casalingo per l'estrazione di BTC.

Figura 4: Interconnessione di più sistemi per l'estrazione della criptovaluta.

2.3. SPRECO DI ENERGIA O NECESSITÀ?

Spendere energia per rendere la rete Bitcoin sicura ed assicurarne in questo modo la prosperità, non è sicuramente un'attività inutile. E' in questo ambito che si colloca l'attività di *mining*.

Come ogni sistema di pagamento, l'utilizzo di Bitcoin implica dei costi per le operazioni. Tutti i sistemi monetari utilizzano energia, anche quelli bancari (carte di credito, bonifici, assegni e così via). Il vantaggio sostanziale con il modello Bitcoin è che

l'energia spesa è facilmente quantificabile.

Il *mining* Bitcoin è stato programmato e studiato per ottenere una maggiore ottimizzazione, attraverso l'utilizzo di appositi algoritmi, e con l'aiuto di hardware *low-energy*. Le previsioni indicano che la spesa, per mantenere operativa la moneta, nel prossimo futuro continuerà ad essere proporzionale alla sua richiesta. In sintesi, anche se l'attività di *mining* diventerà più costosa, in termini energetici e hardware, rimarrà per i minatori un buon margine di guadagno.

Il *mining*, in ragione di quanto detto, rimane quindi un'attività

proibitiva – ecco perché gli autori si sono tanto prodigati per redigere un metodologia alternativa che consentisse di guadagnare BTC – basti pensare ai consumi (dell'ordine dei megawatt) necessari per mantenere una sola Bitcoin Farm.

Una recente indagine statunitense ha quantificato il consumo energetico intorno a 140'000 $ (circa 127'000 €) ogni 24 ore. Nei periodi di maggiori picco, l'hardware dedicato al *mining* richiede 982 MW/h (megawatt/ora), la potenza fornita per il fabbisogno di 31'000 abitazioni statunitensi. L'indagine ha preso come riferimento per la componente

energetica un'unità di prezzo di circa 0.15 $ per KW/h (kilowatt/ora).

L'obiettivo attuale, è produrre dispositivi che riducano sempre di più i dispendi energetici cercando di progettare direttamente, per quanto possibile, l'hardware sul problema da risolvere. In Figura 5 è riportato un esempio di ASIC utilizzato nel processo di estrazione dei BTC.

Figura 5: Esempio di ASIC utilizzato nel processo di estrazione dei BTC.

2.4. COME FUNZIONA

Chiunque può diventare minatore Bitcoin utilizzando un software, open source, ed un hardware appositamente dedicato. Il software si pone in ascolto (*receive mode*) delle transazioni in corso sulla rete P2P (*Peer-to-Peer*) ed esegue una serie di attività al fine di elaborare e confermare queste transazioni.

Il lettore può immaginare il processo del *mining* come l'attività di un piccone – ancora più giustificata l'analogia con l'oro – che cerca di rompere una roccia, all'interno della quale sono presenti BTC, le cui

dimensioni (ossia la difficoltà) crescono transazione dopo transazione, circa ogni 10 minuti. Il crescente aumento delle difficoltà, quindi l'inevitabile necessità di disporre di un ambiente di calcolo sempre più veloce e performante, ha fatto sì che fossero necessari dispositivi, molto costosi, come gli ASIC.

Gli ASIC si sono imposti come soluzione finale dopo il passaggio dalle CPU alle GPU (*Graphic Processing Unit*, Unità di Controllo Grafico), e dalle GPU agli FPGA (*Field Programmable Gate Array*, Matrici di Porte Logiche Programmabili).

L'attività dei minatori non è solo rivolta – come già ribadito – alla

creazione di BTC ma rende sicura la rete dei pagamenti attraverso la gestione delle conferme, meccanismo fondamentale alla base del protocollo Bitcoin. In parole semplici, le conferme costituiscono un meccanismo di garanzia, il cui scopo è quello di evitare che un utente venda o spenda monete che non ha, o che ha già speso. Infatti, una transazione non apparirà completata se non avrà raggiunto un numero sufficientemente adeguato di conferme.

Per ottenere conferme occorre risolvere i blocchi (approfonditi nel Paragrafo 2.8.1), contenenti prove di lavoro matematiche, in cui sono presenti le transazioni da confermare. La prova

di lavoro è realizzata in modo tale da essere funzione delle prove presenti nei blocchi precedenti, questo al fine di evitare manomissioni da parte di terzi, ciò significa che se non si conosce il risultato delle prove precedenti non è possibile risolvere la successiva. Inoltre, esse richiedono un'elevata capacità computazionale per essere risolte, e questo demotiva possibili malintenzionati. Il tutto con il fine di imporre un ordine cronologico all'interno di un enorme database: la ***BlockChain***.

La BlockChain è figurabile come un grande libro mastro di tutte le transazioni che, partendo dalla creazione

della moneta (avvenuta all'inizio del 2009), è sempre stato aggiornato, costantemente e minuziosamente, senza il minimo errore.

La necessità di operare una serie così numerosa di calcoli costringe gli estrattori ad eseguirli prima che i loro blocchi vengano accettati dalla rete, e prima che siano assegnati ad altri minatori. Quante più persone concorrono al processo di estrazione, tanto più aumenta la difficoltà di trovare blocchi validi nella rete (blocchi non risolti), garantendo nello stesso momento che il tempo medio per trovare un blocco resti uguale a 10 minuti. Queste sono le principali ragioni per cui

un'estrazione è molto competitiva, e nessun estrattore riesce a controllare ciò che contiene la BlockChain.

Volendo realizzare un'analogia per chiarire la cosa, si può pensare all'intero processo come una gara. Il vincitore è colui che risolve il problema in un preciso lasso di tempo (10 minuti). Il problema assegnato ha una complessità che aumenta con il numero di partecipanti, il primo che lo risolve può passare al livello successivo aggiudicandosi un premio, rendendo vani gli sforzi degli altri. Maggiori sono i problemi risolti, maggiori saranno i guadagni per i vincitori.

Questo rende estremamente

difficile invertire le transazioni precedenti, richiederebbe il calcolo delle prove di lavoro di tutti i blocchi successivi. **I minatori non hanno la possibilità di barare**, aumentando la loro ricompensa, **né validare transazioni fraudolente,** che possano corrompere la rete, perché tutti i nodi respingerebbero ogni blocco contenente dati non validi secondo le regole del protocollo Bitcoin. Perciò, la **rete resta sicura anche se non tutti i minatori fossero persone affidabili**.

2.5. LA BLOCKCHAIN

La BlockChain è un file distribuito, presente cioè su più dispositivi (anche sul vostro PC, se installate BitcoinCore, come si vedrà successivamente), che contiene un elenco di tutte le transazioni dall'inizio del sistema Bitcoin, e viene aggiornato ogni dieci minuti. Questo compito è portato avanti da migliaia di computer detti "nodi", collegati in tutto il mondo alla rete Bitcoin.

E' la BlockChain a consentire le sostanziali differenze, che ne costituiscono la natura decentralizzata della rete Bitcoin, rispetto ai sistemi

bancari, garantendo:

- *Sicurezza e controllo*: gli utenti Bitcoin controllano totalmente le proprie transazioni; ad esempio, i commercianti non possono forzare cambiamenti indesiderati o inosservati, così come avviene con gli altri metodi di pagamento.

- *Trasparenza e neutralità*: tutte le informazioni riguardanti i movimenti di denaro Bitcoin sono prontamente disponibili sulla BlockChain a chiunque, per verifica ed utilizzo in tempo reale. Nessun privato o organizzazione può controllare e

manipolare il protocollo Bitcoin, perché è sicuro dal punto di vista crittografico. Questo permette al nucleo di Bitcoin di essere considerato sicuro e completamente neutrale, trasparente e prevedibile. Allo stesso tempo nessuno conosce le informazioni anagrafiche dell'intestatario del conto, ma può consultare transazioni e saldo di un singolo indirizzo.

La natura pubblica della BlockChain, insieme ad algoritmi di crittografia che controllano il processo di aggiornamento, garantisce la sicurezza e l'affidabilità del nucleo del

sistema. Inoltre, l'aggiornamento imposto ogni dieci minuti dal protocollo, ne garantisce l'integrità come una reazione a catena: aggiorna i nodi con tutte le transazioni effettuate nella rete Bitcoin.

2.5.1. Immunità alle manomissioni

Il libro mastro o BlockChain non risiede in un singolo posto – come già detto – ma su ogni computer che partecipa alla rete Bitcoin. Attualmente, la rete è formata da centinaia di migliaia di nodi, su ognuno dei quali è presente

una copia della BlockChain.

La validità del file è data dal confronto continuo che viene effettuato da ogni singolo nodo con tutti gli altri. Affinché una data transazione sia valida è necessario che almeno il 51% delle copie della BlockChain sui diversi nodi connessi alla rete siano esattamente identiche tra loro. Dunque, per prendere il controllo del sistema, sarebbe necessario violare il 51% dei nodi presenti in rete, cosa a dir poco impossibile.

Queste sono le ragioni che rendono la rete Bitcoin immune alle manomissioni. A corredare il tutto ci pensa il protocollo di criptazione **SAH-**

256 (Secure Hash Algorithm). Si tratta di un protocollo di sicurezza implementato dalla NSA (*National Security Agency*, Agenzia di Sicurezza Nazionale Statunitense), tutt'altro che banale o poco sicuro.

Senza entrare in tecnicismi troppo si accenna il funzionamento di questo sistema di criptazione dell'informazione, utilizzato addirittura come **standard federale statunitense**.

Come ogni algoritmo di *hash* (dall'inglese "to hash", sminuzzare) produce una stringa alfanumerica di lunghezza **fissa**, partendo da un messaggio di lunghezza arbitrale. Dunque, la sicurezza di questo algoritmo

risiede nel fatto che non sia possibile risalire al messaggio originale conoscendo solo quello di *hash*. In Figura 6 è riportato un esempio del suo funzionamento.

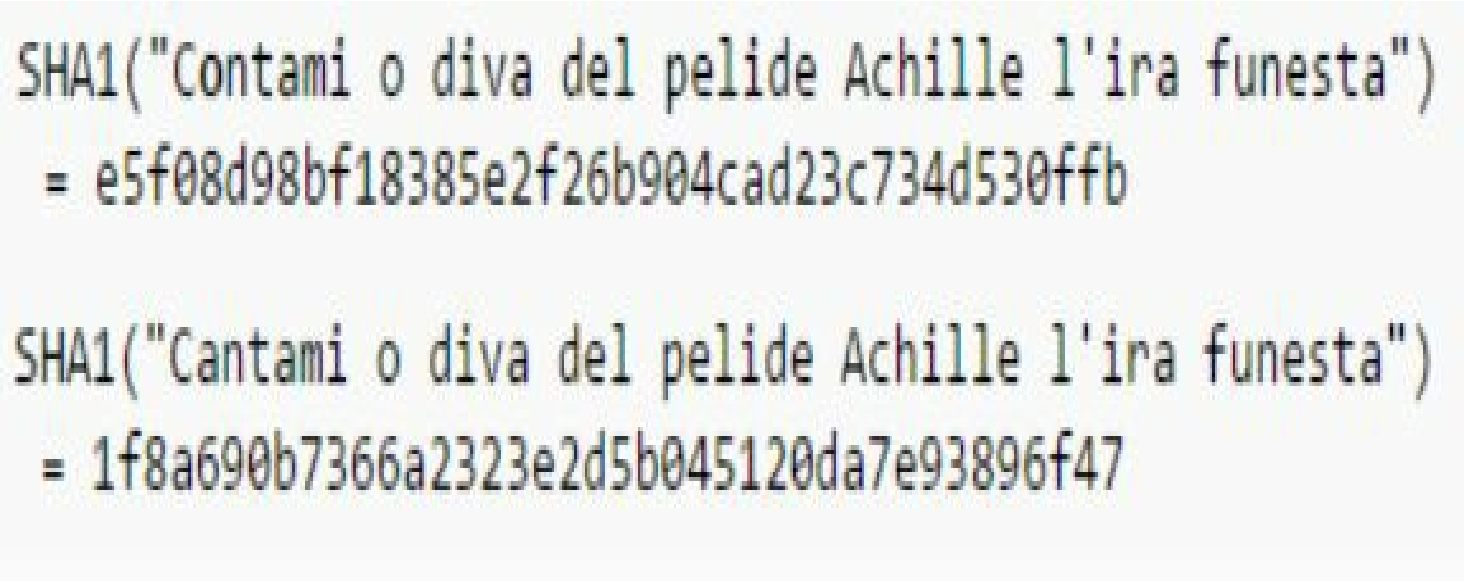


Figura 6: Esempio di trasformazione di una stringa con algoritmo SAH-256.

Come si evince, anche una minima variazione della composizione della stringa (“Cantami” è divenuto

“Contami”) ne cambia totalmente il risultato. Nel protocollo Bitcoin questa crittografia è utilizzata per spedire le transazioni da un nodo alla BlockChain.

Tale è l’importanza di questa operazione, che il protocollo utilizza la parola *Hash* come unità di misura per classificare le prestazioni dell’hardware utilizzato per effettuare *mining*. In Figura 7 si può vedere, attraverso un semplice grafico, come la capacità di calcolo cresca continuamente nel tempo. Sull’asse delle ordinate è riportato il numero di GH/s (GigaHash/secondo) mentre sul quello delle ascisse l’intervallo temporale che va dal Ottobre 2013 al Settembre 2014.

Attualmente si parla di GigaHash.

Figura 7: Serie temporale capacità di calcolo

degli ASIC.

2.5.2. Le conferme

Semplificando al massimo, possiamo dire che una transazione contiene:

- L'ora di invio;
- L'importo;
- L'indirizzo bitcoin di provenienza;
- L'indirizzo bitcoin di destinazione;
- I dati della transazione precedente.

La presenza di dati inerenti alla

transazione precedente, consente di affermare che le transazioni sono collegate l'une alle altre come una catena. Partendo da qui che nasce il **concetto di conferma**.

Volendo passare attraverso un'analogia, possiamo paragonare la BlockChain ad un circuito elettrico costituito da tanti nodi. La corrente, pur essendo disponibile, non circolerà all'interno della BlockChain finché tutto il circuito non sarà chiuso. E' sufficiente che un solo nodo rimanga aperto per bloccare il transito della corrente.

Quindi, la BlockChain è un insieme di ponti (anche detti punti di controllo) ognuno dei quali si occupa di

validare la transazione confrontandola con copia della BlockChain a propria disposizione. Perché la transazione avvenga, è necessario che tutti i nodi confermino la correttezza della transazione, trovandone traccia all'interno della copia della BlockChain in loro possesso.

Solo quando tutti i nodi coinvolti hanno validato la transazione avviene l'effettivo trasferimento, e al tempo stesso diventa definitiva ed immutabile. Da qui – il lettore – capirà l'importanza delle conferme e la necessità di mantenere sempre aggiornata la BlockChain.

2.6. REGOLARIZZAZIONE DEI PREMI

Il sistema garantisce, per sua costituzione, un premio – accennato all'inizio del capitolo – in BTC ad ogni minatore che risolve il problema contenuto in un blocco, per poi passarne il risultato alla BlockChain. Il premio, è costituito da una componente deterministica, fissata dal tasso di inflazione della moneta che ad oggi è fissata intorno ai 25 BTC ma che ne le tempo è destinato a decrescere; una componente aleatoria, funzione del

numero di transazioni che sono presenti in un blocco, oggi pari a 0.1 BTC ma che è destinata, al contrario di quella deterministica, a crescere nel tempo.

Per un attimo, il lettore pensi il sistema Bitcoin costituito da un solo minatore che, grazie alla sua capacità di calcolo, riesce a risolvere la prova di lavoro matematica in 10 minuti. Questo riceverà, per il lavoro svolto, un premio. A questo punto, il lettore immagini un secondo minatore, con le stesse capacità computazionali del primo, che inizi a contribuire alla risoluzione delle prove di lavoro. Dunque, per risolvere lo stesso problema, con la partecipazione dei due

minatori, non saranno più necessari 10 bensì 5 minuti, e ad ognuno sarà corrisposto un premio eguale.

Questo, però, non è il comportamento desiderato. Infatti, il protocollo prevede che alla risoluzione di un problema, ogni 10 minuti, venga corrisposto premio. Dunque, è presente un'anomalia in termini temporali nel rilascio del premio, che deve sempre avvenire ogni 10 minuti.

Per sopperire questa anomalia, il sistema provvede ad aumentare la difficoltà del problema – da qui l'abbandono dei personal computer e l'adozione degli ASIC – in questo modo è garantito che il premio sia corrisposto

non prima di 10 minuti.

Tornando all'esempio. Il sistema, accortosi della presenza dei due minatori, raddoppia la difficoltà del problema in modo tale che, insieme, i due minatori impieghino sempre 10 minuti per risolverlo. In generale, il problema subisce un incremento di difficoltà in funzione del numero di minatori che partecipano alla sua risoluzione.

Per evitare che la difficoltà cresca all'infinito, sono nate le *mining* pool (i club dei minatori). I club raggruppano al loro interno più minatori che, in maniera ridotta, collaborano alla risoluzione del problema. Il sistema

vede la singola pool e non i minatori, la difficoltà continua ad aumentare ma con un tasso di crescita molto minore rispetto a quella che si avrebbe nel caso in cui i minatori lavorassero singolarmente (cosa non più possibile).

Il motivo di tanta severità è da ricercare nella regolazione dell'immissione di BTC. Se non vi fossero queste regole i BTC si svaluterebbero perché i minatori accumulerebbero un enorme numero di BTC in un breve lasso di tempo, cosa assolutamente contro i principi della moneta il cui numero di produzione è già fissato nei prossimi 140 anni.

Obiettivo futuro che si prepone

lo standard è diminuire i dispendi energetici mantenendo, allo stesso tempo, gli elevati standard di sicurezza.

2.7. RESILIENZA ED OPEN SOURCE: PUNTI CHIAVE

I Bitcoin ereditano il concetto informatico di resilienza. Hanno la capacità di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati. Per far comprendere ai nostri lettori quanto i Bitcoin siano resilienti, si riporta un esempio pratico.

Il 2 Ottobre del 2013, negli Stati Uniti, fu bloccato il sito di e-commerce Silk Road. Si trattava di noto sito web dove venivano venduti beni illegali,

pagati in Bitcoin. L'FBI riuscì ad individuare chi gestiva questo portale e lo arrestò. Contestualmente all'arresto, il prezzo di cambio dei BTC precipitò passando da 140 $ al valore di circa 90 $ per bitcoin.

Diffusa la notizia in rete, si pensò subito che questo attacco avesse dettato la fine della moneta matematica, ma così non fu. La fiducia, crollata temporaneamente, dopo pochi giorni portò nuovamente il Bitcoin al valore di 140 $ unitario. Oggi si assesta intorno agli 240 $.

Questo piccolo esempio, fa capire quanto la moneta sia robusta agli attacchi. Il sistema è decentralizzato ed

anche se attaccato, ciò non ne provoca la morte della tecnologia che, in linea di massima, può risentirne solo momentaneamente.

Altro punto chiave della moneta è utilizzare software e protocolli open source. Il codice sorgente Bitcoin è disponibile online sia in consultazione che in modifica. Tutti coloro che hanno voglia e tempo, conoscendo almeno le basi dei linguaggi di programmazione in particolar modo di C++, possono contribuire al miglioramento della struttura. Questo garantisce una vita teoricamente infinita alla moneta, in continuo aggiornamento come accade alle App dei nostri Smartphone.

Una community, sempre crescente, costituita da persone, pagate e non, cerca di dare un contribuito migliorando costantemente il codice sorgente, mantenendo la moneta e l'intero sistema sempre più sicuro. Testando danni provocati da possibili attacchi, e così via.

Nessuna paura – gli autori tengono a precisare che questo avviene su server appositi che simulano la rete Bitcoin. La comunità non è pagata per distruggere la rete, bensì il contrario.

2.8. IL PROTOCOLLO BITCOIN

Bitcoin è realizzato da un sistema e non da un software, due concetti molti diversi. I software che girano su due o più computer sono gli elementi che costituiscono il sistema. Dunque, il Bitcoin non è il risultato delle operazioni svolte dai singoli software, ma il risultato della loro interazione.

Per garantire che strumenti diversi possano comunicare in modo universale è necessario fissare un **protocollo**, una "lingua", che definisca il modo di comunicare, l'entità dei

messaggi, un insieme di regole prestabilite, che regolino lo scambio di messaggi.

Alla base dei Bitcoin vi è una particolare struttura che ha due caratteristiche fondamentali: è un **sistema distribuito** ed è una **rete P2P**. Il primo aggettivo (distribuito) indica che gli elementi sono interconnessi tra loro, da un punto di vista informatico, e scambiano continuamente messaggi per comunicare; il secondo (P2P) indica una rete in cui tutti gli elementi hanno lo stesso ruolo, tutti contribuiscono al conseguimento del risultato, nessuno è indispensabile. L'ultimo concetto da forza e sicurezza alla rete.

Bitcoin è una rete che si controlla da sola grazie al meccanismo delle verifiche. Quindi, la chiave di sicurezza della rete è la distribuzione. Il sistema è tanto più sicuro quanti più nodi partecipano alla rete P2P. I nodi devono essere tanti, sparsi, controllati da soggetti diversi che non hanno interessi comuni se non quello di far funzionare la rete. Tanto più si verificano queste condizioni tanto più difficile sarà per un soggetto malintenzionato prendere il controllo di più della metà dei nodi per modificarne il comportamento.

2.8.1. Il sistema Bitcoin

I bitcoin sono rappresentati nel sistema tramite la loro storia di passaggi da un portafoglio ad un altro. Ad ogni passaggio, una firma digitale (lo stesso concetto utilizzato per la posta elettronica certificata) garantisce che la moneta sia stata spesa dal legittimo proprietario e che l'informazione non venga alterata in un momento successivo. Per rendere questa trattazione non eccessivamente pensante, gli autori hanno deciso non approfondire ulteriormente questo livello di dettaglio.

Quando il legittimo proprietario di un bitcoin vuole eseguire una transazione, aggiunge all'elenco chi è il

prossimo proprietario, pone la propria firma digitale, e comunica la nuova transazione a tutti i nodi della rete che ne verificano la correttezza. E' evidente che per fare queste verifiche i nodi devono conoscere tutte le transazioni fatte dalla nascita della rete Bitcoin, da qui ancora una volta l'importanza della BlockChain.

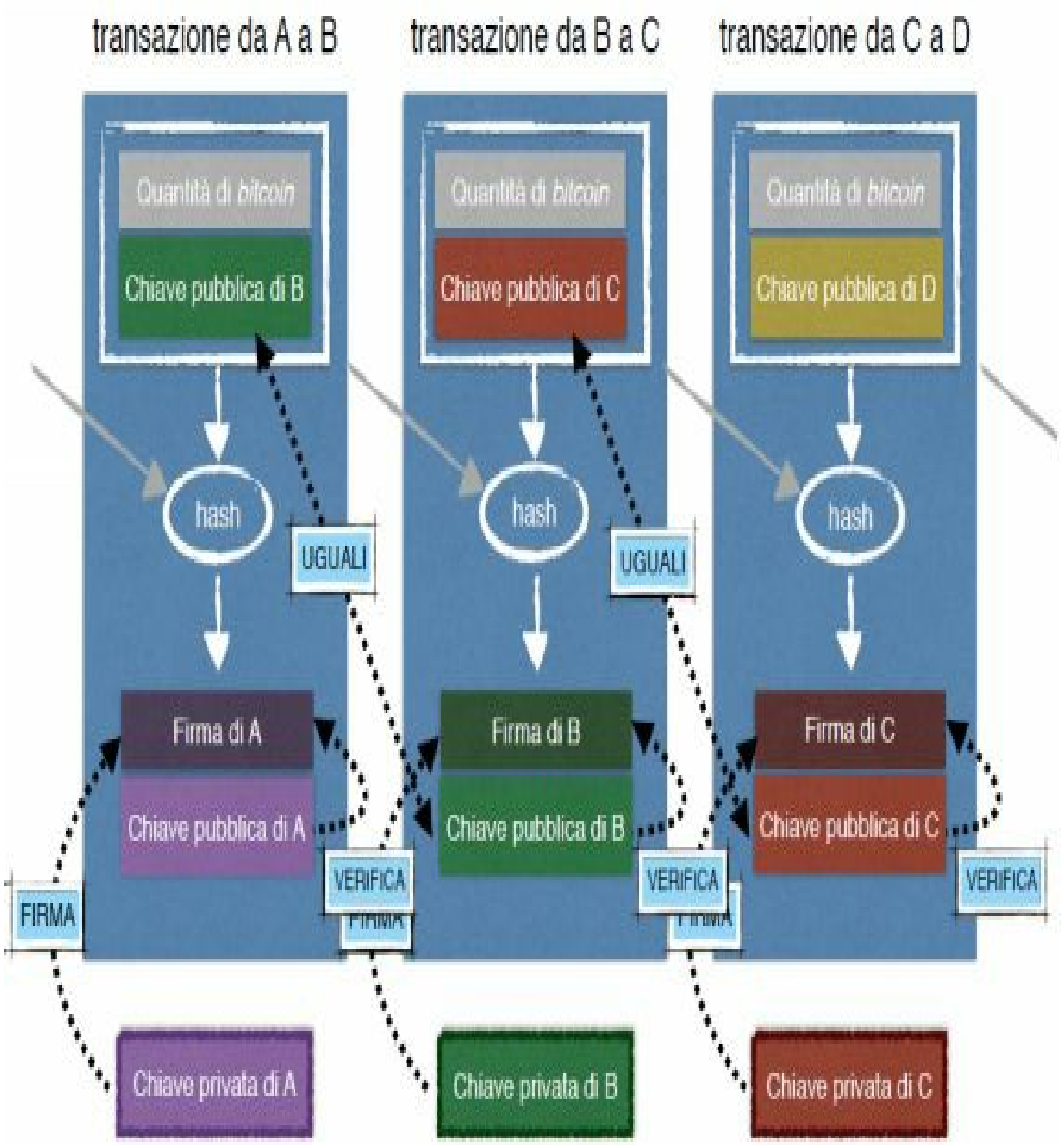


Figura 8: Schema riassuntivo del

funzionamento di una transazione.

Questo meccanismo (Figura 8) è quello che garantisce che ognuno possa spendere solo i propri BTC. Per impedire che qualcuno possa spendere quello che non ha, è necessario controllare la penultima transazione, in modo da rifiutare la seconda se questa è illegittima. Questo porta alla nascita dei blocchi.

I blocchi sono pacchi di transazioni. Sono collegati in una sequenza temporale garantita da una prova di lavoro, che deve svolta per poter “chiudere” il blocco ed iniziare a lavorare il successivo. La prova di

lavoro è semplicemente un calcolo che richiede molto tempo, in media 10 minuti, indipendentemente dalla velocità dei calcolatori (per meccanismi legati all'aumento della difficoltà).

Se un nodo disonesto volesse cambiare una transazione già validata, dovrebbe rifare la prova di lavoro del blocco che la contiene, rifare la prova di lavoro per ognuno dei blocchi chiusi successivamente e chiudere un nuovo blocco prima che lo faccia qualcun altro. Si può riuscire nell'impresa solo se si controlla più della metà dell'intera capacità di calcolo della rete. Operazione impossibile.

Un'osservazione: anche

controllando più del 50% della capacità di calcolo, un malintenzionato non può fare qualsiasi genere di alterazione. Ad esempio, non riuscirà mai a spendere i soldi di qualcun altro perché non potrà mai falsificare la firma digitale del legittimo proprietario. Le transazioni devono essere sempre formalmente corrette, altrimenti gli altri nodi non le accetteranno mai.

2.8.2. Il sistema delle firme digitali

Ogni blocco contiene una specie d'impronta digitale (valore SAH) del

blocco precedente in modo che, se questo viene alterato, l'impronta non corrisponda più. Oltre ad un elenco delle transazioni, nel blocco è anche presente il risultato della prova di lavoro, a dimostrazione che il lavoro è stato fatto. Si crea così una sequenza di blocchi che viene chiama "block chain" (Figura 9).

Figura 9: Schema riassuntivo composizione di un blocco.

Ogni catena di blocchi rappresenta il registro di tutte le transazioni avvenute dalla nascita del protocollo Bitcoin stesso. Ogni nodo della rete lavora a un nuovo blocco raccogliendo le transazioni e cercando di “chiuderlo”, svolgendo la prova di lavoro. Quando la prova di lavoro è terminata, il blocco viene passato a tutti gli altri nodi e si inizia a lavorare ad un nuovo blocco.

Visto che ogni nodo procede per conto suo, potrebbero comparire delle biforcazioni in questa catena ma, tramite opportuni accorgimenti, le biforcazioni vengono poi riassorbite. Il punto chiave

è che, in presenza di più catene, predomina quella più lunga. E' per questo che il malintenzionato oltre a rifare il lavoro **deve chiudere un nuovo blocco prima di che lo faccia qualcun altro**.

La prova di lavoro è una specie di enigma crittografato, calcolato in base al contenuto del blocco stesso, per cui se viene alternato, anche la soluzione dell'enigma cambia, per motivi legati al funzionamento del sistema di crittografia SAH-256. Inoltre, il grado della prova viene continuamente aggiornato in modo da seguire la capacità computazionale totale della rete, ed in modo che il tempo medio per la chiusura di un

blocco rimanga intorno ai 10 minuti.

2.9. *MINING*: TROPPE RISORSE E POCO GUADAGNO

In sintesi il lettore avrà capito che in passato il *mining* era il metodo migliore e più sicuro per guadagnare BTC, contribuendo nello stesso momento a mantenere sicura l'intera rete.

L'incremento, sempre maggiore, delle capacità di calcolo necessarie per risolvere i problemi di natura matematica e gli elevati consumi energetici dei dispositivi, accesi ventiquattro ore al giorno, hanno portato

allo sviluppo di farm dedicate.

Infatti, se è vero che tutti possono far *mining* ci si rende conto – il lettore l'avrà capito già leggendo i primi paragrafi – che l'attività comporta un costo iniziale (hardware ed energetico) che è ripagata solo nel lungo periodo.

Se ciò non bastasse, per poter diventare minatori è necessario unirsi a dei gruppi, tanta la mole di calcoli da fare, e solo insieme si riesce a risolvere il problema. Ovviamente, il premio verrà diviso tra tutti i membri del gruppo. Maggiore è il numero dei partecipanti, minore sarà il capitale accumulato dal singolo.

Per farla breve, se si dispone di

un unico dispositivo e si vuole contribuire, anche se in minima parte, a salvaguardare la rete, ben venga fare *mining*. Al contrario, se con il *mining* il lettore crede di creare la sua fortuna, lo può dimenticare di certo. Il capitale iniziale per avviare lo sviluppo di una farm, che deve essere costantemente aggiornata con nuovi dispositivi, stando sempre al passo delle ultime tecnologie, ripaga solo se siete Microsoft, Apple (…) ossia avete già a disposizione gruppi di calcolatori ad alte prestazioni (super computer).

Oggi, esistono metodi alternativi – obiettivo principale sul quale si fonda l'e-book – celati a molti,

che consentono, conoscendo i posti e le tecniche giuste, di guadagnare BTC nel breve tempo senza spenderne troppi, senza lasciare il PC acceso ventiquattro ore al giorno o acquistare macchine complesse (vedi Capitolo 5).

CAPITOLO 3

GESTIONE E SICUREZZA DEL PORTAFOGLIO BITCOIN

Chiari i meccanismi alla base del funzionamento della criptovaluta, è fondamentale capire come conservare ed utilizzare (invio e ricezione di denaro) questa moneta, quali sono i problemi relativi alla sicurezza e come risolverli, inoltre quali sono le giuste azioni da intraprendere per fare della “banconota anonima” lo strumento di lavoro per eccellenza.

3.1. COME FUNZIONA UN PORTAFOGLIO VIRTUALE

Con lo stesso approccio pratico che precede l'approfondimento teorico – chiave di lettura dell'intero e-book – saranno illustrate tutte le fasi necessarie per aprire un portafoglio virtuale, partendo da uno dei siti web più popolari del momento: BlockChain.info.

Questo, ovviamente, non è l'unico presente sul web, è possibile suddividerli per tipo: *Desktop, Smartphone* e *Web*. Tra quelli su Smartphone, volendoli distinguere per

sistema operativo di utilizzo, annoveriamo:

- Bitcoin Wallet (solo per BlackBerry ed Android);
- BreadWallet (solo per iOS);
- Hive e Green Address (per Android e iOS);
- KnC Wallet e Mycelium (solo per Android).

Per i Desktop, distinguendoli tra Windows, Linux e Mac, e troviamo:

- Bitcoin Core, Electrum mSIGNA, MultiBit, Armony, Green Address

(per Windows, Linux e Mac);

- Hive (solo per Mac).

Per il web, utilizzabili con un normale browser e senza bisogno di installazione, invece:

- Hive, BitGo, Green Address, Xapo, Coinapult, Coinbase e Coinkite.

3.1.1. APRIAMO UN PORTAFOGLIO VIRTUALE (Web Based)

Si inizierà illustrando il

funzionamento di un portafoglio *Web Based,* che ha il vantaggio di non richiedere alcuna installazione sul proprio Computer (quindi non necessita di scaricare la BlockChain sull'hard disk), e tra i vantaggi vi è sicuramente la fruibilità ovunque vi sia un accesso Internet.

Si stabilisce una connessione con il portale, utilizzando un qualunque browser per internet – nel corso di tutti gli esempi è stato utilizzato Google Chrome – e si accede alla sezione denominata "Portafoglio" (Figura 10). A questo punto, ipotizzando di non averne ancora un Portafoglio, si può procedere alla creazione. L'intero processo

richiederà non più di un minuto.

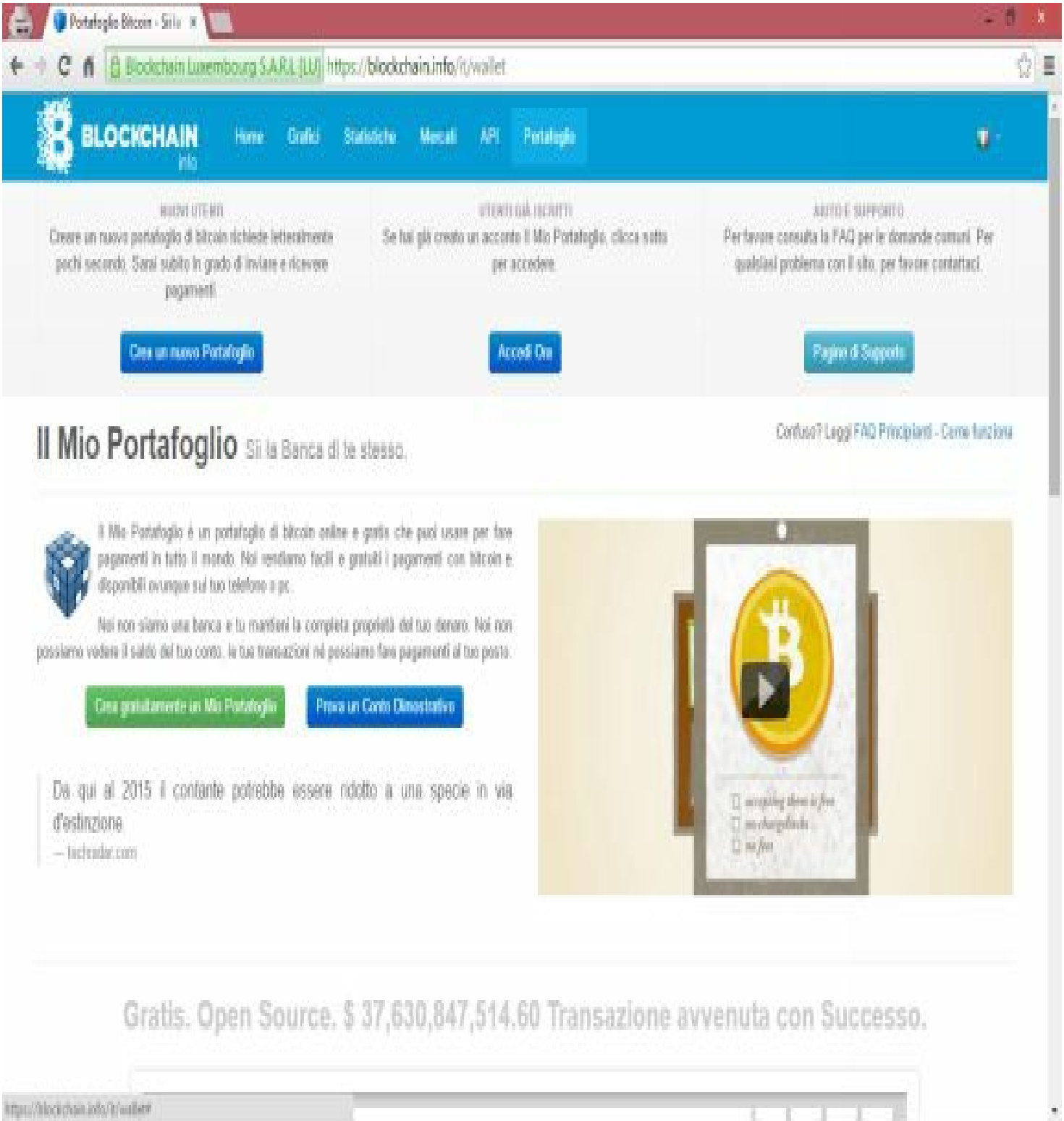


Figura 10: Blockchain.info, sezione apertura

nuovo portafoglio.

Si inizia con il cliccare su "Crea un Nuovo Portafoglio" e si inseriscono le informazioni richieste:

- *E-mail*: verrà utilizzata per tutte le comunicazioni di carattere tecnico e commerciale (ricezione e invio di bitcoin, sconti sull'acquisto in particolari store, e così via), sarà, a tutti gli effetti, il secondo strato di verifica per l'accesso all'account;
- *Password*: proteggerà il portafoglio da accessi indesiderati.

Inserite le informazioni richieste, un messaggio confermerà l'avvenuta creazione del portafoglio e, per la sicurezza dell'utente, consiglia di salvare lo **mnemonico** (vedi Paragrafo 3.8), documento fondamentale per recuperare le credenziali di accesso in caso di smarrimento della password. Seguendo la stessa linea di BlockChain.info, anche gli autori si sentono di consigliare di stampare il documento, o annotarlo in un posto sicuro (Figura 11).

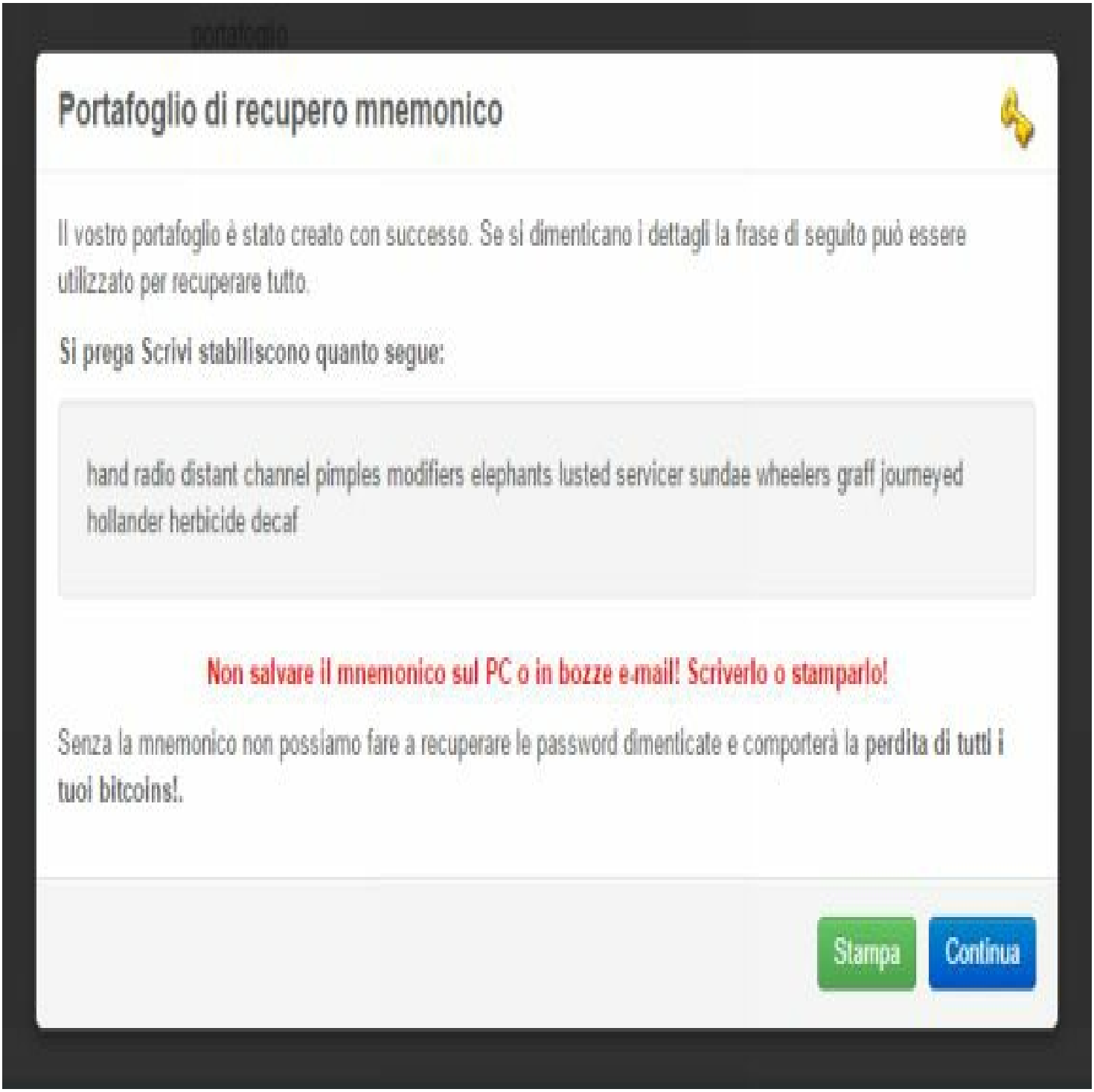


Figura 11: Pagina web attraverso la quale è possibile salvare lo Mnemonico.

Fondamentale, prima di poter

accedere al portafoglio, è confermare l'indirizzo di posta elettronica inserito in fase di registrazione. Basterà accedere alla casella di posta e cliccare sul link di conferma presente nella e-mail inviata da BlockChain.info.

Identificativo e password alla mano, si può accedere al "portafoglio virtuale", inserendo i dati nelle caselle di testo e cliccando su "Apri il Portafoglio".

Per tutelare la sicurezza dell'utente, BlockChain.info utilizza sistemi di verifica aggiuntivi se si prova ad accedere al wallet attraverso postazioni non usuali, tramite il controllo dei cookie e dell'indirizzo IP.

In caso la postazione d'accesso non venga riconosciuta, BlockChain.info richiederà di verificare l'identità tramite un messaggio inviato nella casella di posta elettronica associata al conto, e procedere con la verifica.

In questo modo, il portale garantisce elevati standard di sicurezza perché, meticolosamente, verifica l'identità prima di consentire l'accesso a bitcoin. Di conseguenza, anche se un pirata riuscisse a risalire ai dati contenuti all'interno dello mnemonico, senza conoscere la password della casella di posta elettronica associata, non potrebbe mai trafugare i bitcoin. Queste le ragioni che ne fanno il wallet

web based tra i più consigliati.

Il processo è terminato, il lettore è ora pronto per ricevere tutti i bitcoin che desidera.

3.1.2. WALLETT E BITCOIN ADDRESS: DIFFERENZE

Partiti dall'esempio pratico, gli autori desiderano soffermarsi sulla necessità di disporre di un wallet per la conservazione della criptovaluta.

I Bitcoin consentono di scambiare denaro in modo diverso da quanto avviene nei circuiti bancari

(argomento già ampiamente discusso nel Capitolo 1 e 2), da qui l'importanza di prestare la massima attenzione con il "portafoglio virtuale", proprio come se fosse il portafoglio fisico che portiamo quotidianamente appresso. D'altronde, si vedrà che le differenze tra il portafoglio "reale" e quello "virtuale" dei bitcon, sono davvero minime.

All'atto della creazione di un portafoglio (questo è il significato letterale di "wallet") sarà possibile creare automaticamente un indirizzo (*34 caratteri alfanumerici*) chiave univoco per il riconoscimento del "conto bitcoin.

Al lettore più attento una domanda sorge spontanea: ma qual è la

differenza sostanziale tra un “bitcoin address” ed un “wallet”? Il primo è un codice univoco, se ne possono generare di infiniti (teoricamente); il secondo è un contenitore nel quale si possono inserire tutti i “bitcoin address” generati, ossia gli indirizzi tramite i quali vengono ricevuti ed inviati i pagamenti.

3.2. COME EFFETTUARE UN BACKUP DEL PROPRIO CONTO

Prima di operare con la criptovaluta, è necessario comprendere come garantire la sicurezza del proprio conto. In questo paragrafo gli autori analizzeranno come tutelarsi efficacemente, tramite il sistema offerto da BlockChain.info.

In primis, è fondamentale accedere al proprio conto utilizzando l'identificativo – per gli smemorati è presente nello mnemonico – e la

password scelta in fase di apertura del conto. Recatisi nella sezione "Salvataggio", è possibile scegliere tra le diverse opzioni: Download, Dropbox, Google Drive, Email e Paper. Ciascuno di essi verrà ora brevemente affrontato.

Backup in locale:

BlockChain.info fa di tutto per mantenere al sicuro i bitcoin, ma una copia di salvataggio in locale non guasta mai. Cliccando semplicemente sul bottone "Download", è possibile scaricare il file "wallet.aes.json" contenente tutto il necessario per ripristinare i bitcoin.

Backup sui servizi cloud: È consigliabile salvare il contenuto del

proprio wallet anche sui servizi cloud più conosciuti come Dropbox e Google Drive. Anche in questo caso sarà necessario soltanto cliccare sul pulsante apposito, a seconda del servizio cloud scelto. Verrà richiesta l'inserimento delle credenziali per il servizio, nel caso già si disponga di un account. Alternativamente, è possibile crearne uno nuovo.

Backup per e-mail:

BlockChain.info consente, ancora, di salvare lo stato del proprio wallet per e-mail, il tutto possibile cliccando semplicemente sul bottone "E-mail". La comparsa di un messaggio, presente in un riquadro verde, confermerà

l’avvenuto invio della mail.

Stampa del backup: Al fine di aumentare il livello di sicurezza del conto, è possibile stampare lo mnemonico, cliccando su “Paper”. L’apertura di un box indicherà la necessità di inserire la password del conto per concludere l’operazione. Inserita la password, basterà premere su “Continua”. Capita che il nostro browser possa bloccare il popup[4] che consente di stampare il contenuto del conto. Per risolvere il problema è necessario cliccare con il proprio mouse sull’icona nella barra degli indirizzi, e consentire l’avvio del popup per poi cliccare su “Fine”. Basterà salvare e

stampare il documento per essere sicuri che nessuna frode informatica potrà mai intaccare i bitcoin.

Famosa è la storia di un sistemista inglese, James Howells, che rottamò il suo vecchio hard disk, dimenticando di aver salvato sul proprio computer bitcoin per un valore di 5 milioni di dollari. Questo e altri sfortunati esempi dovrebbero portarci a concludere che, sicuramente, la strategia vincente per proteggere i propri bitcoin sia sfruttare il binomio cloud e copia di backup in locale, ed è per questa ragione che gli autori consigliano l'utilizzo simultaneo di più sistemi di backup.

3.3. TANTI WALLET, QUALE SCEGLIERE?

Tanti sono i wallet presenti in rete, ognuno con i suoi pro e contro. Gli autori hanno cercato di riassumerli brevemente:

- *Il portafoglio desktop*: è un client installabile sul computer, che consente un controllo completo da parte dell'utente. Tuttavia, è un onere dello stesso utente proteggerne il contenuto da attacchi indesiderati, operati da pirati informatici, o perdite accidentali (nuovamente

l'importanza di effettuare un backup). Tra i client più diffusi sicuramente si può annoverare MultiBit, facile e veloce, indicato per utenti alle prime armi; Bitcoin Core, il più sicuro e professionale, a patto di avere sufficiente spazio sul proprio hard disk. Infatti, quest'ultimo necessita di salvare in locale l'intera BlockChain, richiedendo più di 20 GB (gigabyte) destinati ad aumentare nel tempo;

- *Il portafoglio mobile*: è un applicazione per smartphone, consigliabile se si utilizza la criptovaluta in movimento. Ad

esempio, si può pagare in un negozio che accetta Bitcoin scansionando un QR Code[5]. Rileva la sua utilità in tutti luoghi in cui sono presenti utenze commerciali che accettano la valuta digitale. Le migliori applicazioni, decisamente, BitcoinWallet e MyCelium Wallet.

- *Il portafoglio web*: il sistema più utilizzato per chi vuole provare i bitcoin senza troppi rompicapi. Ci si iscrive ad un servizio online, si crea un account e si accede al portafoglio attraverso un normale browser per internet. Tra i siti web che godono di maggiore reputazione si ricorda il

già discusso BlockChain.info.

3.4. COME RIPRISTINARE IL PROPRIO CONTO

Effettuata la copia di backup del saldo e delle transazioni, è fondamentale capire anche come ripristinarlo a seguito di un furto oppure dello smarrimento delle credenziali d'accesso. Due sono le soluzioni che differiscono, in caso che BlockChain.info sia online o meno, ossia nel caso che il sito web non risulti raggiungibile.

3.4.1. Nel caso in cui

BlockChain.info è offline

Nel caso in cui BlockChain.info è offline, è possibile utilizzare client esterni come *Multibit* (software terzo che consente la gestione dei bitcoin, come il già citato Bitcoin Core) per recuperare il saldo e le relative transazioni.

Ora è fondamentale scaricare l'installer da **multibit.org** – nel caso in esame gli autori utilizzano un sistema operativo Windows – disponibile per diverse piattaforme: Windows, Mac e Linux.

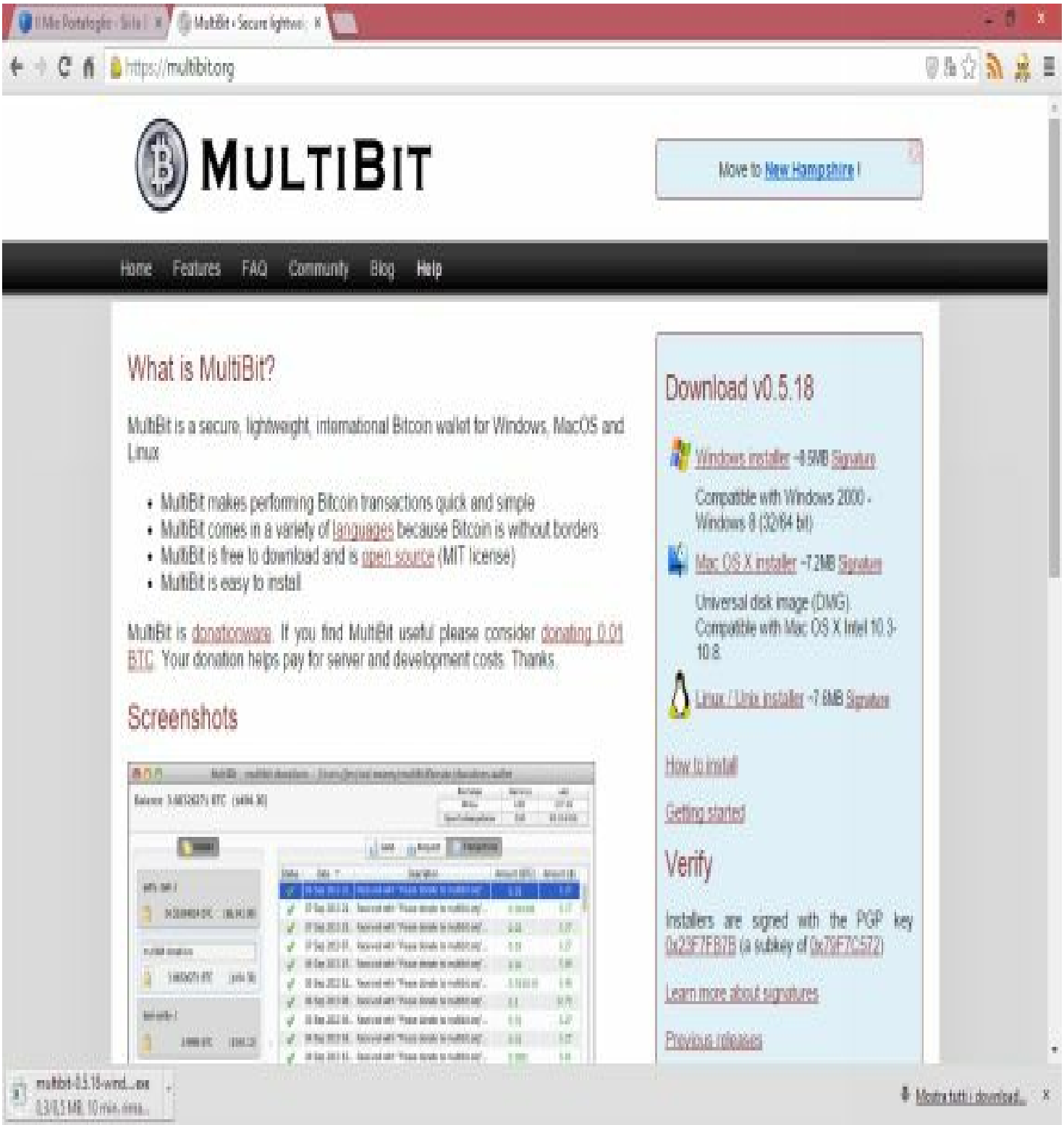


Figura 12: Homepage del client Bitcoin Multibit.

A download terminato, è possibile installare il client. Il processo di installazione non durerà più di qualche minuto.

A questo punto, avviato l'applicativo, prima di poterlo utilizzare è necessario attendere il completamento del processo di sincronizzazione con la BlockChain. Multibit, oltre a consentire tutte le operazioni di un normale wallet con la criptomoneta, mantiene costantemente aggiornato l'utilizzatore comunicando il valore di cambio bitcoin/dollari aggiornato quotidianamente (Figura 13).

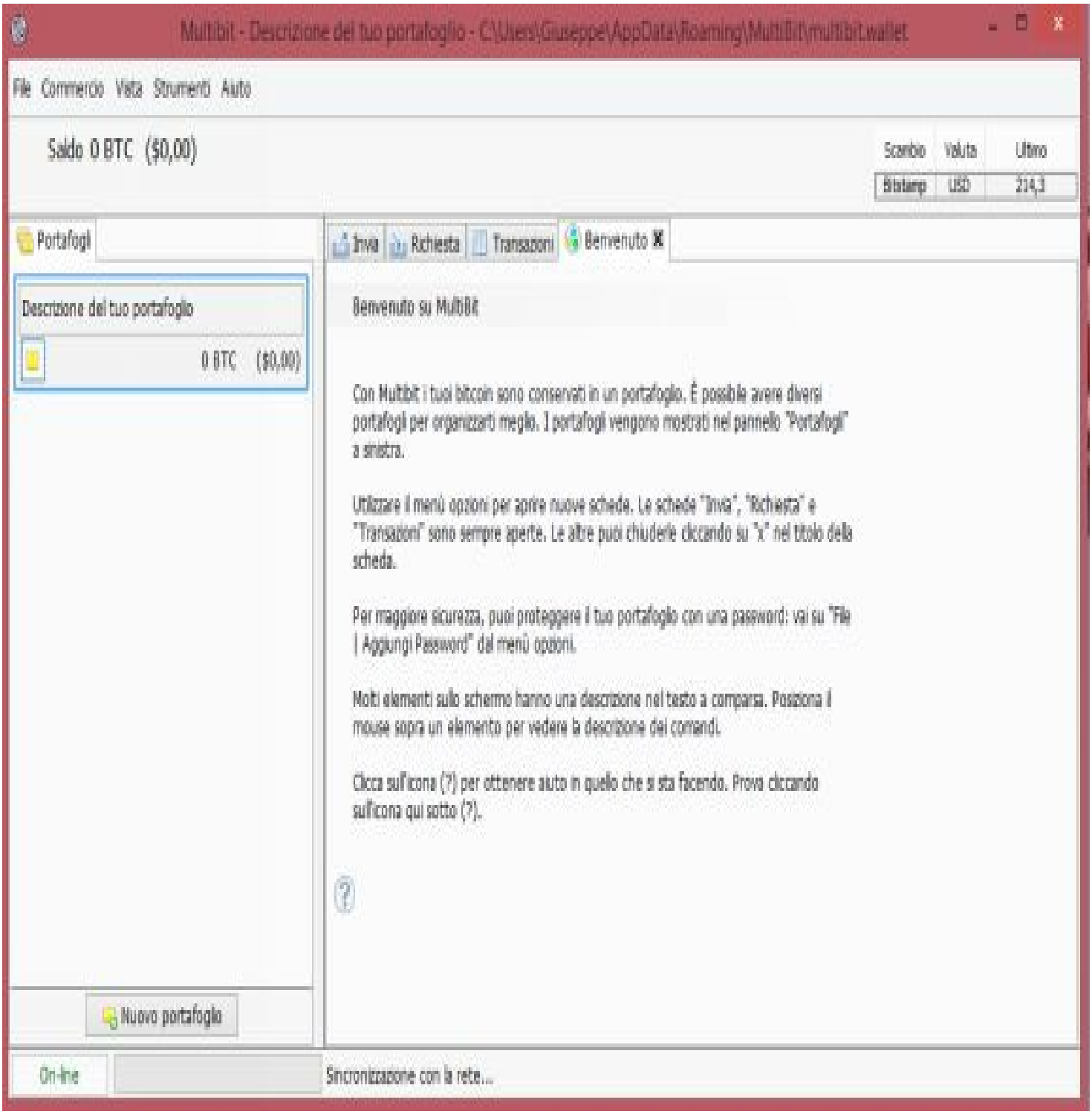


Figura 13: Interfaccia principale Multibit.

Il download della BlockChain

la prima volta richiederà molto tempo (si ricorda che si tratta di un database di oltre 20GB). Una volta terminato, sarà possibile importare il file di backup, realizzato con Blockchain.info. Si seleziona, dal menu, la voce “Strumenti” e poi “Importa chiavi private”. Il totale del conto sarà ripristinato non appena la BlockChain confermerà i bitcoin, tutto per evitare frodi.

3.4.2. Nel caso in cui BlockChain.info è online

Nel caso in cui non vi siano problemi di sorta con il sito web, per

ripristinare lo stato del wallet è possibile utilizzare il tool che il portale mette a disposizione. La soluzione consente di creare un nuovo wallet da un backup esistente.

La prima cosa da fare è collegarsi al conto, si seleziona la voce "Download" presente nella sezione "Salvataggio" posta nella parte in basso a destra del sito web. A questo punto, comparirà una schermata che consente di scegliere la modalità con la quale si vuole ripristinare lo stato del conto. Quindi si clicca su "Import wallet tool". Si aprirà una nuova scheda (Figura 14), all'interno della quale si dovrà trascinare il file di backup salvato in

precedenza.

Figura 14: Interfaccia ripristino backup da

Atteso il tempo necessario ad effettuare l'upload del file di backup verrà richiesto l'inserimento della password del precedente wallet, tutto atto a confermerà la nostra identità. Inserita la password è necessario cliccare su "Continue" e seguire le istruzioni a schermo.

3.5. LE TRANSAZIONI

Capito come mettere al sicuro la "moneta anonima", entriamo sempre più all'interno del suo funzionamento indagando su come sia possibile ricevere ed inviare bitcoin attraverso il proprio wallet. Si precisa che verrà analizzato nello specifico soltanto BlockChain.info, ma le funzioni sono specularli per la totalità dei wallet, siano essi Desktop o Web Based. Il lettore non avrà quindi problemi a scegliere la soluzione più adatta alle sue esigenze una volta comprese le opzioni disponibili.

3.5.1. Invio Denaro

Per poter inviare denaro è necessario recarsi nella sezione “Invia Denaro”. Da qui è possibile scegliere tra le diverse funzioni che il portale mette a disposizione:

- *Invio Veloce*: l’invio avviene conoscendo esclusivamente l’indirizzo bitcoin (indirizzo alfanumerico o QR Code) del destinatario ed inserendo l’ammontare di bitcoin da spedire (in real time è possibile valutare il corrispettivo in euro dell’ammontare della cifra inviata);

- *Moneta comune*: questa opzione è peculiare di BlockChain.info, e consta in una maggiore protezione della privacy nell'effettuare il trasferimento di BTC, in ragione del fatto che BlockChain.info rimane comunque un servizio terzo che si interfaccia tra la rete Bitcoin e l'utente. Questa opzione non si rende necessaria se si utilizza un wallet Desktop. Il servizio "moneta comune" ha un costo compreso tra lo 0.5% e l'1% della somma inviata. In concreto, maschera le transazioni e le rende incomprensibili in caso di controlli;

- *Personalizzata*: è possibile selezionare da un elenco di indirizzi, precedentemente salvati, a chi e quanti bitcoin inviare. E' previsto il pagamento di una commissione, il cui importo è fornito prima che si concluda la transazione. Inoltre, è possibile allegare all'invio dei bitcoin un messaggio al destinatario (analogo alla causale in un bonifico bancario, tuttavia pubblico a chiunque consulti la BlockChain);

- *Invio a mezzo mail*: è possibile inviare bitcoin inserendo semplicemente l'indirizzo e-mail del

destinatario e l'ammontare di bitcoin da inviare, sarà BlockChain.info a preoccuparsi di tutto il resto;

- *Invio a mezzo sms*: è possibile inviare bitcoin utilizzando gli sms. È sufficiente inserire il paese della persona a cui si intende inviare bitcoin, il numero di telefono e l'ammontare della somma da inviare. BlockChain.info si preoccuperà di notificare il beneficiario.

3.5.2. Ricezione Denaro

Ricevere bitcoin è

un'operazione semplicissima. È sufficiente condividere la stringa alfanumerica univoca, ed attendere di ricevere il pagamento in completo anonimato. Alternativamente, per semplificare l'intera procedura, ed evitare fastidiosi copia-incolla, è possibile creare un QR Code (Figura 15). Scansionando quest'ultimo con smartphone, o altri device, il debitore potrà inviare immediatamente il pagamento della cifra in BTC prestabilita.

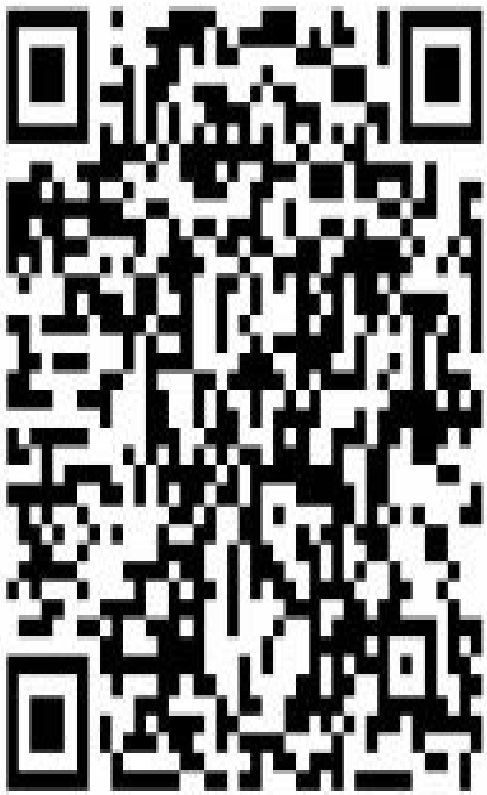
BlockChain.info consente all'utente di creare una richiesta di pagamento, contenente anche il QR Code, in tutta semplicità. Basta recarsi

nella sezione “denaro” e compilare il form corrispondente.

Create Payment Request

Usa questo modulo per richiedere a qualcuno di inviarti dei bitcoin o anche solamente per mostrare alle persone che hai un indirizzo bitcoin.

Importo: BTC 0.01 = EUR 1.89



Close

Request Payment into address 1DAtzAqMM64pgLEC2419Tk9xQb6Ah6T7aF

Figura 15: QR Code generato automaticamente da Blockchain.info

3.5.3. Movimenti sempre presenti

In qualunque momento è possibile monitorare, accedendo al wallet, lo storico dei movimenti, il tutto in maniera abbastanza simile a quanto avviene utilizzando i circuiti bancari.

Per consultare la lista dei movimenti basta effettuare l'accesso all'area personale, per poi recarsi nella sezione "Le mie Transazioni".

Cliccando sull'indirizzo bitcoin,

presente nell'elenco delle transazioni, è possibile accedere ad informazioni in merito al conto con il quale si è avuto un rapporto scambio. Una finestra (Figura 16) indicherà il numero di conferme ricevute della transazione, ed inoltre avviserà se si è trattato di una "Doppia Spesa" (come descritto nel Capitolo 2).

Transaction Summary

Hai Ricevuto

0.0003038 BTC ($ 0.07)

Valore alla Data della Transazione $ 0.07

Hash	3ed1a820880c7cdbda5fd4cbb...
Orario di Invio	2015-02-01 17:15:26 (+0 minuti da confermare)
Conferme	437 Conferme
Dippia Spesa	Non è stata rilevata un Doppia Spesa
Commissione di Transazione	0.0004 BTC

Close

Figura 16: Sintesi transazione in BTC.

3.5.4. Tempi e costi di una transazione

Ricevere un pagamento con BItcoin è quasi istantaneo. Mediamente, sono necessari 10 minuti prima di che la rete inizi a confermare la transazione, includendola nel blocco e dando la possibilità di spenderla.

La maggior parte delle transizioni non ha alcun costo di commissione, ma molto spesso gli utenti pagano qualche percentuale infinitesimale di BTC per avere una

maggiore velocità nelle conferme.

Le commissioni di transazione sono utilizzate come protezione, quindi a pieno vantaggio di chi usa i BTC, contro i malintenzionati che inviano transazioni solo per intasare la rete. Le commissioni non sono applicate in funzione della somma da trasferire, paradossalmente chi trasferisce 0.002 BTC si troverà a pagare quasi la stessa commissione di chi invia 100 BTC.

3.6. IMPORTA/ESPORTA INDIRIZZO BTC

BlockChain.info, in accordo ai suoi principi di wallet, consente ai propri utenti di gestire più indirizzi BTC all'interno di un unico portafoglio. Per importare un indirizzo BTC all'interno del wallet è sufficiente recarsi nella sezione "Importa/Esporta", e compilare il form come quello in Figura 17.

Due sono le informazioni richieste dal wallet per poter gestire, in completa libertà, i propri BTC presenti su più indirizzi: *bitcoin address* e

private key. La prima (il bitcoin address) consente di individuare il conto tra la moltitudine presenti all'interno della BlockChain; la seconda (la private key) consente di confermare il possesso dell'indirizzo BTC. Nel caso non si disponga di entrambe le informazioni, sarà possibile solo osservare le transazioni che coinvolgono l'indirizzo senza poter operare con lo stesso.

Gli autori hanno preferito entrare nel dettaglio, e capire come estrarre la chiave privata di un indirizzo bitcoin utilizzando sia un wallet Desktop (Multibit ed equivalenti) che uno Web Based (BlockChain.info e similari).

Chiave privata su wallet

Desktop: per estrarre la chiave privata associata ad un particolare indirizzo BTC è sufficiente recarsi nel menu "Strumenti" per poi cliccare su "Esportare le chiavi private", da qui selezionare il percorso nel quale salvare il file contenente la key. Alcuni wallet consentono di corredare il file con una password, in modo da proteggerne il contenuto da malintenzionati. Per conoscere la chiave basterà utilizzare un qualunque editor di testo, come Notepad++.

Chiave private su wallet Web Based: per estrarre la chiave privata associata ad un determinato indirizzo BTC è sufficiente recarsi

BlockChain.info, da qui spostarsi nella sezione “Importa/Esporta”. Dal menu a sinistra, selezionare la voce “Esporta Cifrato” o “Esporta Decifrato”, che rispettivamente restituiranno la chiave privata in formato testuale cifrato o meno.

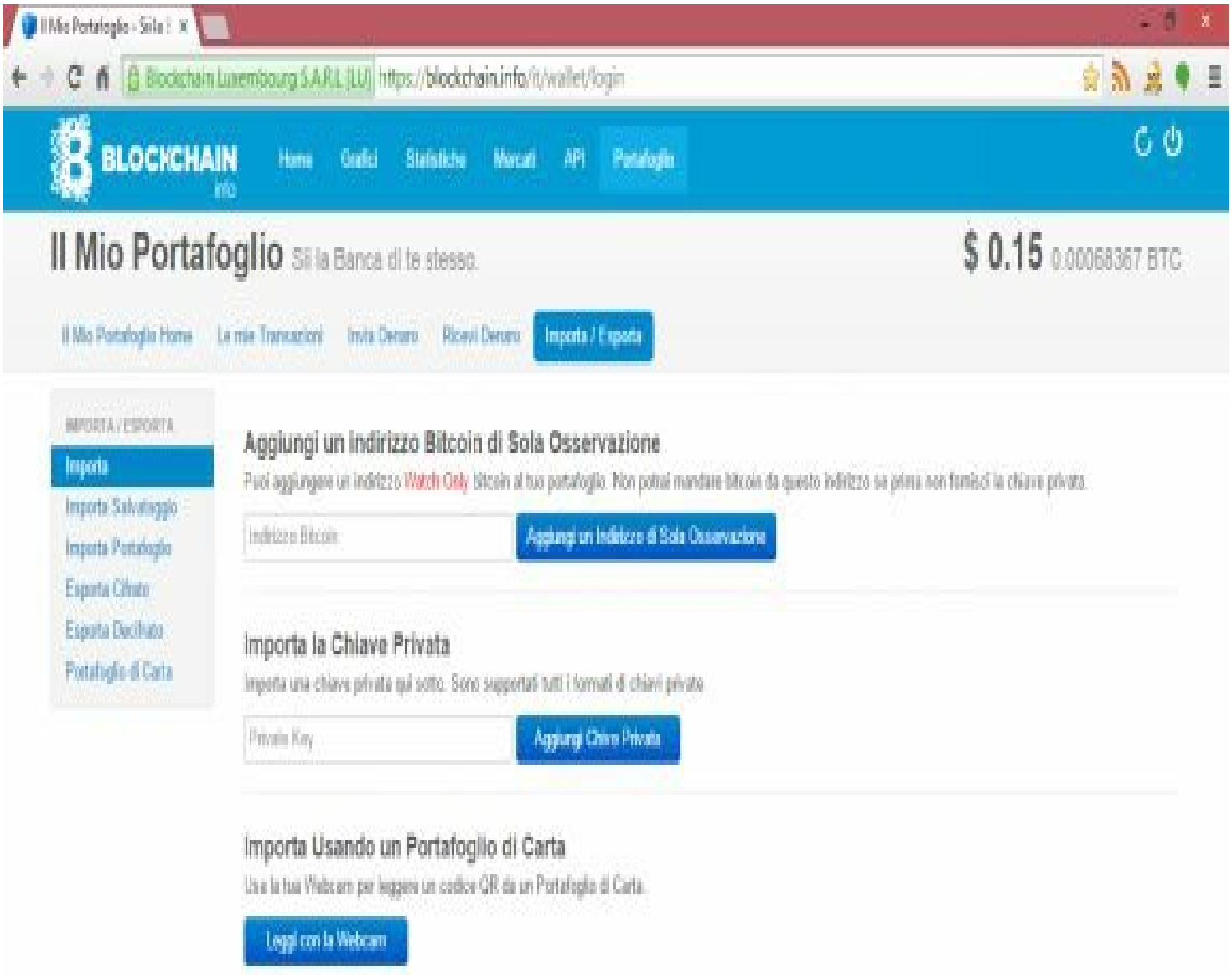


Figura 17: Sezione di BlockChain.info per l'importazione di un altro indirizzo Bitcoin.

Utilizzando la funzione "Importa Salvataggio" di BlockChain.info, è possibile monitorare i backup richiesti

al portale e, all'occorrenza, decidere se importarne il contenuto utilizzando la funzione "import".

3.7. LO MNEMONICO (DI BLOCKCHAIN)

Lo mnemonico non è altro che un file .pdf realizzato all'atto della creazione di un indirizzo bitcoin. E' costituito dal link per il login al wallet (Figura 18).

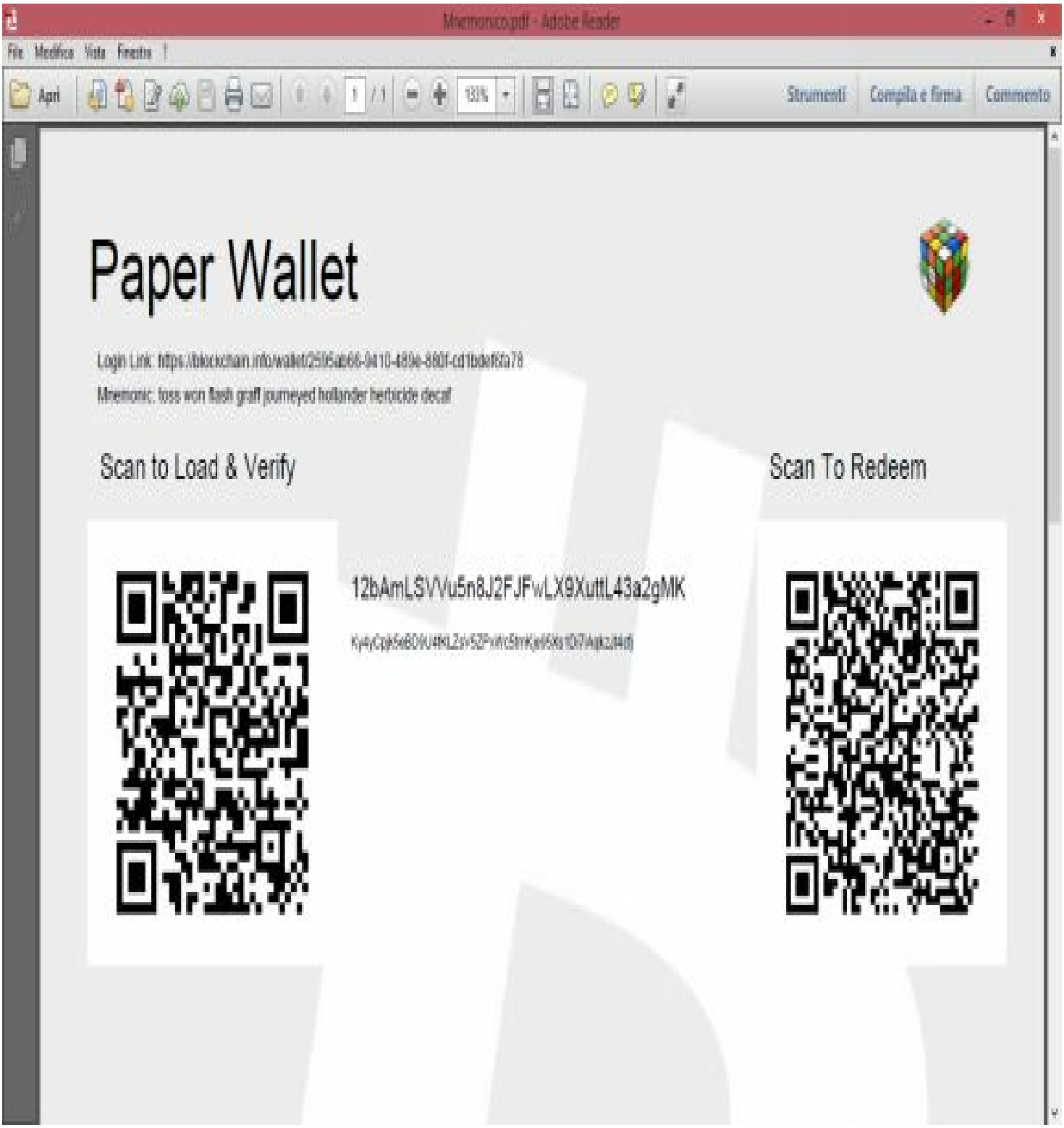


Figura 18: Print Screen dello mnemonico generato da BlockChain.info

Inoltre, sono presenti:

- *L'indirizzo bitocoin*: attraverso il quale possiamo ricevere BTC;

- *La chiave privata*: utile per l'utilizzo dell'indirizzo bitcoin anche su altri wallet e per recuperare le credenziali di accesso al conto;

- *QR Code*: come sostituto del link, se si preferisce accedere tramite smartphone.

Chiara la struttura del file, è di importanza rilevante capire le ragioni

per le quali questo documento è cruciale per la vita del conto. Si tratta dell'unico strumento utilizzabile per accedere all'account. In caso di smarrimento dello mnemonico, i bitcoin in posseduti su BlockChain.info andranno persi per sempre.

CAPITOLO 4

GUADAGNARE BITCOIN

In questo capitolo gli autori affronteranno i migliori metodi che consentono, in maniera semplice e veloce, di guadagnare Bitcoin, senza troppi dispendi energetici e/o temporali che affliggono il processo del *mining* (vedi Capitolo 2). Le tecniche affrontate, suddivise in categorie – al fine di garantire una migliore leggibilità – verranno trattate con ampio dettaglio. Esempi pratici anticiperanno i concetti teorici. Ogni categoria verrà analizzata con ampio giudizio critico al fine di rendere chiaro al lettore i pro e contro.

Al termine di ogni categoria è

presentato un elenco dei migliori siti web, presenti in rete, che utilizzano quella particolare tipologia di marketing per elargire BTC ai propri utenti.

4.1. BITCOIN: UNA GRANDE VALUTA

Prima di poter indagare sul mondo Bitcoin, capire quali sono le strade che consentono di guadagnare BTC in maniera veloce e senza troppi pensieri, è necessario tenere bene a mente una cosa: la moneta, rapportata alle principali valute internazionali (euro, dollaro, e tante altre), è una moneta “forte”. Con queste parole, forse un po’ troppo criptiche, gli autori vogliono semplicemente dire che la moneta ha un elevato valore unitario, oggi 1 BTC equivale a circa 225 €. Per tale ragione è necessario conoscerne i

sottomultipli, il loro valore e soprattutto il loro nome.

Dunque, volendo fare una suddivisione:

- *1 BTC*: è l'unità della moneta. Per via dell'alto valore unitario, difficilmente si sente parlare di centinaia di BTC ed ancora più di rado si sente parlare di migliaia di BTC;

- *1 mBTC (milli-bitcoin)*: sono l'equivalente di 0.001 BTC, circa 0.20 € (rifacendoci all'attuale tasso di cambio, è possibile consultarlo su

BlockChain.info);

- *1 μBTC (micro-bitcoin)*: sono l'equivalente di 0.000001 BTC, circa 0.0002 €;

- *1 Satoshi (in omaggio al creatore della moneta)*: sono l'equivalente di 0.00000001 BTC, circa 0.000002 €. E' la più piccola quantità di BTC che è possibile scambiarsi in rete.

Conoscere i sottomultipli della moneta costituisce il metro di giudizio con il quale valutare i tanti siti che promettono guadagni elevati, ma talvolta

non fanno fede alle loro promesse. Si precisa che queste considerazioni non riguardano i siti web segnalati all'interno di questo e-book, che sono stati testati dagli autori, e quindi sicuri.

4.2. TANTE CATEGORIE, QUALE LA PIÙ CONVENIENTE?

Girando per il web, gli autori hanno scoperto tanti siti che promettono di far guadagnare BTC, alcuni semplicemente cliccando su banner pubblicitari, altri, invece, sfidando la fortuna. Gli autori hanno deciso di raggrupparli in sei categorie:

- *Pagati per click*: siti web che, sotto la visione di spot o click su banner pubblicitari, elargiscono BTC in funzione della "campagna marketing"

a cui appartengono i banner stessi, si capirà in seguito cosa questo significhi;

- *Rubinetti*: siti web che "regalano" BTC ad intervalli regolari di tempo (15, 30 o 60 minuti). Proprio grazie ad uno di questi, gli autori hanno sviluppato un metodo speculativo che verrà affrontato in un capitolo a sé stante (vedi Capitolo 5);

- *Pagati per…:* siti web che elargiscono BTC in cambio di sponsorizzazione sui maggiori Social Network, attraverso account personali o creati per l'occasione;

- *Giochi a premi in BTC*: siti web che sfruttano giochi flash, simili a quelli che si trovano su Facebook, che invogliano a visitare i loro portali, elargendo BTC in maniera proporzionale alla bravura dimostrata nel gioco;

- *Scommettere Bitcoin*: siti di scommesse veri e propri che accettano la criptovaluta come mezzo di pagamento e che, a loro volta, utilizzano la valuta digitale per pagare le vincite;

Queste sono le tipologie più

diffuse in rete, ciò non toglie che sia possibile scovarne altre che utilizzano strategie diverse per attirare utenti e "pagare" la loro attenzione in BTC. Tutto è legato alla diffusione della moneta, più la moneta diventerà di uso comune, più siti di questo tipo diventeranno all'ordine del giorno.

Si precisa che tutti questi servizi erogatori di bitcoin a titolo "gratuito" basano il loro *business model* sulla pubblicità. Infatti, è grazie alla permanenza dell'utente su tali portali che i banner pubblicitari remunerano tutti questi siti web, i quali condividono parte dei guadagni sotto forma di bitcoin con i propri iscritti.

4.3. REFER LINK

Sulla stessa scia di quanto accade con i maggiori e-commerce, come Amazon ed il suo programma di affiliazione, è possibile guadagnare qualche BTC extra utilizzando i **refer link**. Si tratta di un programma abbastanza semplice, che premia nel lungo periodo, coloro che si prodigano nel pubblicizzare i portali di cui fanno parte.

Dunque i siti web che elargiscono BTC propongono ai loro utenti la possibilità di mettersi in tasca qualche BTC extra in cambio di iscritti. Per dimostrare la paternità dei nuovi

utenti, il sistema richiede, in fase di registrazione, l'inserimento di un codice (il **refer link**) univoco del promotore. Il nuovo utente dovrà inserire il refer link nell'apposita casella di testo, oppure utilizzarlo quale link ipertestuale per collegarsi al sito web, per poi effettuare la registrazione.

Gli autori hanno ritenuto, essendo un'ottima strategia, spiegare in maniera più dettagliata come sfruttare questo metodo per guadagnare BTC extra.

4.3.1. Come utilizzarli

La struttura tipica di un refer

link è http://example.it/?r=1244, dove al posto di "*example*" si trova il nome del fruitore del servizio, colui che elargisce BTC.

Collegarsi al portale, ad esempio **FreeBitco.in** (Figura 19), sul quale si suppone di già aver effettuato la registrazione. Si è scelto questo sito web, appartenente alla categoria "rubinetti", perché è lo stesso utilizzato per l'indagine speculativa.

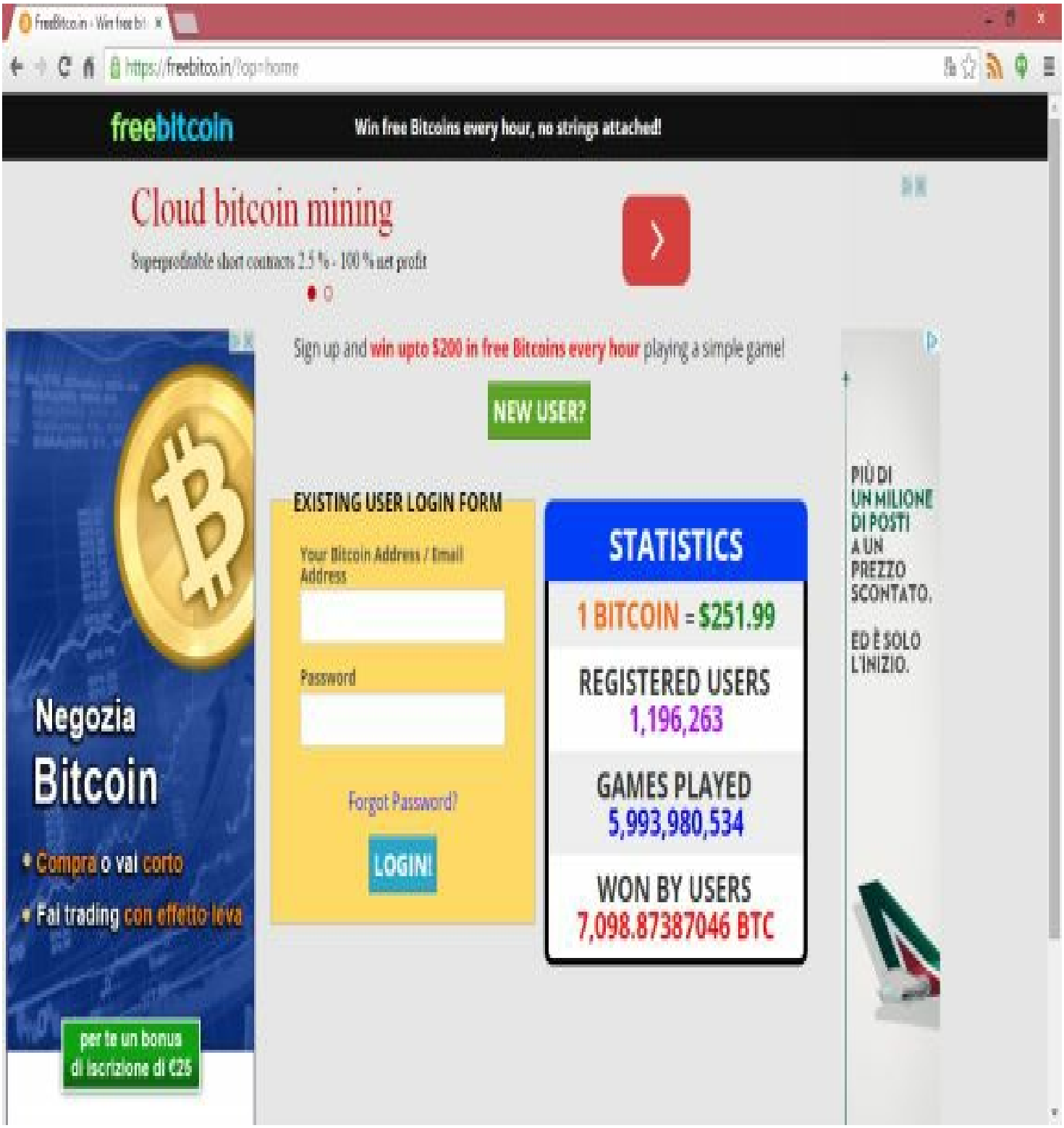


Figura 19: Home page FreeBitco.in

Cliccando sulla sezione

“Refer”, si ha accesso alla casella di testo contenente il refer link (Figura 20).

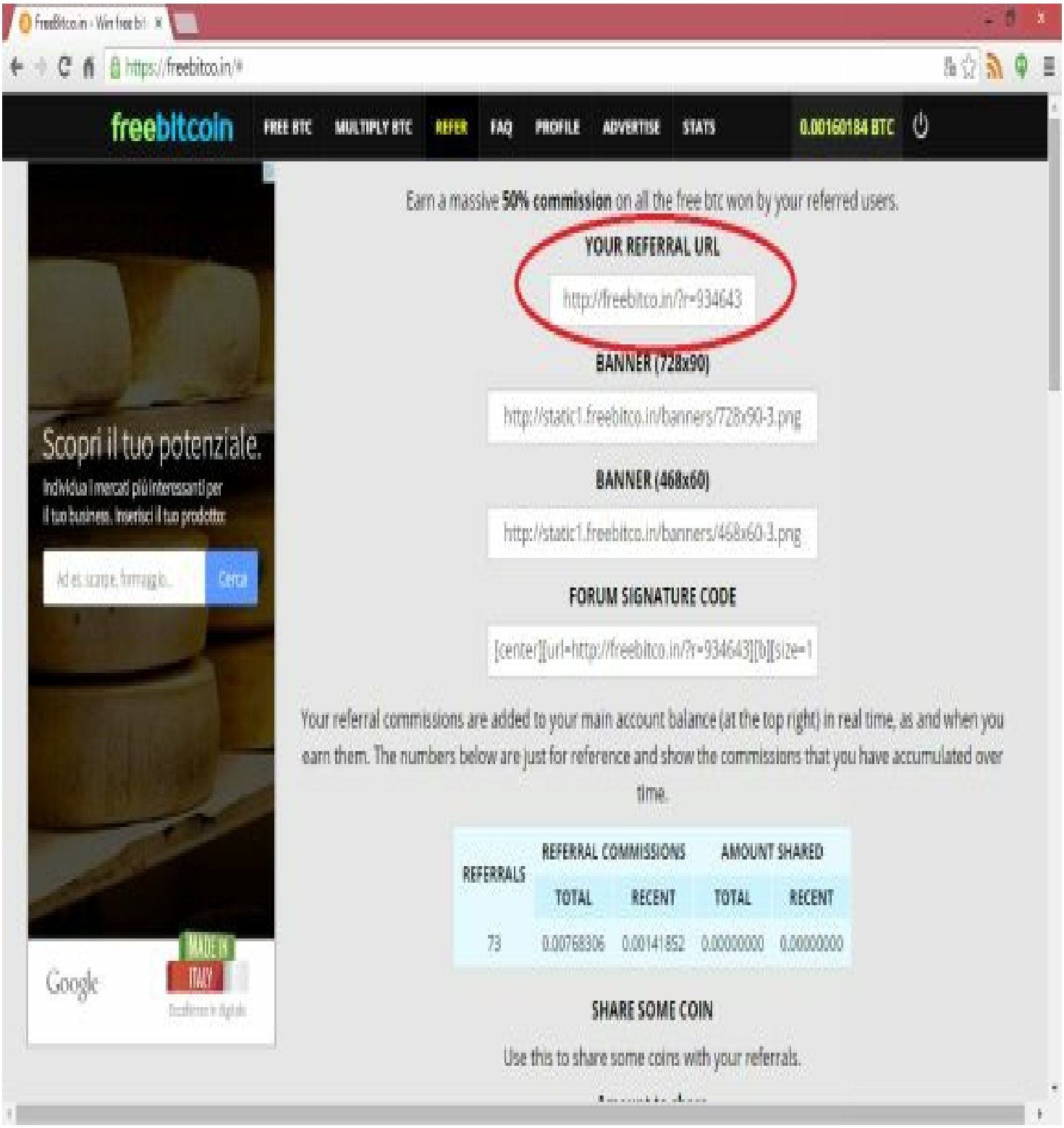


Figura 20: Casella di testo contenente il Refer Link.

A questo punto, per accedere al premio, è sufficiente invogliare qualche amico ad entrare a far parte del portale. Si può decidere di inviare il refer link via Facebook, e-mail, whatsapp, e così via. Se grazie al refer link si darà seguito ad una nuova registrazione, il promotore riceverà **per sempre** BTC extra, proporzionali all'attività del "ref-user" (ossia colui che si è registrato tramite refer link).

4.3.2. Pro e Contro

Le modalità con cui vengono distribuiti gli extra variano da sito a sito. In generale sono proporzionali non solo al numero di iscritti, indotti attraverso il refer link, ma anche all'attività che gli utenti svolgono sul portale. Ad esempio, FreeBitco.in concede una "provvigione" pari al 50% delle entrate realizzate dai nuovi iscritti.

Dunque, i refer link non costituiscono di certo l'ottimo, se l'obiettivo è speculare con i Bitcoin, ma consentono di accumulare, nel lungo periodo, un bel po' di BTC extra.

Inoltre, si tratta di un'attività poco dispendiosa, in termini di tempo. E' sufficiente inviare, utilizzando il

mezzo che più si preferisce, un semplice link. In questo modo si ha la possibilità di guadagnare qualche BTC e, a allo stesso tempo si diffonde la conoscenza della criptomoneta.

4.4. PAGATI PER LINK

Come anticipato nel Paragrafo 4.3, la categoria "**pagati per link**" è costituita da siti web che premiano, i propri utenti, in BTC sulla base del numero di click che effettuano su banner pubblicitari, o del tempo che spendono nella visione di spot commerciali. Il più conosciuto in questo settore è **BitVisitor**. Il noto portale promette guadagni strabilianti a tutti i partecipanti.

4.4.1. Come Funziona

Come prima cosa ci si collega a **BitVisitor** (Figura 21) utilizzando un normale browser per internet come Google Chrome.

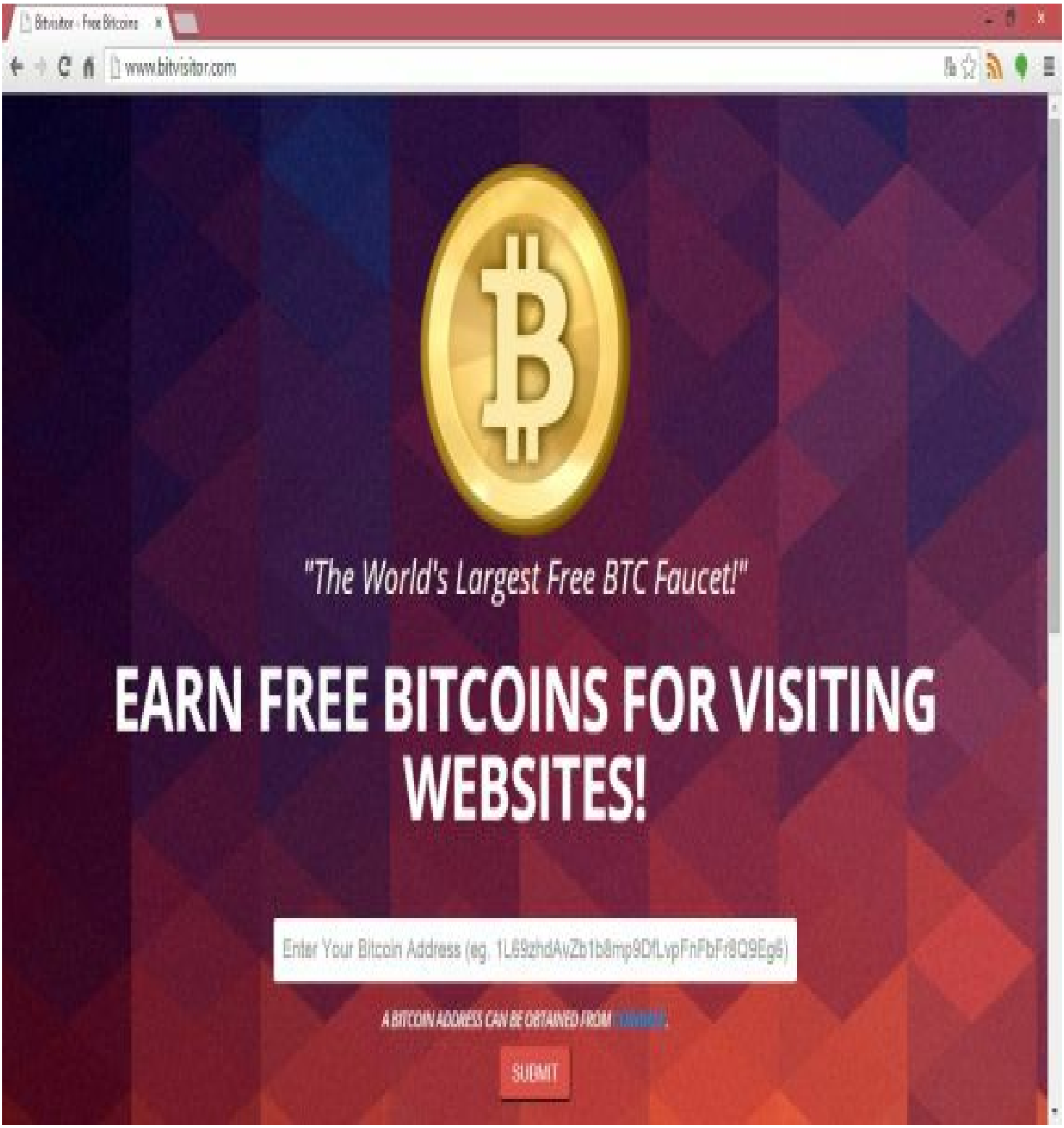


Figura 21: Home page BitVisitor.

Si inserisce l'indirizzo Bitcoin

(sul quale si vuole ricevere l'accredito) nella casella di testo e si clicca su "Submit". Il sito web, in linea con la filosofia della criptovaluta, non ha bisogno d'altro e invita subito a guadagnare risolvendo il captcha, necessario per sbloccare la visione dei banner.

Per poter riscattare il premio è sufficiente mantenere aperta la scheda del browser contenente il banner di BitVisitor per una durata di 5 minuti. Nel caso in cui venga chiusa prima che sia trascorso tutto il tempo, non si avrà diritto ad alcun BTC.

Avuto accesso al banner (Figura 22) si può continuare ad utilizzare il

computer, svolgendo le normali attività quotidiane. Infatti, non è richiesto di guardare i contenuti pubblicitari o quantomeno non è implementato alcun controllo di questo tipo.

Al termine dei 5 minuti (o in generale un certo lasso temporale), un beep (eseguito dallo script presente all'interno pagina) ricorderà che il tempo è trascorso. A questo punto, risolvendo nuovamente il captcha, si potrà accedere alla visione di un nuovo banner, guadagnando altri BTC.

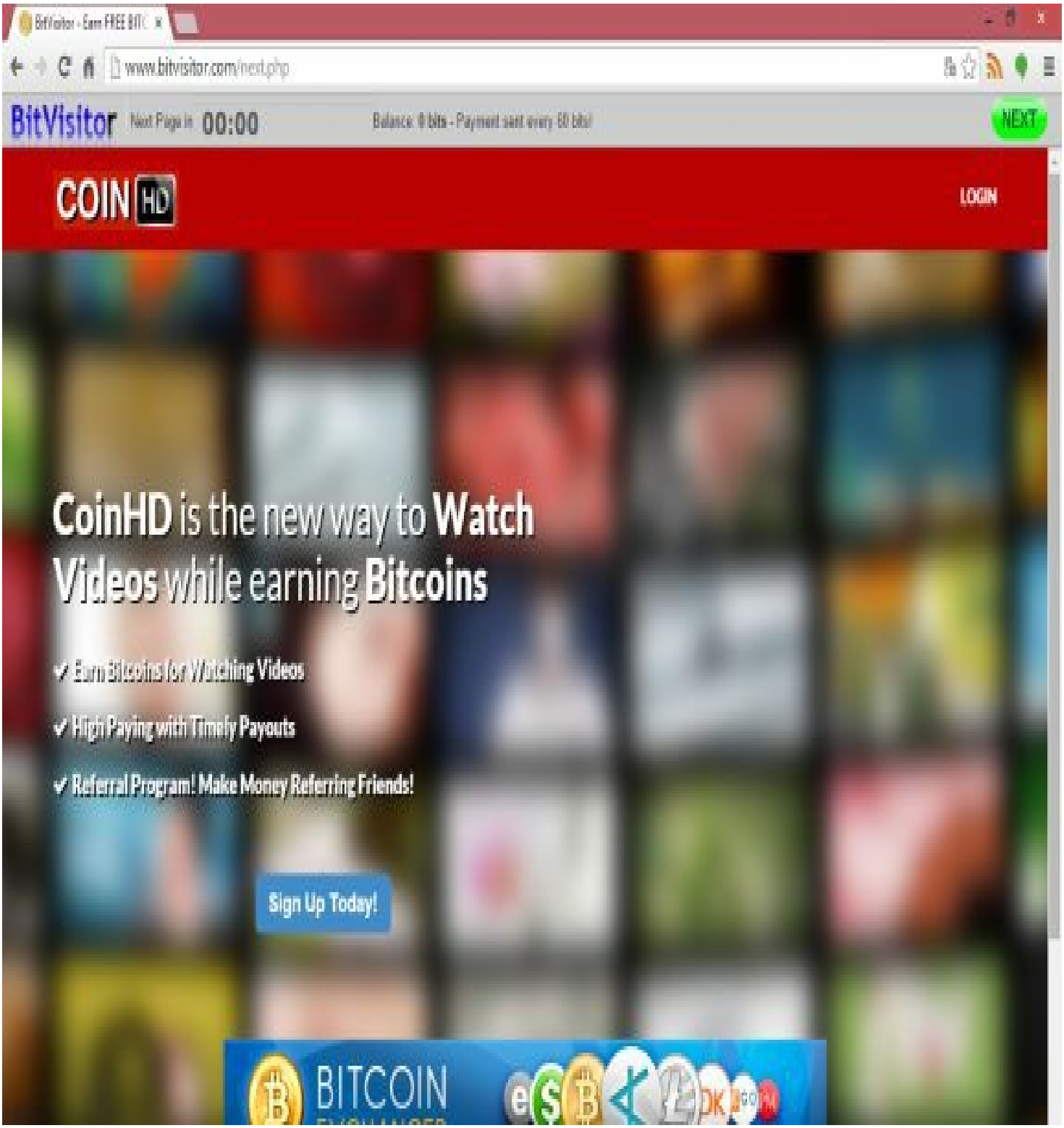


Figura 22: Banner di BitVisitor.

Raggiunti i 60 µBTC – il lettore

incomincerà a comprendere l'importanza di conoscere i sottomultipli della moneta – si potrà procedere al payout, ovvero al trasferimento sul conto Bitcoin.

Il sistema non richiede username o password di accesso, utilizza il *Bitcoin address* per identificare l'utente. Difatti, è sufficiente ogni qual volta si accede al portale, indicare esclusivamente l'indirizzo Bitcoin sul quale si vuole ricevere l'accredito. Il sistema di BitVisitor aggiungerà i nuovi guadagni ai precedenti.

4.4.2. Pro e Contro

Dopo giorni di utilizzo, combinando anche i guadagni derivanti dai refer link, gli autori hanno formulato le valutazioni al riguardo.

È sembrato un sito web poco reattivo, consente di guadagnare in giornate buone meno di 0.001 BTC (circa 0.50 €), a causa del funzionamento intrinseco del sistema che richiede tempi di attesa minimi di 5 minuti.

Gli autori sconsigliano vivamente questo sito a chi ha poco tempo da dedicare. Tra i pro si cita la puntualità, il pagamento è arrivato non appena raggiunta la somma minima per

il payout; tra i contro si collocano i guadagni irrisori che non ripagano del tempo passato ad aspettare il prossimo banner.

Sicuramente è un'opzione da tenere in considerazione se si sta sempre vicino al computer, per i motivi più disparati, ma non può essere utilizzata da chi accende il computer di rado e/o chi non ha voglia di aspettare cinque minuti per guadagnare qualche millesimo della valuta digitale.

Infine, molti siti web utilizzano il sistema delle campagne. Tale sistema dà la possibilità all'utente di selezionare i banner da una lista, differenziati in termini di remunerazione e tempi di

visione necessari. Il concetto è il medesimo del sistema affrontato in questo paragrafo, l'unica differenza risiede nel fatto che l'utente, in base alla sua disponibilità, ha la facoltà di selezionare il banner con il rapporto tempo di visione/remunerazione che più si addice ai suoi obiettivi.

4.4.3. I più importanti

Come preannunciato all'inizio del capitolo, ecco una lista dei siti web più diffusi per questa particolare categoria. Ogni sito web è accompagnato da una piccola descrizione in modo che il lettore possa

scegliere quello più adatto alle proprie esigenze:

- *BTCClicks (https://btcclicks.com/)* – Il sito web non è secondo a nessun altro, tenendo in considerazione la mole di banner presenti.

- *CoinAdder (http://coinadder.com/index.php/)* – Da poco sul web, rispetto ai pari della categoria, consente di guadagnare 0.1 mBTC al giorno. Elargisce un bonus all'atto dell'iscrizione ed un'elevata provvigione per gli iscritti tramite refer link.

- *BittoClick (http://bittoclick.com/)* – Serio ed affidabile, ha il vantaggio di non imporre soglie elevate per il payout, se paragonato a molti suoi concorrenti.

- *Visitbit (http://visitbit.com/)* – Spesso sottovalutato, molto simile a BitVisitor, paga di più per singolo banner ma ha tempi di visione più lunghi.

4.5. RUBINETTI

I rubinetti, o nel gergo **faucets**, elargiscono BTC lasciando il tutto nelle mani del fato. Basano l'assegnazione di BTC, che vanno da 800 Satoshi ai 0.8 BTC, sull'estrazione di un numero. A seconda che il numero estratto sia compreso in un intervallo piuttosto che un altro, sarà assegnato un premio diverso definito a priori, prima di avviare il gioco. Si tratta di un metodo molto semplice che è ripetibile solo dopo un dato lasso di tempo (differente da portale a portale).

Come di rigore, gli autori passeranno prima attraverso un esempio

di utilizzo, per poi illustrarne i pro e i contro, ed infine dando un elenco dei portali più affidabili.

4.5.1. Come Funziona

Il sito più comune in questo ambiente è **FreeBitcoin** (https://freebitco.in/?op=home). Al contrario di quanto accade per i "**Pagati per link**", è necessario registrarsi al portale prima di procedere all'accumulo di BTC. Sono necessari solo pochi dati:

- *Indirizzo Bitcoin:* sul quale verranno accreditati i guadagni provenienti

dalla ruota della fortuna;

- *E-mail*: sulla quale si riceveranno tutte le comunicazioni di carattere tecnico e commerciale.

Registrati al portale ed effettuato l'accesso, cominciare a guadagnare è davvero molto semplice. È sufficiente collegarsi alla homepage del sito web, risolvere il captcha, e cliccare su "ROLL" (Figura 23). L'estrazione del numero è immediata, e la vincita viene accreditata sul conto virtuale di FreeBitco.in. Ogni fine settimana, il totale delle vincite viene trasferito in automatico sull'indirizzo Bitcoin specificato in fase di registrazione (e

sempre modificabile a discrezione dell'utente), senza dover necessariamente raggiungere un payout minimo. È possibile ripetere l'operazione ogni 60 minuti.

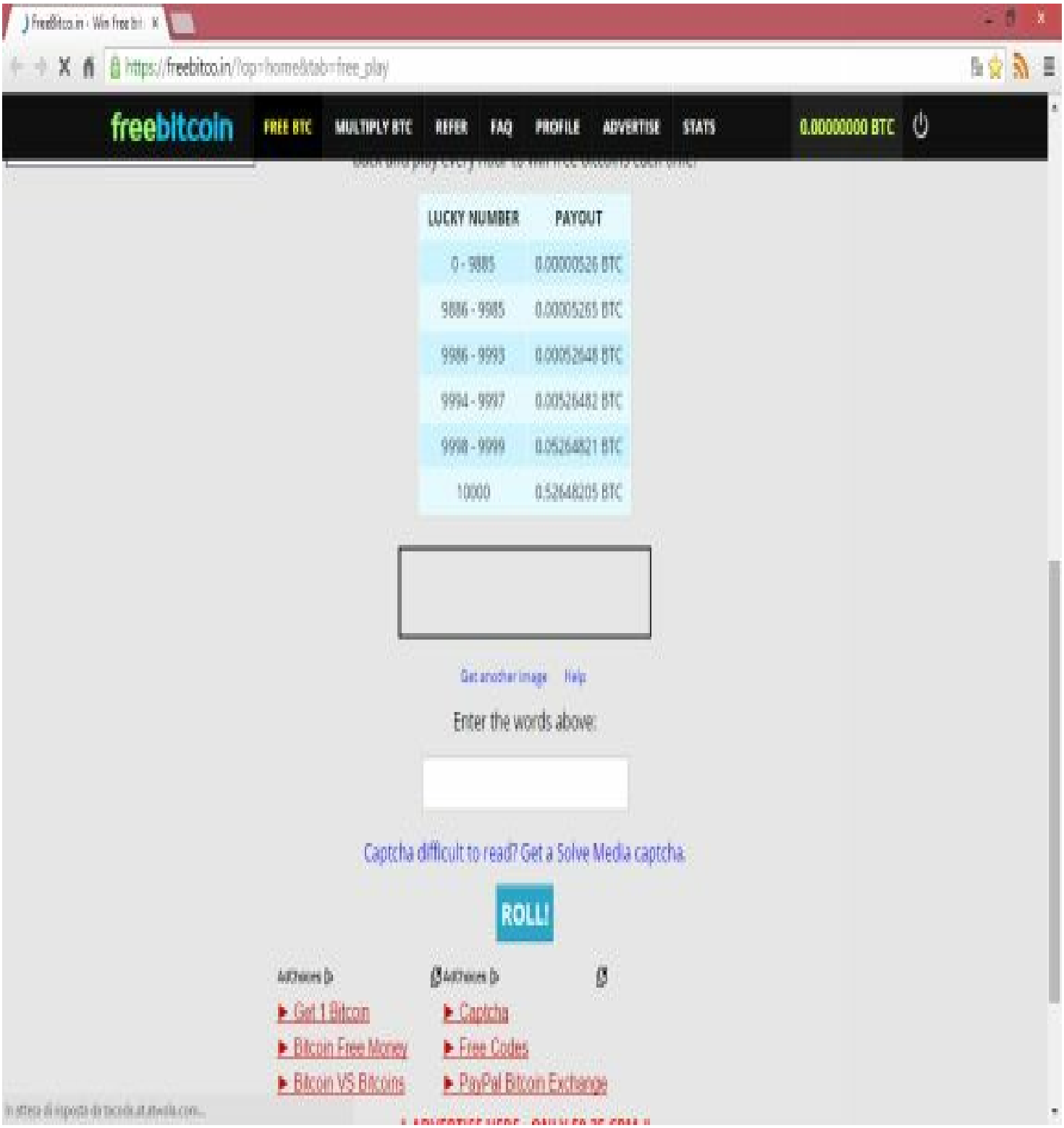


Figura 23: Estrazione dei BTC su FreeBitco.in

4.5.2. Pro e Contro

Durante le numerose prove, condotte con diversi account e diverse strategie, provando ad utilizzare anche i refer link, gli autori si sono accorti che questo servizio è davvero ottimo: anzitutto il guadagno minimo è ottenuto mediante un semplice click e senza tempi d'attesa (a differenza del servizio visto in precedenza). Ma soprattutto, è stato grazie a FreeBitco.in che gli autori hanno svolto lo studio statistico volto alla moltiplicazione sistematica dei proprio bitcoin: per approfondimenti si rimanda il lettore al Capitolo 5.

L'interfaccia è davvero

semplice ed intuitiva, ragion per cui utilizzabile senza alcun problema anche tramite smartphone. Per invogliare i propri utenti a permanere quanto più possibile sul portale, visionando il maggior numero di banner pubblicitari, FreeBitco.in mette a disposizione un simpatico giochino, presente nella sezione “MULTIPLY BTC”.

Il gioco consente di scommettere parte dei BTC ricavati, e tentare la sorte indovinando se un numero, generato in maniera casuale, sarà maggiore (HI) o minore (LOW) di una certa quantità visibile in tabella (Figura 24).

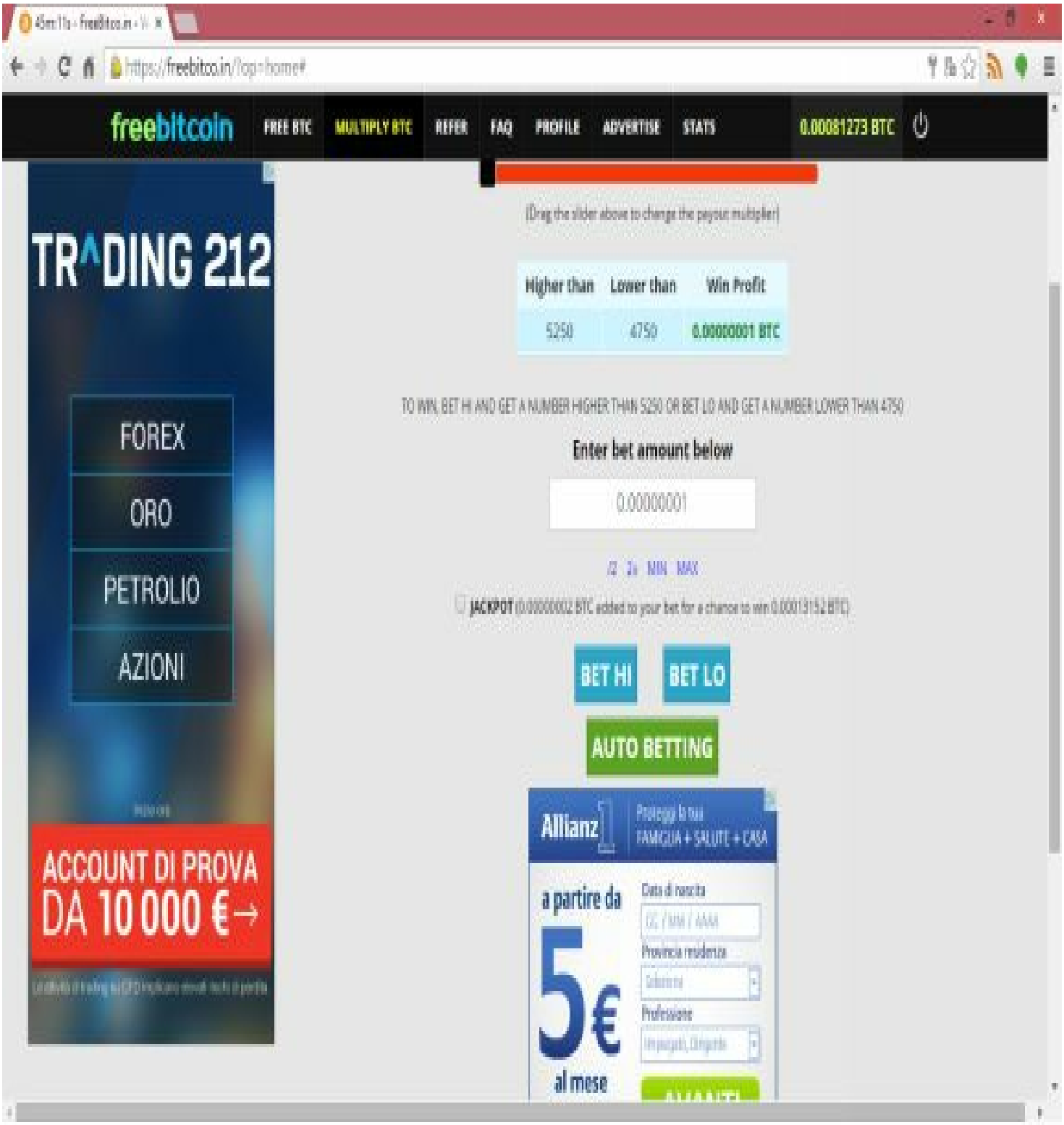


Figura 24: Sezione FreeBitco.in per la moltiplicazione di BTC.

4.5.3. I più importanti

Gli autori presentano una lista di siti web facenti parte della stessa categoria (rubinetti), che si precisa non essere gli unici presenti in rete, ma quelli con il più elevato rapporto ricavo/tempo dedicato:

- *LandofBitcoin* (*http://www.landofbitcoin.com/*) – Regala Satoshi per ogni visita e restando collegati al portale.

- *777Bitcoin* (*http://777bitco.in/*) – Sito gemello di FreeBitco.in,

permette di ricevere ogni ora µBTC. I pagamenti avvengono al raggiungimento 0.00025000 BTC.

- *DoubleBitcoins* (*http://doublebitcoins.com/*) – Ottimo portale, garantisce dai 770 ai 1'110 Satoshi all'ora. Inoltre, il portale offre dei giochini remunerativi e divertenti da non perdere.

- *ChronoFaucet* (*http://www.chronofaucet.com*) – Da poco in rete, permette di accumulare circa 1'000 Satoshi all'ora in maniera del tutto

automatica.

- *GetFreeBitcoin (http://getfree-bitcoin.com/)* – Sito clone di FreeBitco.in, permette di ricevere ogni ora da un minimo di 200 µBTC ad un massimo di 1 mBTC. I pagamenti avvengono al raggiungimento di 0.00015200 BTC.

4.6. PAGATI per…

Questa particolare categoria di siti web sfrutta l'essere sociali per far guadagnare BTC. Sicuramente, la scelta migliore per chi ha tanti amici o followers su Twitter.

Il sistema è davvero molto semplice, vengono distribuiti BTC in cambio di sponsorizzazioni sui maggiori social network. Attenzione a non condividere troppi dati personali, perché la fregatura potrebbe essere dietro l'angolo.

Anche se non molto fiduciosi di questa categoria – gli autori non credono nel business model dei social network

che promettono guadagni facili – si è creduto doveroso trattare anche questa possibilità.

4.6.1. Come Funziona

Il più famoso del settore è **Shout4Coin** (http://shout4coin.com/). Per poter iniziare a guadagnare con questo portale (Figura 25) è fondamentale disporre di un account Google o Twitter.

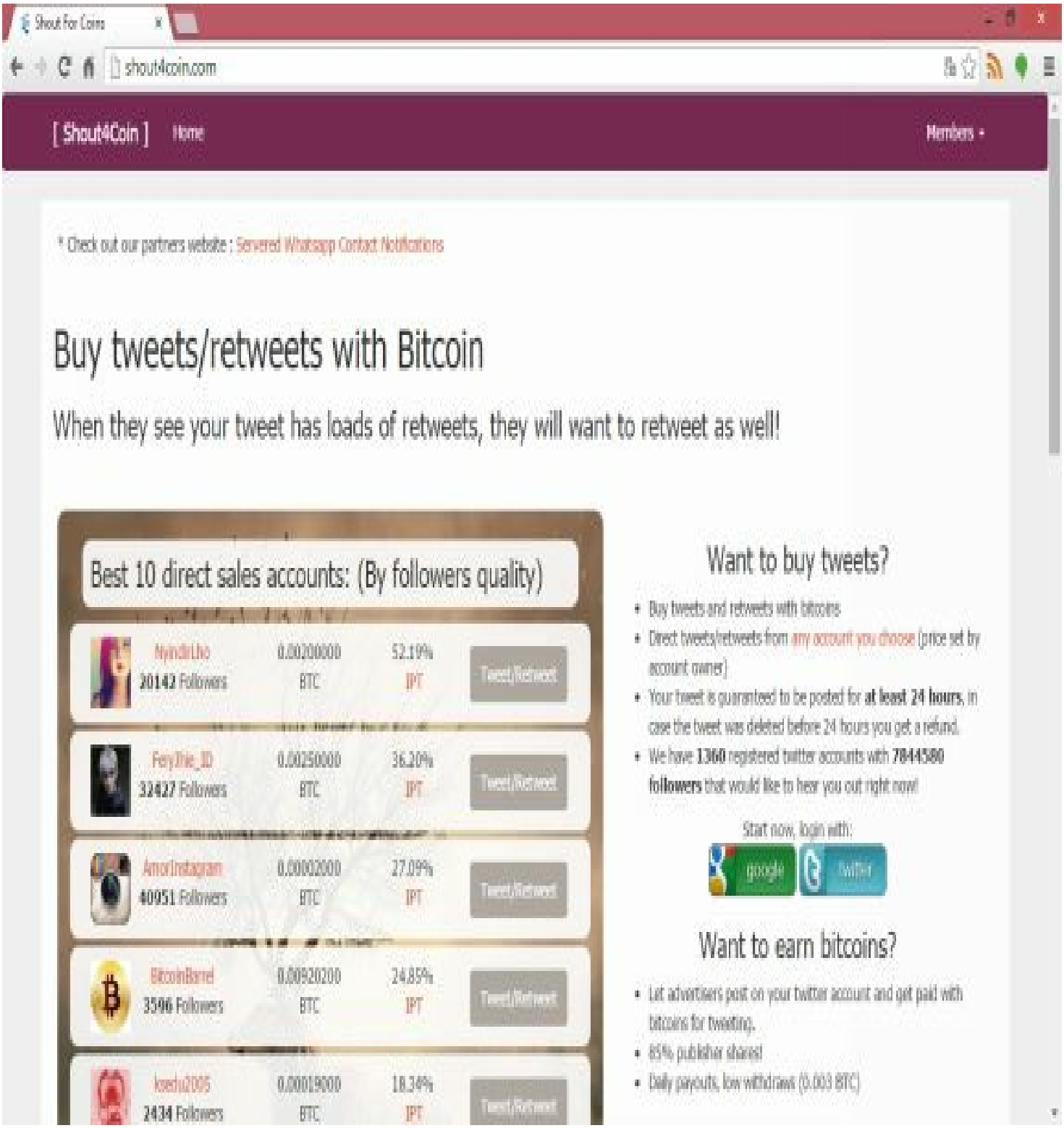


Figura 25: Home page di Shout4Coin.

Difatti, per poter accumulare

BTC è necessario dapprima effettuare l'accesso con uno di questi due portali, utilizzando gli appositi bottoni presenti sul sito web.

A questo punto per guadagnare BTC basterà twittare i messaggi (Figura 26) presenti sul portale. Appena il twitt sarà pubblicato sarà possibile visualizzare i BTC guadagnati sulla dashbord, e si potrà decidere se procedere con il payout. Più persone riceveranno il messaggio (tweet o e-mail), più BTC verranno corrisposti all'utente.

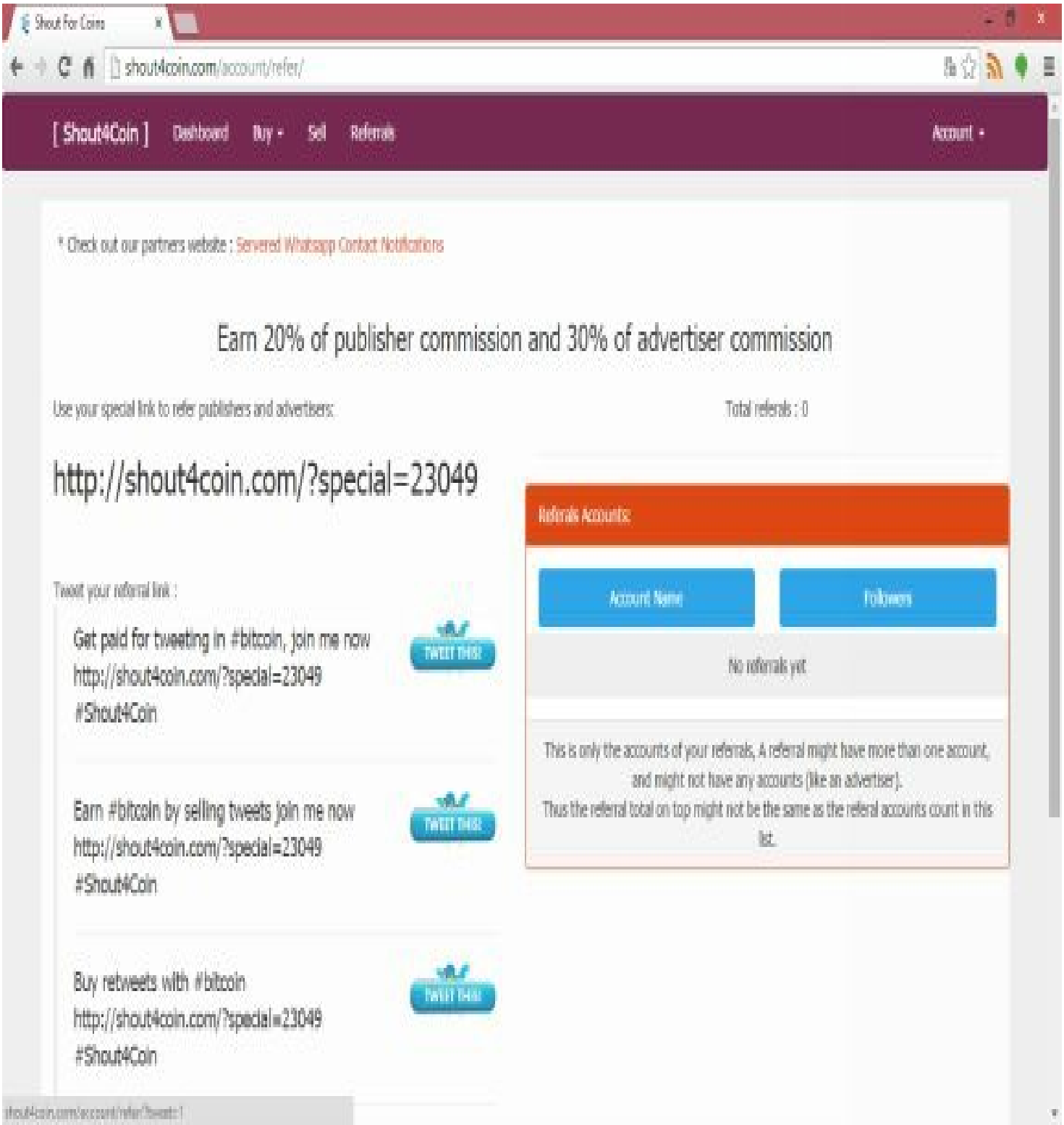


Figura 26: Pagina dalla quale è possibile decidere quale messaggi ritwittare.

4.6.2. Pro e Contro

Stilare i pro e i contro di questa categoria – a dire degli autori – è stato abbastanza semplice: di pro si è trovato ben poco.

Seppur i guadagni non siano bassi, in considerazione agli altri metodi presentati, si è ritenuto buona norma non usufruire di questo servizio.
Condividendo contenuti pubblicitari e di dubbia qualità, l'attenzione che l'utente riceverà ai propri post è destinata a calare nel brevissimo periodo, annullando di fatto ogni possibilità di guadagno, oltre a rendersi inutilmente sgradevole ai propri contatti.

Il lettore potrebbe quindi pensare di creare account fake solo per guadagnare BTC, cosa possibile ma invero poco remunerativa. Infatti, come già spiegato si viene pagati in maniera proporzionale a quante persone giunge il messaggio, in funzione del numero di followers. Risulta tuttavia difficile avere un numero elevato followers utilizzando account fake.

Essi si potrebbero acquistare attraverso servizi terzi, ma a questo punto il guadagno si annullerebbe del tutto, se non addirittura subire delle perdite. Inoltre, da tenere a mente, che i siti di questa categoria non richiedono solo ed esclusivamente di twittare

messaggi; all'occorrenza potrebbero chiedere anche l'invio di SMS o mail pubblicitarie, scaricare applicazioni, iscriversi a servizi terzi … Insomma, di male in peggio!

4.6.3. I più importanti

Sempre per dovere di cronaca, gli autori presentano i più importanti siti web di categoria:

- *CoinBucks (https://coinbucks.io/)* – Altro portale che paga per compiere piccole azioni quali: compilare sondaggi, scaricare applicazioni per

smartphone, partecipare a concorsi, scaricare canzoni, e così via.

- *BitcoinRewards* (*http://www.bitcoinreward.net/*) – Permette di ottenere Bitcoin completando offerte, iscrivendosi a siti, rispondendo a questionari, ed altro. Per incentivare le iscrizioni regala 1'000 Satoshi come bonus.

- *BitcoinSurvey* (*http://bitcoinsurvey.com/index.php*) – Elargisce BTC al completamento di questionari.

4.7. GIOCHI A PREMI IN BTC

Come premesso nel Paragrafo 4.3, si tratta di portali che consentono di guadagnare BTC semplicemente giocando a giochi flash, simili a quelli presenti su Facebook. Più si gioca, più si guadagna.

4.7.1. Come Funziona

Il funzionamento è davvero molto semplice. È sufficiente collegarsi ad uno di questi siti web, come **TremorGames**

(http://www.tremorgames.com) ed effettuare una banale iscrizione. Ad iscrizione avvenuta, collegandosi sulla homepage del portale (Figura 27) e selezionando uno dei tanti giochi disponibili, sarà possibile guadagnare BTC semplicemente giocando.

Figura 27: Home page di TremorGames.

Difatti, più tempo si spenderà

sul portale a giocare maggiore sarà il numero di BTC che si accumuleranno. Dunque, si tratta di un lavoro per nulla noioso anzi divertentissimo.

4.7.2. Pro e Contro

Come il lettore potrà immagine, i guadagni derivanti da categorie di questo tipo sono davvero molto bassi. Nonostante le numerose prove ed i tanti account, cercando di accumulare BTC utilizzando i refer link, gli autori non sono arrivati neppure a 0.001 BTC in una settimana.

Dunque, tra i contro sicuramente

i guadagni, mentre tra i pro si può annoverare il divertimento.

4.7.3. I più importanti

In questo caso, gli autori si sentono in dover di segnalare i portali, non tanto per indicare quali siano i più proficui in termini di bitcoin (consentono infatti di guadagnare tutti lo stesso ammontare di valuta digitale), quanto i più divertenti:

- *FreeBitcoinMiner* (*http://www.freebtcminer.com/*) – Giocare è semplicissimo, basta

muovere l’omino con i tasti direzionali, scavare e trovare la propria strategia per vincere più premi.

- *Gambit (http://www.gambit.com/)* – Multiplayer basato su Bitcoin. È dotato di molti giochi classici da tavolo a tema bitcoin, si può giocare gratuitamente o con una scommessa in BTC. Sito eccellente se ci si vuole incontrare con un amico, oppure giocare online con la comunità di internet.

4.8. SCOMMETTERE BITCOIN

Come lo stesso nome fa presagire, si tratta di siti web che sfruttano il gioco d'azzardo per consentire l'accumulo di bitcoin. Al primo accesso, viene indicata la possibilità di depositare bitcoin già in proprio possesso, oppure utilizzare la carta di credito per acquistarne all'attuale prezzo di mercato.

Lungi dagli autori spiegare come, cosa e quanto scommettere. Quanto di seguito esposto lo si è fatto per ovvie ragioni di completezza, ma non si può ritenere questa categoria

sicura e remunerativa sul lungo periodo.

4.8.1. Come funziona

Il funzionamento è abbastanza semplice, forse per alcuni lettori non sarà la prima connessione ad un sito di scommesse online (SNAI, Lottomatica, Better, Intralot, e tanti altri). Per l'esempio gli autori hanno utilizzato **Betcoins** (https://www.betcoin.ag/). Come sempre, prima di poter entrare a far parte della comunità, è necessaria una minima registrazione. Al contrario di quanto avvenuto nelle precedenti categorie, questa volta viene chiesto di confermare anche l'età che deve essere

superiore, per ovvie ragioni legali, a quella di anni diciotto (Figura 28).

Figura 28: Home page di Betcoins.

Essendo il pagamento in moneta anonima, non è necessario inserire una copia di un valido documento di riconoscimento, né il codice fiscale. Gli autori hanno deciso di non entrare nello specifico dell'aspetto funzionale perché in alcun modo vogliono far propaganda al gioco d'azzardo.

4.8.2. Pro e Contro

Per quanto riguarda i pro e i contro, è difficile entrare nel mero aspetto tecnico. Per alcuni sicuramente risulterà un'opportunità per accumulare

BTC, perché abili nell'indovinare pronostici soprattutto quelli calcistici; per altri invece potrebbe essere la loro più grande sfortuna. Potrebbero perdere non solo i BTC accumulati gratuitamente, ma anche i propri risparmi.

4.8.3. I più importanti

Si presentano, ora, un elenco dei siti di scommesse che accettano bitcoin come metodo di pagamento. Tra questi si trovano:

- *BitBet (http://bitbet.us)* – Sito di

scommesse completo, permette di scommettere su politica, sports, film, televisione, mercati finanziari, e tante altre categorie.

- *BitcoinVideoCasino (https://https//bitcoinvideocasino.co* – I giochi disponibili sono: video poker, blackjack, roulette, craps, keno o slots.

- *BitcoinCasino (http://bitcoincasino.net)* – Il casinò più conosciuto in rete dedicato interamente ai bitcoin. Ha anche una sezione dedicata al poker che offre dei tornei FREEROLL giornalieri

dalle vincite complessivo di 2.5 BTC.

- *SatoshiBet (https://satoshibet.com)* – In linea con i facenti parte della categoria, consente scommesse, tornei di poker, e così via.

CAPITOLO 5

MOLTIPLICARE I PROPRI BITCOIN

Nel capitolo precedente si è parlato dei metodi più semplici per accumulare bitcoin, ed è stato visto che, sebbene permettano di guadagnare senza troppi sforzi, il vero limite risiede nell'ammontare dei profitti. Quest'ultimi risultano, in ultima analisi, non elevati. Si precisa che in questa sede non vengono considerate variazioni nel tasso di cambio bitcoin-euro, che porterebbero aumentare il valore nel tempo della cifra in BTC accumulata (considerazioni che vengono lasciate ai

lettori, nella gestione dei lori investimenti, con relativo orizzonte temporale).

Questo capitolo si spingerà oltre i metodi tradizionali descritti in precedenza, presentando un sistema matematico che permetta di aumentare i ricavi in bitcoin, riducendo addirittura il tempo necessario speso al computer, che i lettori potranno dedicare maggiormente allo sviluppo del loro business.

5.1. METODO DEL "RADDOPPIO" PER MOLTIPLICARE I NOSTRI BITCOIN

La "*regola del raddoppio*" si basa su un semplice concetto matematico che gli autori hanno associato allo studio della statistica, e verrà spiegato come sfruttarlo in un sistema quale quello di https://freebitco.in/ (trattato nel Capitolo 4). Partendo da un capitale iniziale di bitcoin accumulato attraverso il sito stesso, quindi senza investimenti iniziali, sarà possibile moltiplicare senza sosta il capitale. Alternativamente, il lettore

potrà utilizzare direttamente capitale in BTC già in suo possesso semplicemente trasferendolo nel conto virtuale del portale, senza dover spendere tempo per guadagnarlo tramite FreeBitco.in.

In altre parole, verrà sfruttato (vincendo, sempre!) il sistema di "roulette" integrato in FreeBitco.in, per incrementare costantemente i propri bitcoin (Figura 29).

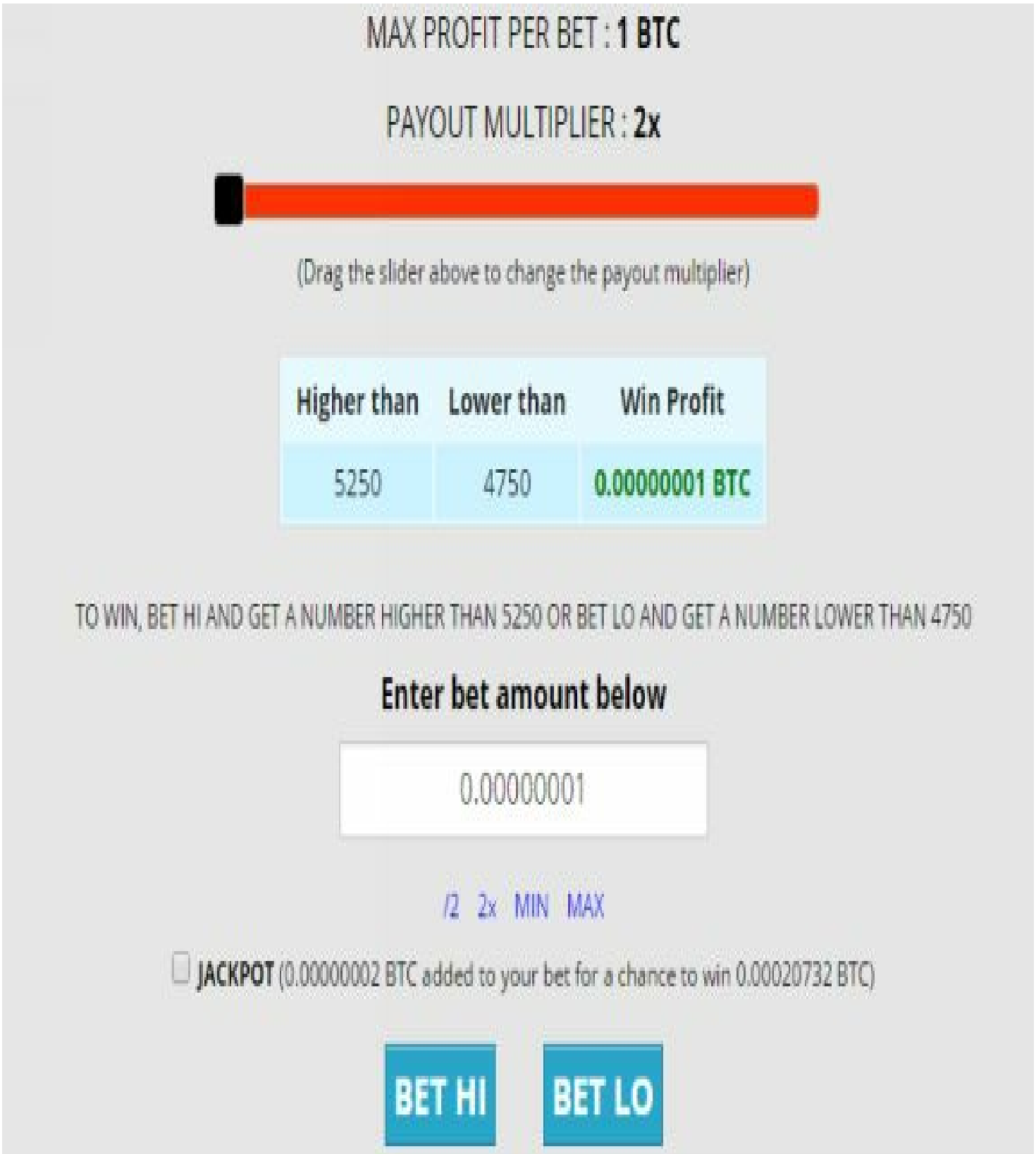


Figura 29: Screenshot della "roulette" di FreeBitco.in.

Dopo questa breve premessa, si può entrare subito nel vivo della spiegazione: il primo passo sarà la dimostrazione matematica del metodo del raddoppio e le implicazioni statistiche – ma non temete, nessuna spiegazione incomprensibile, solo parole semplici ed esempi tangibili. Si procederà quindi, dopo aver compreso le basi statistiche necessarie, ad una dimostrazione pratica del sistema.

Il consiglio è quello di munirvi di una calcolatrice, per seguire agevolmente i calcoli proposti. In ogni caso, non sono necessarie conoscenze matematiche o statistiche pregresse per

poter comprendere il capitolo.

I lettori potranno applicare loro stessi la “regola del raddoppio” immediatamente dopo aver finito di leggere il capitolo. Si tiene a precisare che ogni elaborazione svolta è essenziale per ottenere dei profitti tangibili, ed i lettori sono avvertiti di terminare l’analisi di *tutti* i paragrafi prima di operare con i propri bitcoin.

5.2. REGOLA MATEMATICA DEL RADDOPPIO

Quanto sta per essere enunciato può sembrare incredibile, o contro intuitivo a molti. Viene dimostrato, con opportuni calcoli, che in realtà è nascosto un semplice “trucco” matematico. Saranno invece le interpretazioni statistiche a fare la differenza, ed a permettere al lettore di accumulare bitcoin.

Enunciato:

In un gioco della tipologia

"perdi o raddoppia", indipendentemente dalle probabilità dei due eventi, purché entrambi con probabilità diversa da zero, è possibile, avendo una serie adeguato di tentativi, ***vincere SEMPRE*** *la puntata iniziale.*

Per alcuni lettori questo enunciato potrebbe essere una conoscenza già nota, per altri invece potrebbe sembrare sorprendente (se invece non fosse chiaro, nessuna paura, a breve sarà tutto chiarissimo). In entrambi i casi, conoscere questo semplice gioco matematico **non è sufficiente** perché occorre adeguarlo al

sistema che abbiamo a disposizione.

Si inizi con un esempio pratico per capire immediatamente il funzionamento:

<u>Esempio 1</u>: Immaginare una scommessa con probabilità di vincere (p) del 50% e, specularmente (p-1), 50% di perdere. Indichiamo con X l'ammontare della scommessa, conseguentemente:

	Vincita	Perdita	X= posta iniziale
PREMIO	2X	0	

Tabella 2: Scommessa con 50% di probabilità di vincere (e 50% di perdere)

Si sta parlando di una gioco che, a fronte di una posta X, paga in caso di vincita 2 volte la posta iniziale (X), ed in caso di perdita niente. Paragonabile quindi alla roulette del casinò giocando sul "pari o dispari", sebbene in quest'ultimo caso le probabilità non sono esattamente del 50%, poiché occorre considerare lo zero.

La strategia del "*metodo del raddoppio*" è quella di **raddoppiare ogni qualvolta che si perde la scommessa. Il risultato finale è che, quando la serie negativa (perdita) cesserà, ossia si verificherà una**

vincita, il vostro capitale sarà aumentato esattamente dell'importo corrispondente alla posta iniziale.
Ecco subito un esempio intuitivo (Tabella 3):

		Perdita cumulata	Vincita
Scommessa iniziale	1	1	
	PERDO		
Raddoppio la posta	1x2=2	2+1=3	
	PERDO		
Raddoppio la posta	2x2=4	4+3=7	
	PERDO		
Raddoppio la posta	4x2=8	8+7=15	
	PERDO		
Raddoppio la posta	8x2=16	15+16=31	
	PERDO		
Raddoppio la posta	16x2=32	31+32=63	
	PERDO		
Raddoppio la posta	32x2=64	63+64=127	
	VINCO	64X2=128	128-127=1

Tabella 3

In questo esempio, 6 volte la scommessa viene persa, la probabilità che ciò si verifichi, dato il 50% di probabilità di vincita, è 1/64, ossia 1.56% (molto bassa, a prima vista).

Come appare facilmente comprensibile da questo esempio concreto, detraendo dalla vincita finale (128) tutte le poste "perse" (127), la vincita **netta** finale (128-127=1) è esattamente pari alla scommessa iniziale (i calcoli e l'interpretazione delle probabilità vengono affrontati successivamente, in un paragrafo dedicato).

Il lettore che non fosse convito

può testare autonomamente come questo metodo funzioni sempre (matematicamente parlando), non importa quanto lunga sia la serie di perdite consecutive, a patto che si verifichi, alla fine, una vincita – e sicuramente, prima o poi, una vincita è destinata a verificarsi. Ovviamente il metodo si applica indipendentemente dall'ammontare della scommessa iniziale, che questa sia 10, 100, 10'000, e così via, non ha rilevanza. Raddoppiando la posta ogni qualvolta si perde, si vincerà esattamente la posta iniziale, al netto di tutte le giocate perse. È ora il momento di sviluppare più nel dettaglio il metodo.

ATTENZIONE:

Prima di buttarsi a capofitto nell'utilizzare questo sistema, occorre tenere ben in considerazione come si implementa nel mondo reale. Il lettore più attento avrà già capito come 3 fattori giocano un ruolo fondamentale in questo sistema, e sono:

1. *Le relative probabilità di vincita (p) e perdita (1-p) al gioco.*
   Sebbene sia un dato di fatto che questo metodo funzioni sempre, a patto che la probabilità di vincita sia maggiore di zero (p>0), occorre precisare che in caso di probabilità

di vincita basse la serie di eventi negativi diventa considerevolmente più lunga.

2. *La scommessa iniziale*.
Infatti, raddoppiando sistematicamente, la puntata aumenta velocemente d'importo.
Conseguentemente, è necessario determinare, tramite specifici calcoli, in accordo con le probabilità di vincere (e specularmente, perdere), il capitale minimo in grado di garantire di avere sufficienti fondi per raddoppiare la posta fino alla vittoria finale.

3. *Eventuali limitazioni imposte.*
Sono decretate dal gestore del gioco. Di norma sono una scommessa minima, ed una scommessa massima. Come il lettore avrà già intuito, sono vincoli che possono compromettere la facoltà di raddoppiare fino ad ottenere la vincita certa corrispondente alla posta iniziale. *(Nessuna paura, nel sistema presentato dagli autori non esiste una scommessa minima, come si vedrà a breve).*

Tutti questi limiti vengono analizzati ed elusi, tramite opportuni sistemi matematici che saranno illustrati

ai lettori.

5.3. FREEBITCO.IN E LA STATISTICA – VINCERE O PERDERE

Si analizzino ora le probabilità di vincere, o perdere, tramite il servizio offerto da FreeBitco.in.

È bene precisare che in questa analisi, e quindi nei calcoli seguenti, si parla di **eventi indipendenti.** In altre parole, il fatto che voi abbiate vinto o perso la puntata precedente *non influenza in alcun modo la probabilità della successiva.* Il tipico caso, per comprendere di cosa si parla, è il lancio della moneta. Quest'ultima non ha certo

memoria del fatto che precedentemente sia uscita testa oppure croce.

Si cercherà, in questo paragrafo, di debellare alcune convinzioni ERRATE che i lettori potrebbero avere sul mondo della probabilità, e che porterebbero a interpretare male i risultati e, conseguentemente, fallire nel tentativo di incrementare i bitcoin.

CALCOLO PROBABILITA' EVENTI INDIPENDENTI

Si definiscono gli eventi come *indipendenti* se il verificarsi dell'uno non influisce sulla probabilità del secondo, e nel caso in questione questa premessa è essenziale. Quindi, dati due

eventi indipendenti E1 ed E2, siano la probabilità di E1 p1, e la probabilità di E2 p2. Il calcolo della probabilità che l'evento E1 si verifichi *n* volte è dato da:

$$(p1)^n$$

Cioè la probabilità dell'evento E1 moltiplicata per sé stessa *n* volte. Speculare, ovviamente, il calcolo della probabilità di E2.

La spiegazione statistica di quanto viene enunciato (se il lettore non desidera soffermarsi può procedere direttamente all'Esempio 2) è da

ricercarsi nel **Teorema di Bayes**, riassunto dalla seguente equazione:

$$\mathbf{P(A|B) = \{P(B|A) / P(B)\} * P(A)}$$

L'espressione P (A|B) significa "*probabilità dell'evento A sapendo che si è verificato l'evento B*". Ma essendo gli eventi indipendenti P (B|A) = P(B), cioè è irrilevante il fatto che si sia verificato A nel calcolo della probabilità di B. Cercare la probabilità che un evento si ripeta *n* volte, significa trovare ogni volta l'intersezione P (A ∩B) = P (A) * P (B|A). Quindi, se A e B sono indipendenti, risulta P (B|A) = P (B), per cui P (A ∩B) = P (A) * P (B).

Se il lettore è nuovo a questo

teorema sulla probabilità, non si demoralizzi! Ai fini del raggiungimento del risultato, e dei profitti, non è necessario conoscere approfonditamente alcuna formula. È possibile procedere con la lettura senza soffermarsi ulteriormente.

<u>Esempio 2</u>: una moneta regolare ha il 50% di probabilità che esca testa, ed il 50% di probabilità che esca croce. La probabilità che escano consecutivamente 4 volte testa è data da:

$0.5 * 0.5 * 0.5 * 0.5 = 0.0625$ *ossia il* 6.25%

Ai fini di questa trattazione, gli unici calcoli rilevanti sono quelli degli eventi indipendenti. La "roulette" di FreeBitco.in infatti, non ha memoria delle giocate precedenti.

<u>Domanda:</u> perché se gli eventi non hanno memoria, la probabilità di giocare <u>n volte</u> varia il calcolo delle probabilità?

Per il semplice fatto che la scommessa non è più sul singolo evento E1, la cui probabilità indubbiamente

rimane immutata. Al contrario, scommettendo sul verificarsi di *n volte* consecutive un evento E1 con probabilità p1, occorre considerarlo come un insieme più grande (quello in cui non solo si verifica E1, ma si verifica in successione n volte!), e non come le probabilità del singolo evento! È una differenza sostanziale. Con le dovute semplificazioni, è come dire che si scommette sul verificarsi di un evento non una sola volta, ma *n* volte (è evidente che le probabilità possano cambiare).

In questo caso, l'evento che si vuole stimare è la probabilità di perdere, per *n volte* consecutive.

Partendo da questa informazione si potrà stimare una puntata iniziale ragionevole, che sarà la vincita effettiva per ogni serie. Quindi, si effettueranno giocate per un numero elevatissimo di volte (100'000 giocate ed oltre) per aumentare senza sosta i profitti. Grazie a script automatici, sarà il sistema a fare tutto per i lettori, ed il tempo risparmiato potrà essere dedicato a qualsiasi altra attività.

La prima cosa da fare è calcolare le probabilità relative alla vincita (E1) e relative alla perdita (E2) rispetto alla “roulette” offerta da FreebBitco.in.

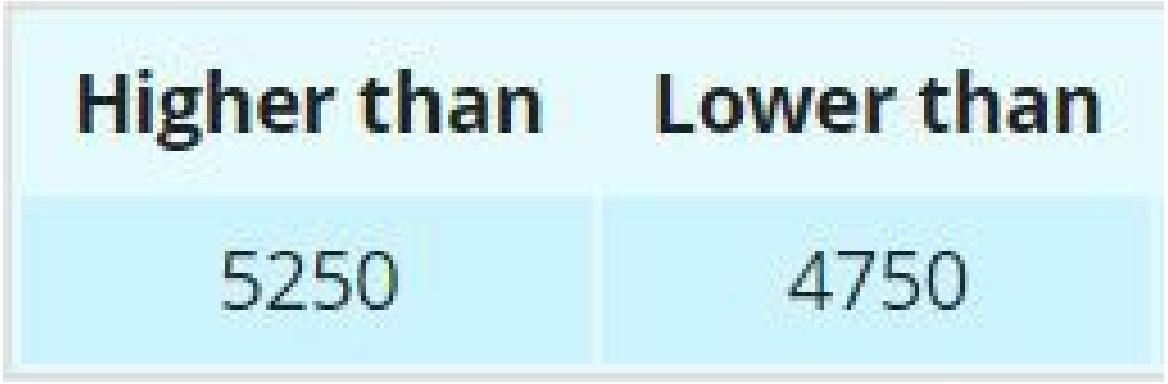


Figura 30: Immagine tratta dalla "roulette" di FreeBitco.in.

La "roulette" di FreeBitco.in funziona in questo modo (Figura 30): estrae un numero *casuale* compreso tra 1 e 1'000. È possibile scommettere che questo sia minore di 4'750 o maggiore di 5'250. **Attenzione**: sebbene il sito offra anche altre possibilità di scommettere, gli autori sconsigliano vivamente di perdere tempo e denaro a sfidare la fortuna. In questo capitolo, nonostante si parli di una "roulette", non centra nulla

il gioco d'azzardo. Al contrario, il sistema sviluppato lascia ben poco al caso e alla fortuna. Non solo tutto deve essere previsto *ex ante*, ma è anche possibile stimare *esattamente* l'ammontare della vincita per ogni serie giocata.

Indipendentemente dal fatto che puntiamo su "maggiore di 5'250", oppure "minore di 4'750", le probabilità di vincere sono esattamente del 47.5%. Questo perché il sistema, furbescamente, detiene un margine per fare in modo che, giocando normalmente, il banco riesca sempre a risultare vincente. Ma non sarà un nostro problema, e si vedrà perché.

Come anticipato

precedentemente, si è interessati alla percentuale di perdita, che a prescindere dal fatto di puntare su maggiore o minore, è rappresentata dal 52.5%. Il lettore più attento avrà senz'altro già capito che più la percentuale di perdere la scommessa è elevata, più la serie negativa che ci costringerà a raddoppiare sarà lunga, statisticamente parlando.

Riassumendo, si elencano i passi per incrementare, senza sosta, i bitcoin:

1. Stimare l'*importo della puntata iniziale* dopo aver fatto un breve

studio statistico. Questo consentirà di raddoppiare la posta senza il pericolo di arrivare a serie negative così lunghe da consumare completamente il capitale, bloccando l'operazione.

2. Stimare un *capitale minimo di sicurezza*, tramite opportuni calcoli, come conseguenza di quanto appena detto.

3. Eseguire un test per prendere consapevolezza delle fluttuazioni statistiche[6] contro-intuitive sui grandi numeri. Infatti, è importante ricordare che non si sta lavorando su

piccoli numeri, per i quali una percentuale, per esempio dello 0.5%, sarebbe trascurabile. Al contrario, sui grandi numeri, anche percentuali "piccole" assumeranno una importanza notevole.

4. Infine, si stabilisce il *valore atteso* (definito nel paragrafo 5.5) della vincita per ogni serie. In altre parole, il controvalore in bitcoin (e, anche in euro).

Inoltre, grazie ai software che gli autori mettono a disposizione al seguente indirizzo http://www.extremegeneration.it/ebook/

, il lettore potrà svolgere ulteriori test personalmente, variando i parametri secondo la sua strategia.

5.4. ANALIZZIAMO LE PROBABILITA' DELLE GIOCATE

Il primo passo da fare è studiare esattamente le probabilità di perdere consecutivamente *n volte*. Si riporta di seguito una tabella che sintetizza le probabilità relativamente al numero di giocate:

Giocate consecutive	Probabilità di perdere
1	52,50%
2	27,56%
3	14,47%
4	7,597%
5	3,988%
6	2,094%
7	1,099%
8	0,577%
9	0,303%
10	0,159%
11	0,0835%
12	0,0438%
13	0,0230%
14	0,0121%
15	0,00634%
16	0,00333%
17	0,00175%
18	0,000918%
19	0,000482%
20	0,000253%
21	0,000133%
22	0,0000697%
23	0,000037%
24	0,000019%
25	0,000010%

Tabella 4: Le percentuali sono state calcolate come spiegato nel paragrafo 5.2.

Si nota come, a partire dalla 14esima giocata, la probabilità di perdere per *n* volte consecutive si riduca drasticamente, con valori inferiori allo 0.01%.

ATTENZIONE:

L'errore più comune sarebbe interpretare queste probabilità paragonandole agli eventi quotidiani, e quindi ritenere che una percentuale dello 0.01%, o addirittura dello 0.00001%, sia del tutto remota e pressoché

impossibile. Tuttavia, come già anticipato, non si parla di una singola giocata. Infatti, per massimizzare i profitti, verranno lanciate in serie 100'000 giocate o più, ed ecco che probabilità “piccole” diventano improvvisamente rilevanti. A tal fine è stato configurato un software per simulare il sistema, disponibile per i lettori al link già citato http://www.extremegeneration.it/ebook/ .

5.5. IL VALORE ATTESO DELLA VINCITA

Il valore atteso è il valore che, statisticamente, ci si aspetta di ottenere dalla serie di giocate. Questo valore è aleatorio, ossia è un valore stimato dalla statistica e come tale soggetto a fluttuazioni. Tuttavia, si vedrà immediatamente come queste fluttuazioni sono trascurabili operando con una lunga serie di puntate.

Si introducono quindi i software di calcolo configurati *ad hoc* per facilitare la comprensione dei lettori.

Si prenda in considerazione una

serie di 10'000 puntate, ed una scommessa iniziale in bitcoin di 0.000004 (la spiegazione su come determinare una scommessa iniziale adeguata verrà trattata nel prossimo paragrafo, per il momento ci si concentri sul valore atteso).

Numero di scommesse	10000
Ammontare scommessa (in BTC)	0.000004
Guadagno atteso (in BTC)	**0.019**

Tabella 5: Simulazione svolta con il foglio di calcolo di www.ExtremeGeneration.it.

Il valore atteso viene calcolato come segue (10000 * 0.000004 *

0.475). Generalizzando: (numero puntate * scommessa iniziale * percentuale di vincita (p))

Si attende quindi, al termine della serie di 10'000 puntate, un *guadagno di 0.019 bitcoin.* Si simuli quindi un test statistico con gli stessi parametri (Tabella 6).

Risultato del test:

VALORI IN BITCOIN			
BIGGEST BET	0.0008192		
BIGGEST LOSS	-0.0004096		
CAPITALE NEGATIVO MASSIMO		-0.0013612	
GAIN TOTALE	**0.00192840**	*VALORE ATTESO*	0.001900000
		FLUTTUAZIONE STATISTICA	0.000028400
EURO (controvalore)	€ 0.53	*PERCENTUALE*	1.49%

Tabella 6: Simulazione svolta con il foglio di calcolo di www.ExtremeGeneration.it.

Il valore evidenziato (*gain totale=0.00192840 BTC*) è l'effettivo guadagno in bitcoin, che corrisponde proprio a quanto inizialmente stimato grazie al metodo del valore atteso (con una minima fluttuazione statistica, quantificabile, dell'1.49%).

Si può ripetere questo test un numero elevatissimo di volte, e ottenere sempre i medesimi risultati, con fluttuazioni statistiche massime di pochi punti percentuali (questo perché si sta lavorando su serie elevate di numeri).

Gli altri valori presenti in questo box verranno approfonditi nei prossimi paragrafi, e rappresentano i *fattori di rischio* da valutare attentamente per stabilire la scommessa iniziale. Infatti, la scommessa massima (*Biggest bet*) non può essere più elevata del capitale a disposizione, e dell'importo massimo della puntata imposto dal sistema.

5.6. STIMARE LA SCOMMESSA INIZIALE

Si parla ora dell'elemento più critico e centrale di tutto il processo. Stimare la scommessa iniziale non è affatto un'operazione da prendere sottogamba, *sbagliare questa stima può portare velocemente a perdere tutti i bitcoin*.

Si immagini di aver scelto una scommessa iniziale *troppo* elevata in relazione al capitale in bitcoin disponibile. È molto probabile che una serie "sfortunata" (termine non rigoroso ma che è usato in questa sede per rendere l'idea) sia lunga a tal punto da

non avere più capitale necessario per raddoppiare la scommessa. Ecco un esempio:

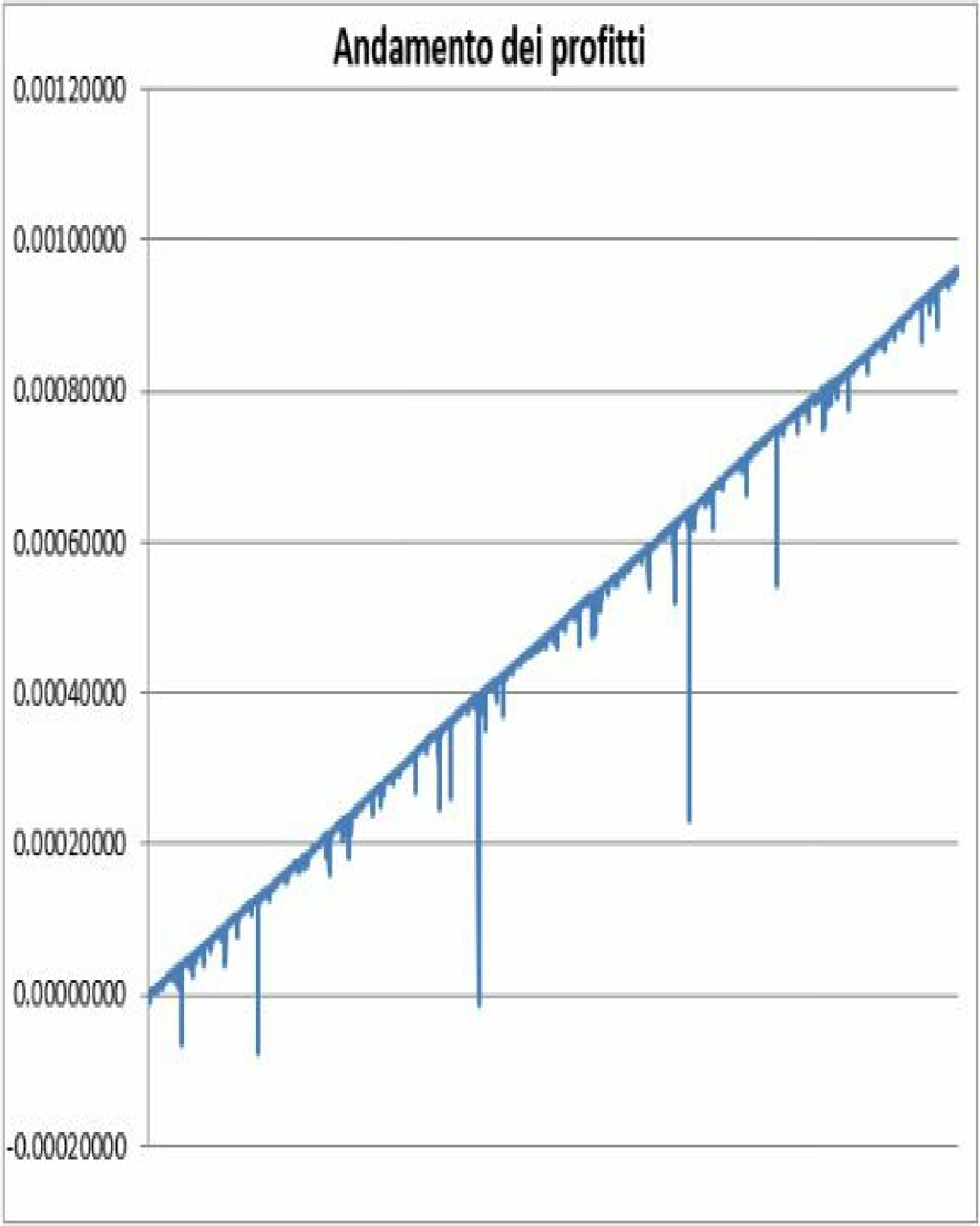


Figura 31: Simulazione svolta con il foglio di

calcolo di www.ExtremeGeneration.it.
Sull'asse verticale è rappresentato il profitto in funzione del numero di puntate.

In questo test sono state giocate 10'000 puntate, con una scommessa iniziale di 0.000002 bitcoin. È evidente come la funzione dei profitti cresca in maniera lineare affine (ricordando una retta). Tuttavia, sono quelle "candele" verso il basso a richiamare l'attenzione: esse rappresentano serie "sfortunate" relativamente lunghe, per le quali occorre avere un capitale sufficiente da garantire il raddoppio.

Sono riepilogati i risultati del test nella seguente tabella, che offre tutte

le informazioni utili per comprendere i dati chiavi dell'intera procedura. Inoltre, per chiarezza, è riportato sempre il controvalore del guadagno al tasso corrente di cambio BTC/EURO.

VALORI IN BITCOIN			
BIGGEST BET	0.0008192		
BIGGEST LOSS	-0.0004096		
CAPITALE NEGATIVO MASSIMO		**-0.001213**	
GAIN TOTALE	**0.00094180**	*VALORE ATTESO*	0.000950000
		FLUTTUAZIONE STATISTICA	-0.00000820
EURO	€ 0.26	*PERCENTUALE*	-0.86%

Tabella 7: Simulazione svolta con il foglio di calcolo di www.ExtremeGeneration.it.

Si ponga ora l'attenzione sul punto centrale di questo metodo: una volta settati tutti i parametri, basterà 1 "click" del mouse su FreeBitco.in per guadagnare bitcoin! Occorrerà certamente non essere precipitosi nel voler ottenere per ogni singola operazione guadagni troppo elevati, ma con gli strumenti forniti da questo capitolo, accumulare capitale sarà relativamente semplice e sicuro.

E' importante ribadire che i profitti sono SEMPRE crescenti, raggiungendo al termine della serie il valore atteso calcolato (al netto di minime fluttuazioni).

Si valuti l'importanza dell'ammontare della scommessa iniziale con quest'altro esempio.

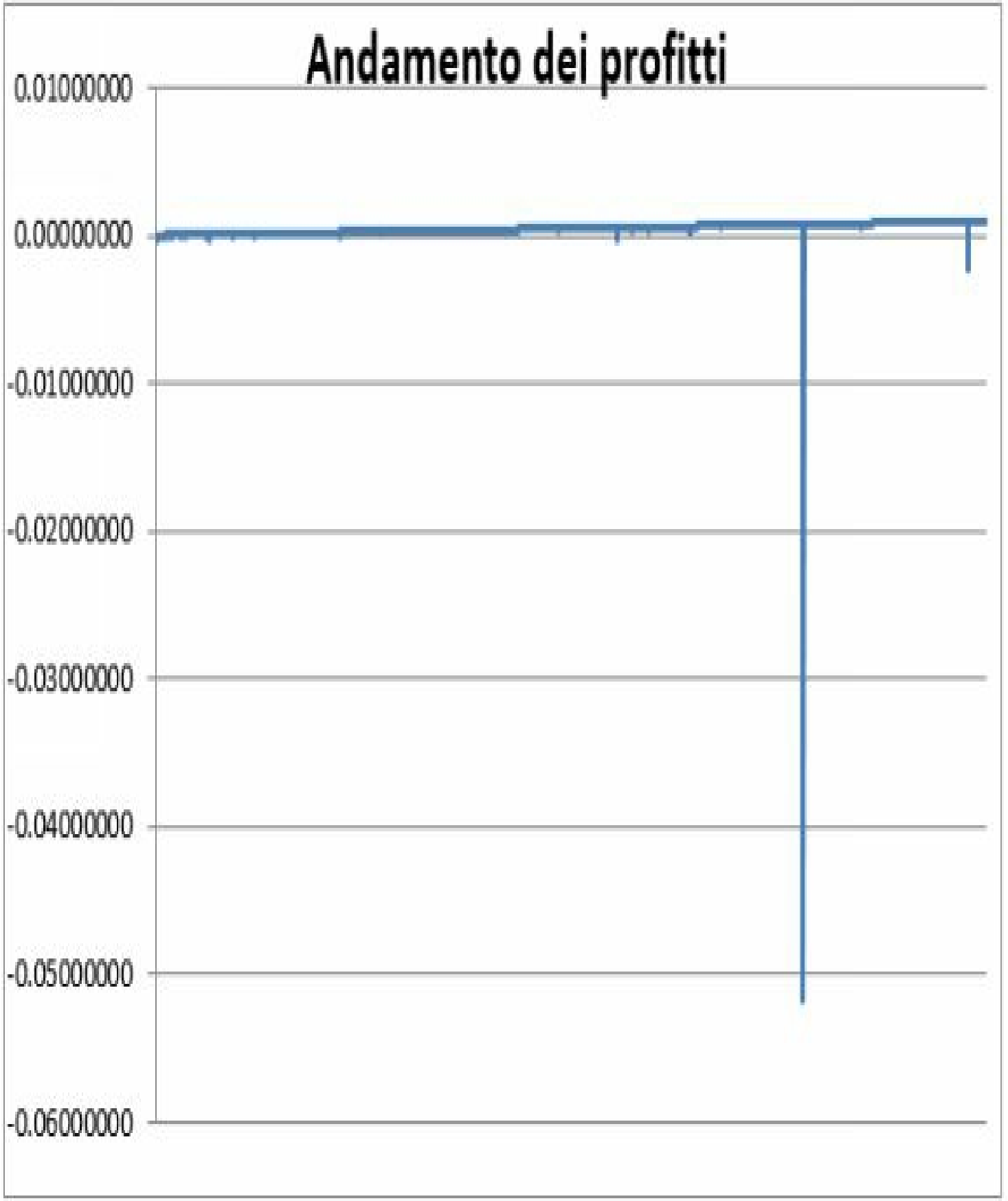


Figura 32: Simulazione svolta con il foglio di calcolo di www.ExtremeGeneration.it.

Sull'asse verticale è rappresentato il profitto in funzione del numero di puntate.

È stata usata, questa volta, una scommessa iniziale di 0.000032 BTC. Si noti la presenza di una serie "sfortunata" tale che il grafico non mette più in risalto i profitti (la linea sembra piatta), sebbene i guadagni siano **MOLTO** più elevati che nell'esempio precedente (4.18€ contro 0.26€).

Anche in questo caso, il profitto finale era previsto. La differenza, però, risiede in un importo della scommessa iniziale troppo elevato, tale da rendere impossibile il raddoppio della puntata in serie negative relativamente lunghe,

perché il sistema non permetterebbe puntate di importo così elevato. Notare che, sebbene il grafico sembri presentare valori anomali, la fluttuazione statistica è davvero minima (meno dell'1%), ovvero l'andamento dei profitti ha raggiunto proprio il valore atteso (Tabella 8).

BIGGEST BET	1.6777216		
BIGGEST LOSS	-0.8388608		
CAPITALE NEGATIVO MASSIMO		**-3.3526784**	
GAIN TOTALE	0.01510400	*VALORE ATTESO*	0.015200000
		FLUTTUAZIONE STATISTICA	-0.000096000
EURO	€4.18	*PERCENTUALE*	-0.63%

Tabella 8: Simulazione svolta con il foglio di calcolo di www.ExtremeGeneration.it.

Quel valore estremo evidente nel grafico corrisponde ad essere momentaneamente in negativo per 3.35 bitcoin! Ed è un importo troppo elevato, come il lettore intuitivamente avrà già capito, e che si approfondirà nel prossimo paragrafo. ***Bisogna tenere conto che il capitale negativo massimo è dato dalla sommatoria di tutte le perdite, fino al momento in cui si verifica la vincita. Appare evidente come sia fondamentale mantenere e calcolare un margine di capitale minimo adeguato***.

5.7. STIMIAMO L'ESATTO IMPORTO DELLA SCOMMESSA INIZIALE

È stato accennato precedentemente che la "roulette" di FreeBitco.in non impone limitazioni per la scommesso minima, al contrario è l'importo massimo della vincita ad essere regolamentato, come riportato di seguito:

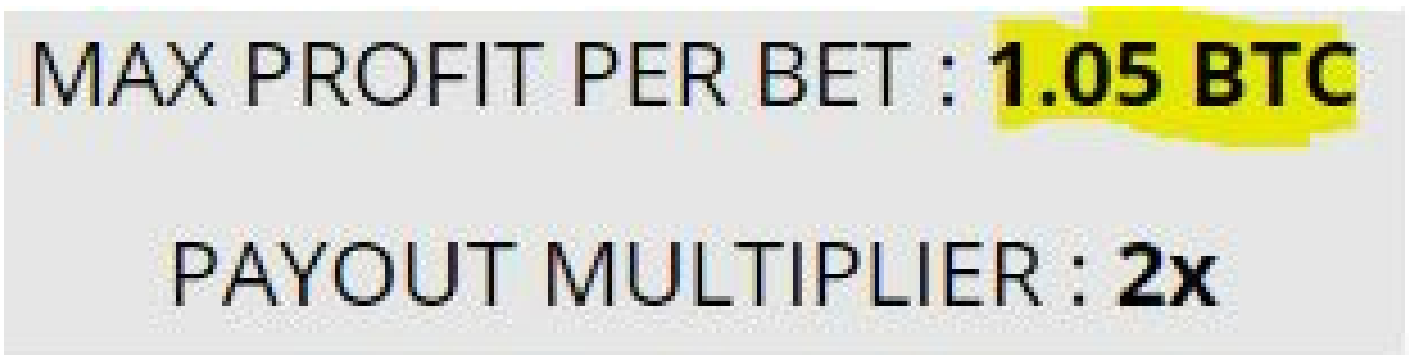


Figura 33: Screenshot delle condizioni di FreeBitco.in, aggiornato al 08/5/2015

Questo importo cambia leggermente ogni giorno, per il semplice fatto che FreeBitco.in mantiene un rapporto costante sui jackpot in base al tasso di cambio bitcoin/dollaro, ma tali variazioni ovviamente non incidono minimamente sul metodo presentato. In relazione al profitto massimo riportato (1.05 BTC), il lettore potrà periodicamente verificare eventuali variazioni significative sul sito di FreeBitco.in.

In questo caso, significa che è possibile, **al massimo**, puntare

1.05BTC. Se fosse necessario dover raddoppiare ulteriormente, NON SAREBBE POSSIBILE in alcun caso, pur avendo disponibile il capitale in bitcoin per farlo.

Conseguentemente, occorre *calcolare a priori la scommessa iniziale*, in modo da scongiurare la possibilità di finire il capitale a disposizione durante il raddoppio, o peggio ancora, raggiungere la scommessa massima consentita.

Per questo calcolo, occorre basarci nuovamente sulle probabilità (Tabella 4), confidando in serie di raddoppio da 22 volte, che si ricorda equivalere ad una probabilità dello

0.000069%, come dimostrato nel paragrafo 5.4. Inoltre, i lettori possono utilizzare i software messi a disposizione per testare autonomamente, con infiniti tentativi, l'efficacia di questi calcoli.

Di seguito viene definito il capitale iniziale, necessario per garantire una serie negativa di almeno 22 perdite. Si ricorda che il calcolo del ***capitale di sicurezza*** è così composto

$$Ultimo\ raddoppio + \sum scommesse\ perse\ precedentemente$$

Detto in parole: tutte le puntate

perse fino al verificarsi della vincita.

AMMONTARE SCOMMESSA INIZIALE (in BTC)	CAPITALE DI SICUREZZA PER SERIE DI 22 PERDITE CONSECUTIVE (in BTC)	Guadagno atteso per ogni serie da 10000 puntate (in BTC)	Controvalore in Euro (al tasso di cambio 1BTC=224€)
0.0000001	0.4194303	0.000475	€ 0.11
0.0000002	**0.8388606**	0.000950	€ 0.21
0.0000003	**1.2582909**	0.001425	€ 0.32
0.0000004	1.6777212	0.001900	€ 0.43
...	...	...	
0.0000032	13.4217696	0.015200	€ 3.40

Tabella 9: Simulazione svolta con il foglio di calcolo di www.ExtremeGeneration.it.

Grazie a questa Tabella 9 riepilogativa, appare evidente come, volendo mantenere un margine di sicurezza elevato, è necessario non farsi prendere dalla frenesia del "tutto e

subito". Infatti, la scommessa iniziale, che meglio soddisfa i requisiti affrontati, è di 0.0000002 BTC, con un guadagno atteso di 0.000950BTC. Si ricorda ai lettori di partire dal presupposto che la tabella considera una sola serie di 10'000 puntate (nel prossimo paragrafo si vedrà come settare lo script automatico). Con un solo "click" è possibile lanciare altre serie, e ancora, e ancora, e ancora… Ed il guadagno aumenta conseguentemente, sommando i profitti di ogni serie.

Il fattore critico in questo caso è la limitazione della scommessa massima imposta del sistema, che si ricorda essere di 1.05 BTC.

Sempre in riferimento alla Tabella 9, si noti come già da una scommessa iniziale di 0.00000032 BTC una serie di 23 perdite consecutive richiederebbe una scommessa che non soddisfa tale requisito, conseguentemente non sarebbe possibile raddoppiare ed incassare la vittoria.

Ancora una volta gli autori ribadiscono che, in ultima analisi, è il lettore a dover gestire un proprio profilo di rischio. In questa sede viene suggerita una scommessa iniziale ragionevolmente sicura (0.0000002 BTC), ma il lettore potrebbe preferire profili a rischio maggiore, o minore. Si consiglia comunque di utilizzare i software di

simulazione messi a disposizione su http://www.extremegeneration.it/ebook prima di intraprendere decisioni affrettate.

5.8. IMPOSTARE SERIE DI SCOMMESSE AUTOMATICAMENTE

Grazie a questo capitolo sono state ottenute le informazioni necessarie per comprendere il metodo del raddoppio, e soprattutto per evitare di incappare in clamorosi errori di valutazione, sottostimando il rischio e le implicazioni contro-intuitive del mondo della probabilità.

Verrà mostrato ora come implementare una serie automatica di puntate attraverso il sito FreeBitco.in.

Per prima cosa, nella home page

del sito, selezionare “MULTIPLY BITCOIN” (Figura 34)

Figura 34: Sezione MULTIPLY BTC di

A questo punto, cliccare su “AUTO BETTING”, che darà la possibilità di impostare i parametri (Figura 35).

Figura 35: Impostazione parametri "AUTO BETTING"

Si impostino i parametri come segue (Figura 36):

BASE BET	BET ODDS
0.00000002	2

MAX BET/WIN	NUMBER OF ROLLS
1.02	10000

ON WIN	ON LOSE
☑ Return to base bet	☐ Return to base bet
☐ Increase bet by 0.00 %	☑ Increase bet by 100.00 %
☐ Change odds to 2	☐ Change odds to 2

BET ON	ON HITTING MAX BET/WIN
☐ HI ☐ LO ☑ ALTERNATE	☑ Return to base bet ☐ Stop betting

STOP BETTING AFTER

☐ Profit reaches or exceeds 0.00000001

☐ Loss reaches or exceeds 0.00000001

☐ PLAY FOR THE JACKPOT

☐ CHANGE CLIENT SEED BEFORE EACH ROLL

☑ DO NOT REFRESH WHEN FREE BTC TIMER RUNS OUT IF AUTO BET IS RUNNING

☐ SHOW DETAILS OF EVERY BET (MIGHT SLOW BETTING SPEED)

START AUTO-BET

Figura 36: Impostazione parametri "AUTO BETTING".

I campi da modificare sono:

- *NUMBERS OF ROLLS*: è il numero delle scommesse che si vuole giocare in sequenza. Nei test presentati nel capito, sono state utilizzate serie da 10'000 giocate, ma nulla vieta di inserire valori anche molto più grandi. Si consiglia, almeno all'inizio, di prendere familiarità con serie da 10'000.

- *BASE BET:* inserire la scommessa iniziale, stabilita in base ai metodi

presentati in questo capitolo.

- *ON LOSE*: inserire la spunta su *"Increase bet by 100%"*, modificando il valore numerico. Questo comando specifica al sistema di raddoppiare la scommessa ogni qualvolta avviene una perdita.

- *INSERIRE LA SPUNTA SU "Do not refresh when free btc timer runs out if auto bet is running*": impedisce alla pagina di aggiornarsi quando è in corso una puntata automatica.

Si ricorda di disattivare la modalità spegnimento automatico del

proprio Computer, per evitare di interrompere la serie di scommesse.

Tutti i software per:

1. Simulazioni
2. Calcolo delle probabilità
3. Calcolo del capitale minimo di sicurezza data una scommessa iniziale
4. Stimatore dei profitti, fluttuazioni statistiche, grafico guadagni per simulazioni

Sono presenti su http://www.extremegeneration.it/ebook

Si invita il lettore a prenderne visione per ottimizzare al meglio la

propria operatività.

CAPITOLO 6

DA BITCOIN A EURO E VICEVERSA

Nel corso di quest'opera è stato analizzato il mondo dei bitcoin nel suo complesso, partendo dal funzionamento del protocollo Bitcoin ed un inquadrandolo nel contesto economico attuale, fino ad arrivare a metodologie per guadagnare ed amministrare la criptovaluta, garantendone tra l'altro la sicurezza.

Tuttavia, l'opera non sarebbe completa senza una breve introduzione alla possibilità di convertire agevolmente i bitcoin in Euro (o

parallelamente in Dollari, e in tutte le altre maggiori valute internazionali), ed il viceversa.

6.1. CONVERTIRE BITCOIN IN EURO – DOLLARI

I motivi per cui i lettori si potrebbero trovare a convertire euro in bitcoin sono innumerevoli, per esempio la necessità di investire nella criptovaluta e quindi accumulare del capitale in bitcoin, se le aspettative sul tasso di cambio EUR/BTC sono favorevoli, proprio come hanno fatto gli "earlier adopter" (letteralmente "utenti precoci") di cui si è parlato nel capitolo iniziale.

Viceversa, il lettore potrebbe

aver la necessità di convertire in euro o dollari i bitcoin guadagnati attraverso i metodi descritti in questo manuale, o attraverso il suo business. In ultimo, potrebbe verificarsi la necessità operativa di effettuare un pagamento in bitcoin pur non disponendo dell'importo nella criptovaluta. A questo scopo verrà fornito un metodo veloce per evitare una doppia transazione, ed elargire tranquillamente pagamenti in bitcoin partendo dagli euro, senza preoccuparsi degli steps intermedi.

Non ci si soffermerà troppo in questo capitolo sulle implicazioni del tasso di cambio.

6.2. CONVERTIRE BTC/EUR E EUR/BTC

Tanti sono i siti web sparsi per la rete che accettano di ricevere BTC scambiandoli con EUR, ed il viceversa. Tra questi si possono annoverare **Kraken**, **24Change**, **Exmo**, che scambiano BTC per EUR ed altre valute. I lettori capiranno che l'elenco potrebbe continuare per pagine e pagine, ma che volutamente viene terminato ritenendo che queste società siano le principali e più complete in termini di servizi offerti.

Rimanendo in linea con gli obiettivi proposti dall'e-book, verrà

analizzato nel dettaglio solo uno di questi siti web, toccando con mano la possibilità di scambiare i BTC in EUR, ed il viceversa.

6.2.1. Come avviene la conversione

Il primo passo è quello di collegarsi ad uno dei tanti siti web che accettano BTC e li scambiano in EUR, è stato scelto **Exmo** (https://exmo.com).

L'interfaccia utente di **Exmo** è semplice e intuitiva, è sufficiente indicare l'ammontare di BTC che si vuole scambiare in EUR per conoscere

l’effettivo tasso di cambio posto in essere, e le commissioni trattenute dal sito web (Figura 37).

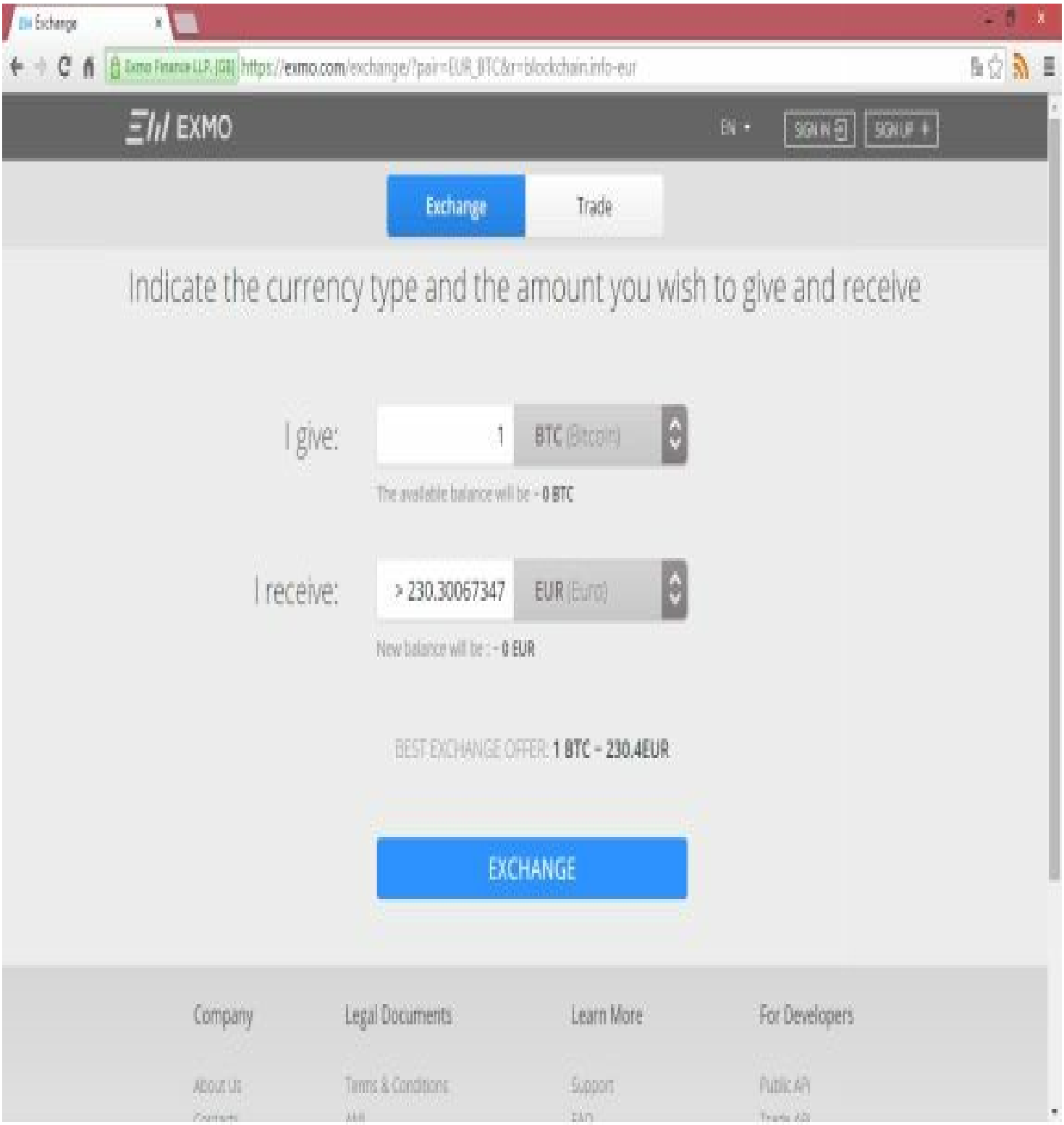


Figura 37: Interfaccia utente di Exmo.

Il portale svolge la duplice di

funzione di accettare BTC per scambiarli in EUR, ed il viceversa. Inoltre, lavora con altre importanti valute internazionali come **USD** (Dollari Americani), **RUB** (Rublo, moneta Russa) ed altre monete matematiche poche note come i **Dogecoin** ed i **Litecoin** (vedi Capitolo 7).

Il primo passo è quello di registrarsi al portale. Il servizio mantiene la filosofia dell'anonimato che contraddistingue la criptovaluta. Infatti, viene richiesto di fornire un semplice username e una password, associando l'account ad un indirizzo e-mail. L'indirizzo e-mail è fondamentale, non solo per la ricezione di newsletter di

carattere tecnico-commerciale, ma anche perché aiuterà a tenere traccia della transazione, notificando in tempo reale le diverse fasi. Terminata la registrazione, previa conferma dell'indirizzo e-mail, cliccare su "**Exchange**" per avviare le trattive di scambio.

Il portale, per ovvi motivi, implementa dei propri standard di sicurezza e vuole essere certo dell'esistenza dei fondi che si intende convertire. Chiede, dunque, di trasferire l'ammontare di BTC sul Wallet gestito da **Exmo**, creato all'atto della registrazione sul portale. Il processo di trasferimento è davvero molto semplice,

viene infatti fornito il QR CODE e l'indirizzo alfanumerico del conto, ed è possibile trasferire i bitcoin sul Wallet come spiegato nel Capitolo 3.

Avvenuto il trasferimento si può convertire i BTC in EUR e, in maniera del tutto equivalente, con una qualunque altra moneta tra quelle proposte dallo stesso Exmo. Il processo è molto semplice, basta indicare nella casella di testo l'ammontare di BTC da convertire, e la valuta che si desidera ottenere dalla conversione. Per terminare il processo basta cliccare su "Exchange" (Figura 38).

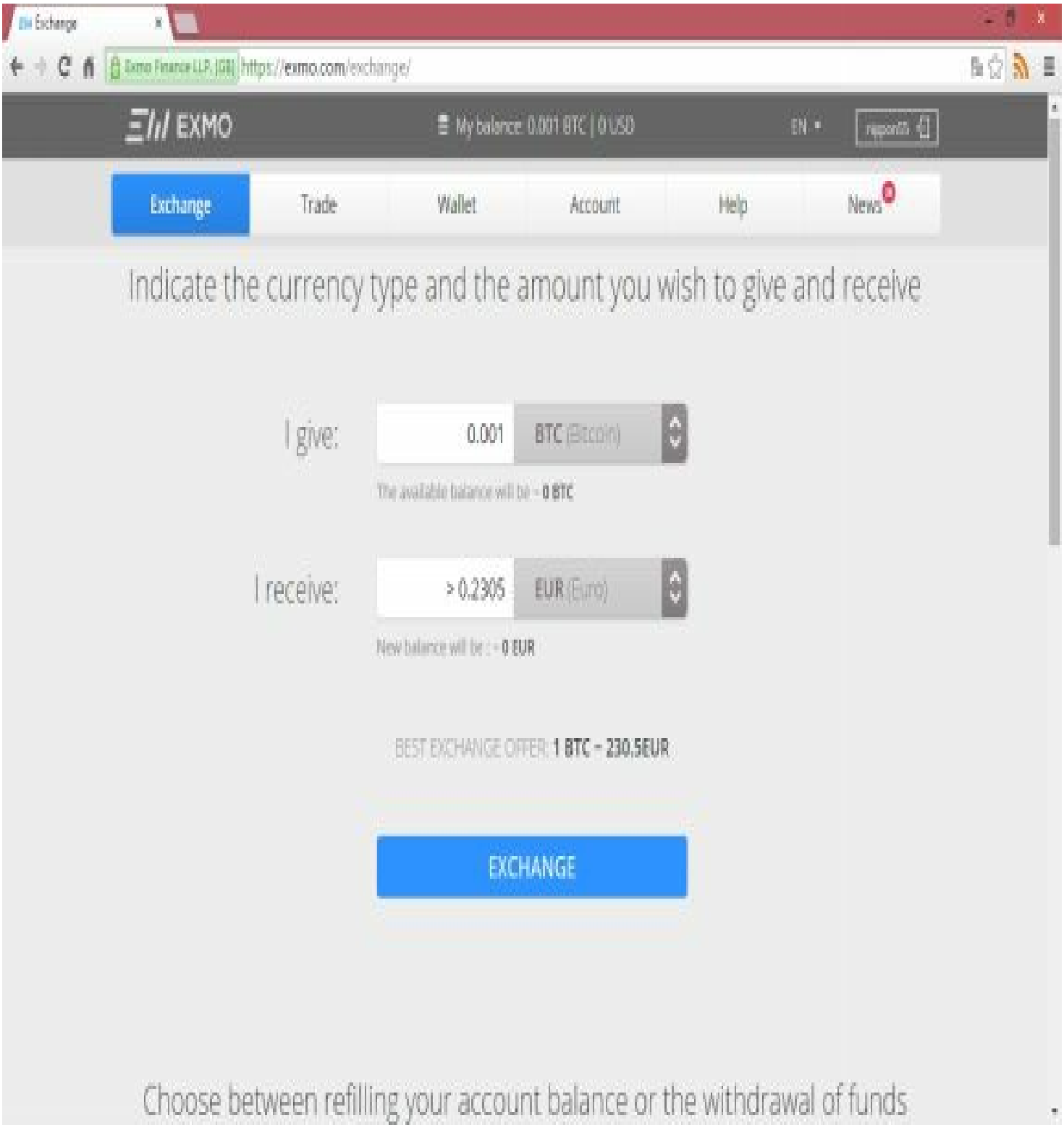


Figura 38: Convertire BTC in EUR con Exmo.

Al termine della procedura,

l’ammontare di euro ottenuti verrà trasferito all’interno del portafoglio dell’utente. È ora possibile trasferirlo ad un proprio conto seguendo una delle modalità rese disponibili dal portale:

- *Bonifico SEPA*: indicando i propri estremi bancari, è possibile ricevere richiedere un bonifico dell’intero o parte del saldo presente sul “portafoglio virtuale”. La somma che trasferibile varia da un minimo di 10 EUR ad un massimo di 10'000 EUR. La commissione da pagare per il trasferimento di denaro è pari ad 1 EUR, qualunque sia il saldo trasferito. I tempi per il trasferimento

sono quelli di un normale bonifico 2/3 giorni lavorativi.

- *Carta di Debito/Credito*: il saldo viene accreditato sulla propria carta di credito/debito. Il minimo saldo richiesto per poter procedere con l'operazione è di 250 EUR mentre il massimo è pari a 2'500 EUR. La commissione da pagare è pari a 7 EUR + il 2% del trasferito. Le informazioni richieste sono: numero di carta, mese ed anno di scadenza. I tempi richiesti sono pari a 1/2 giorni lavorativi.

- *OK Pay*: si tratta di un servizio

equivalente a PayPal. I tempi richiesti per il trasferimento non superano le 24 ore. Il minimo saldo che è possibile trasferire è di 10 EUR mentre il massimo è di 1'000 EUR. La commissione da pagare è pari al 7% di quanto trasferito.

In tutti e tre i casi le commissioni vengono decurtate dall'importo trasferito.

Il servizio offre la possibilità di effettuare l'esatto opposto: convertire EUR, o altre monete aventi corso legale accettate, in BTC. Anche in questo caso è necessario trasferire prima EUR sul wallet di Exmo, per poi procedere alla

conversione ripercorrendo quanto già illustrato. Per poter effettuare il deposito è sufficiente cliccare su “Deposit” (posto di fianco alla moneta che intendiamo depositare), scegliendo tra le due modalità messe a disposizione:

- *Bonifico SEPA*: vengono indicate le coordinate bancarie del conto a cui fare l’accredito, indicando una specifica causale identificativa dell’account Exmo. Il minimo da trasferire è 10 EUR mentre il massimo è pari a 10'000 EUR. La commissione è pari ad 1 EUR qualunque sia la somma trasferita. Valgono le tempistiche prima citate.

- *Ok Pay*: consente il trasferimento di una somma compresa tra 1 e 1'000 EUR. La commissione è pari al 5% del trasferito. La transazione è istantanea, è possibile da subito utilizzare il capitale trasferito.

Il lettore capirà che non vi è bisogno di aggiungere null'altro perché il processo ripercorre quanto già espresso in precedenza. Una volta ottenuti BTC è possibile trasferire il saldo, pagando una piccola commissione, sul proprio conto oppure quello di terzi.

Da tenere a mente che non è

possibile convertire in BTC una somma inferiore ad 1 EUR, e che le commissioni sono sempre pari a 0.0001 BTC, qualunque sia l'importo trasferito.

6.3. PAGARE IN BTC TRAMITE EUR

Sulla rete esistono svariati portali che permettono di velocizzare ulteriormente i tempi per convertire euro in bitcoin, eliminando il doppio trasferimento dall'utente al portafoglio del portale, e da questo nuovamente all'utente. Il sistema che verrà analizzato permette di scambiare in tempo quasi reale (60 minuti al massimo) euro in bitcoin, senza passaggi intermedi ed in completo anonimato, che nel metodo precedente non poteva essere garantito causa utilizzo di circuiti bancari (bonifico, carta di credito, e così via).

Questa procedura consente, inoltre, di risparmiare un po' sui tassi di cambio e sulle commissione, soprattutto per piccole somme.

Si passi dunque ad un esempio pratico, analizzando il funzionamento del noto portale **PosteBit** (http://www.postebit.it/).
Caratteristiche di questo portale sono la facilità con cui è possibile scambiare EUR per BTC ed il completo anonimato. In aggiunta, un incentivo potrebbe essere la familiarità del lettore con carte di debito come PostePay, e similari. Infatti, il servizio permette di effettuare una normalissima ricarica PostePay del controvalore stabilito in bitcoin, ed a

tutto il resto penserà il sito web.

Si immagini, ad esempio, di voler concludere un acquisto in BTC e di non aver abbastanza criptomoneta sul proprio conto. Per eliminare i passaggi intermedi entra in gioco **PosteBit,** che finalizza l'acquisto direttamente, è sufficiente l'indirizzo bitcoin. La prima cosa da fare è collegarsi al portale e compilare il form per l'acquisto di BTC. I campi richiesti, per concludere l'operazione, sono (Figura 39):

- Ammontare di BTC da acquistare attraverso il portale;

- Indirizzo e-mail sul quale verranno

inviate comunicazioni sullo stato della transazione (ricezione dell'ordine, accredito della somma, invio dei BTC);

- Indirizzo BTC sul quale verranno trasferire i BTC appena acquistati.

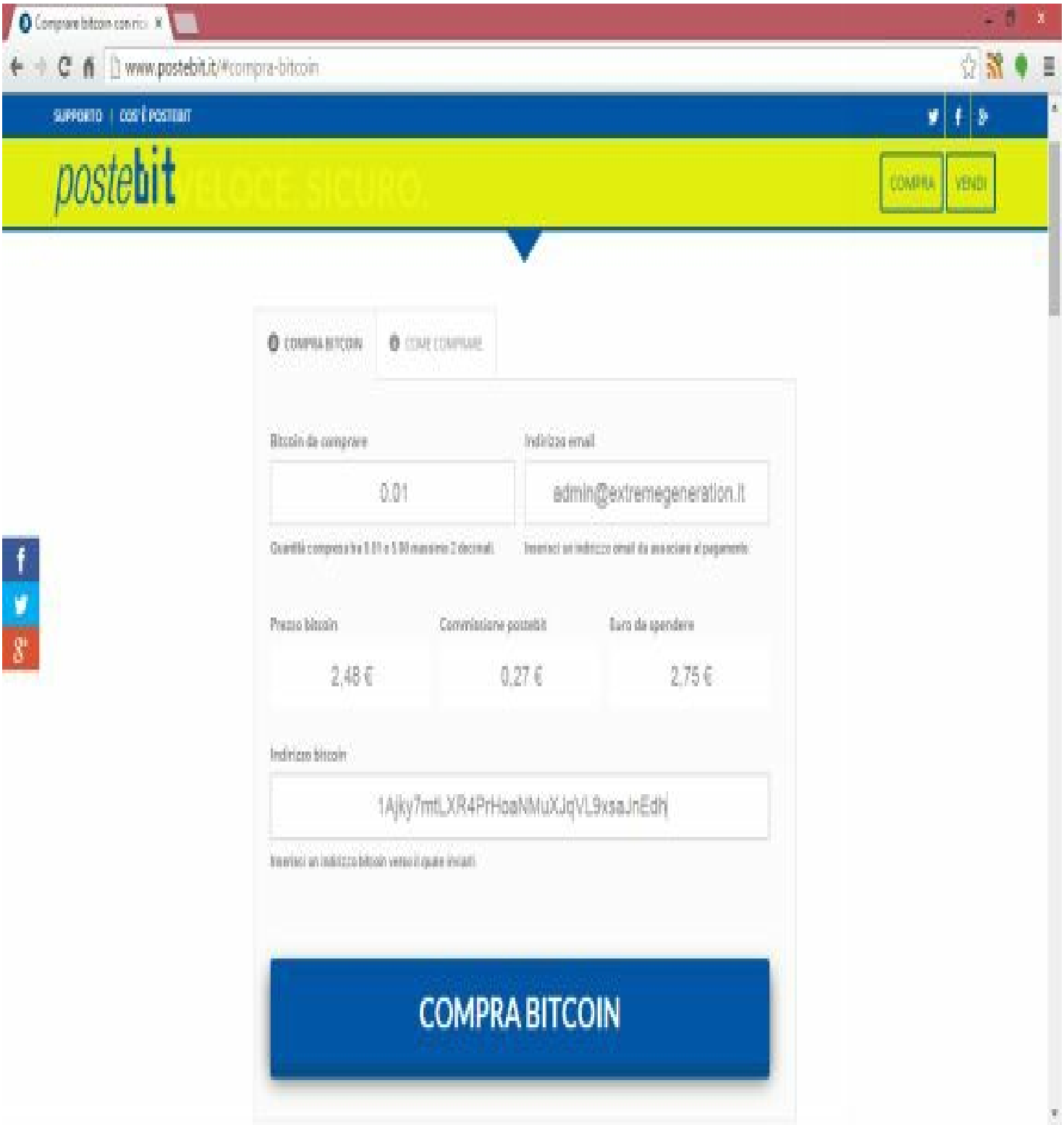


Figura 39: Transazione con PosteBit.

Prima illustrare i passi

successivi, è importante sottolineare che per acquistare BTC non è richiesta alcuna registrazione al portale (al contrario di quanto trattato nel paragrafo precedente), inoltre, in real-time viene fornito il tasso di cambio per i BTC e quello per le commissioni.

Compilati i campi è sufficiente per cliccare su "**Compra Bitcoin**" per avviare la procedura. Nella schermata successiva vengono indicati i dati della PostePay da ricaricare (numero della carta, intestatario e codice fiscale) appartenente a PosteBit. Tramite la ricarica il servizio cederà in cambio i bitcoin all'indirizzo specificato (Figura 40).

Si noti che la ricarica deve avvenire entro e non oltre 30 minuti dalla richiesta, questo per evitare un congestionamento del server. Essa può essere effettuata on-line (attraverso il sito di Poste Italiane), in un qualunque ufficio postale, oppure in un normale esercente con POS abilitato (BancaITB e Sisal). Si badi che soltanto quest'ultima modalità consente il reale anonimato, infatti non viene richiesto alcun documento o dato personale alla persona che effettua la ricarica, mentre effettuandola online e all'ufficio postale si ricade nella tracciabilità tipica delle transazioni bancarie.

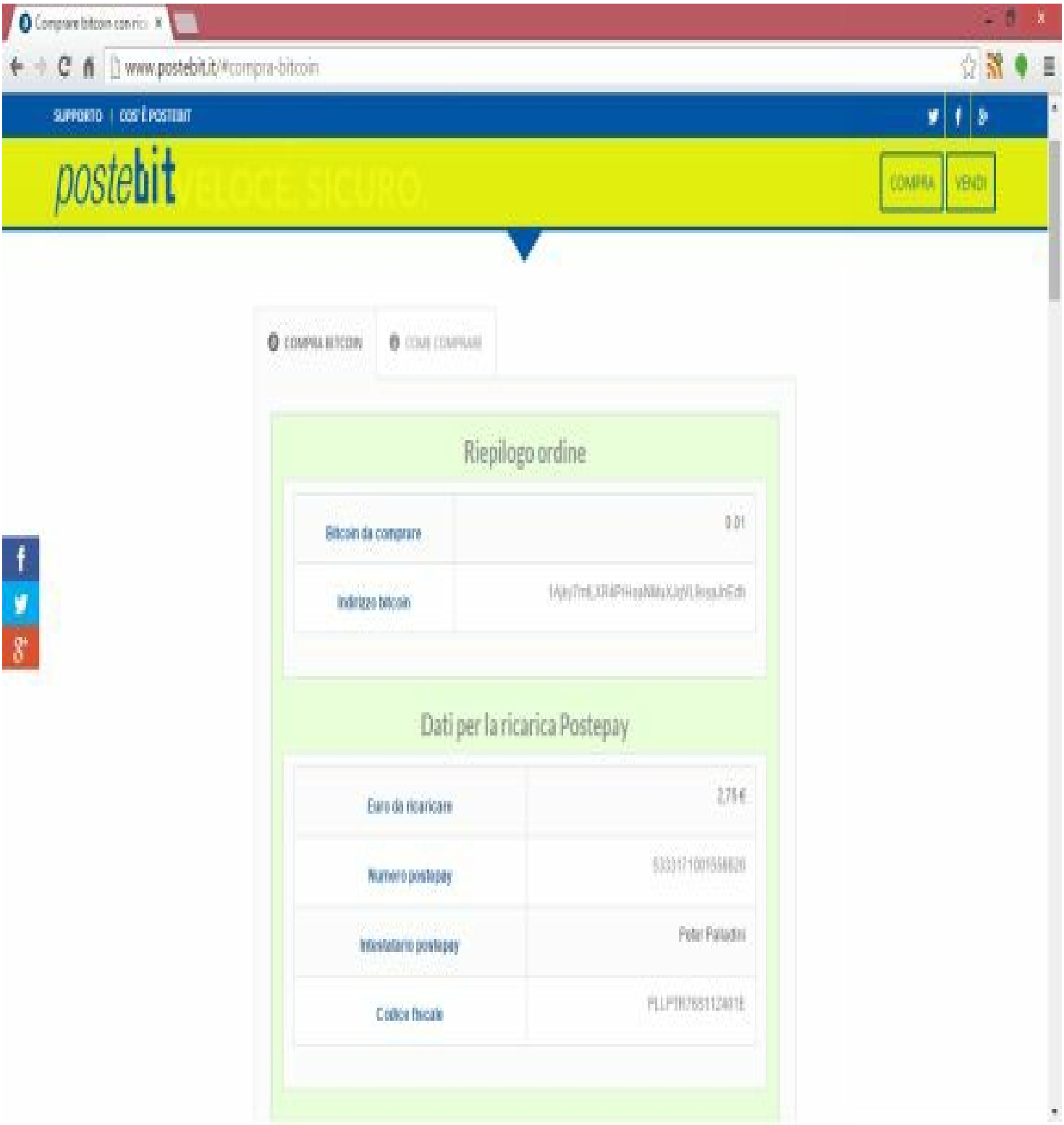


Figura 40: Riepilogo della transazione.

Il portale offre anche la

possibilità di convertire BTC in EUR, ricevendoli attraverso una semplice ricarica sulla propria carta PostePay.

E' sufficiente fornire i dati della propria PostePay sulla quale si vuole ricevere l'accredito. Come nel caso precedente, in real-time, prima di effettuare la transazione, verrà mostrato il tasso di cambio e le commissioni.

Per concludere l'operazione è sufficiente, compilato il form, inviare l'ammontare BTC richiesto all'indirizzo indicato entro e non oltre 30 minuti dalla richiesta di scambio, in maniera del tutto equivalente al caso dell'acquisto.

Ad onore della sua serietà, il portale offre un servizio di assistenza 24

ore su 24, via e-mail e cellulare, ed una FAQ[7] sempre aggiornata.

Gli autori segnalano la possibilità di utilizzare il sistema PosteBit per effettuare dei veri e propri pagamenti in cambio di beni o servizi: è sufficiente inserire l'indirizzo bitcoin del venditore (invece che il proprio) e mantenere il resto della procedura invariata. In questo modo i BTC arriveranno direttamente alla controparte in attesa del pagamento. Tale escamotage è utile a tutti coloro che non hanno a disposizione un wallet, e permette di includere nelle transazioni parti che desiderano utilizzare la criptomoneta con controparti che non ne

posseggono.

Con questo paragrafo si conclude il capitolo, lasciando al lettore il compito di indagare e provare altri siti di scambio, avendo descritto le basi del mondo Bitcoin. Per i più avversi al rischio, il consiglio è quello di utilizzare le piattaforme consigliate in quest'opera, perché sono state oggetto di prova da parte degli autori, e quindi ne certificano il funzionamento.

CAPITOLO 7

CONCLUSIONI

In questo viaggio attraverso la criptovaluta, il lettore ha ottenuto tutti gli strumenti necessari per operare con essa. Le transazioni in BTC (Capitolo 3) ed il protocollo Bitcoin stesso (Capitolo 2) non dovrebbero celare più alcun segreto, così come tutelare la sicurezza del proprio portafoglio (Capitolo 3). Sono stati visti i migliori sistemi per guadagnare qualche bitcoin online (Capitolo 4), ed in esclusiva per quest'opera l'approfondimento su di un sistema matematico per aumentare senza sosta i propri bitcoin (Capitolo 5). Inoltre, il lettore ha ottenuto gli strumenti

per muoversi agevolmente tra bitcoin e le principali valute a corso legale (Capitolo 6).

In questo capitolo conclusivo si farà il punto della situazione attuale e dei possibili sviluppi futuri inerenti il mondo Bitcoin, approfondendo alcune implicazioni economiche già introdotte nel Capitolo 1.

7.1. BITCOIN, SOLO UNA BOLLA SPECULATIVA?

L’incredibile crescita del valore del singolo bitcoin, arrivando a toccare addirittura il picco di 1BTC=1'147$ nel dicembre 2013, seguito da un relativamente rapido deprezzamento, ha celato il dubbio in molti che possa trattarsi di una bolla speculativa, paragonabile a quelle dei titoli hi tech quotati in borsa all’inizio degli anni 2000. In questo paragrafo si approfondiranno le implicazioni dovute alla speculazione nel mondo Bitcoin,

con l'intento di fornire ai lettore gli strumenti per comprendere queste dinamiche.

Anzitutto, occorre precisare sin da subito che la speculazione ha giocato un ruolo fondamentale nel determinare la diffusione dei bitcoin. Sono stati proprio gli investitori attratti dal potenziale di crescita e di guadagno di questa "*distruptive technology*"[8] che hanno fornito la spinta iniziale per una rapida diffusione. Conseguentemente, molti utenti iniziarono a contribuire nella pratica del *miner* proprio grazie alla prospettiva che la moneta continuasse a crescere di valore, e sempre più persone la scelsero come mezzo di pagamento

sul web. Il ruolo degli speculatori è quindi stato quello di aumentare, contemporaneamente, il valore complessivo dell'economia in bitcoin, le transazioni in BTC e, ancora più importante, aumentarne la diffusione e la conoscenza del fenomeno al di fuori delle cyber-comunità troppo circoscritte.

Fatta questa premessa, resta ancora da chiarire se i bitcoin possano essere considerati o meno una bolla speculativa. Si analizzi a tal proposito l'andamento del tasso di cambio nei confronti del dollaro (ovviamente, discorso analogo può essere fatto rispetto all'euro o le altre principali

valute). Dopo aver toccato l'eccezionale valore di 1BTC=1'147$, sicuramente i bitcoin si sono deprezzati considerevolmente. Tuttavia, occorre tenere presente che non si sono verificate altre fattispecie tipiche delle bolle speculative.

Infatti, l'andamento del tasso di cambio, sintetizzato dal grafico seguente, riassume in primis come i bitcoin detengano, a distanza di oltre un anno e mezzo dal valore massimo, valori piuttosto elevati rispetto alle principali valute di riferimento, a dimostrazione che il fenomeno bitcoin non si è affatto "sgonfiato".

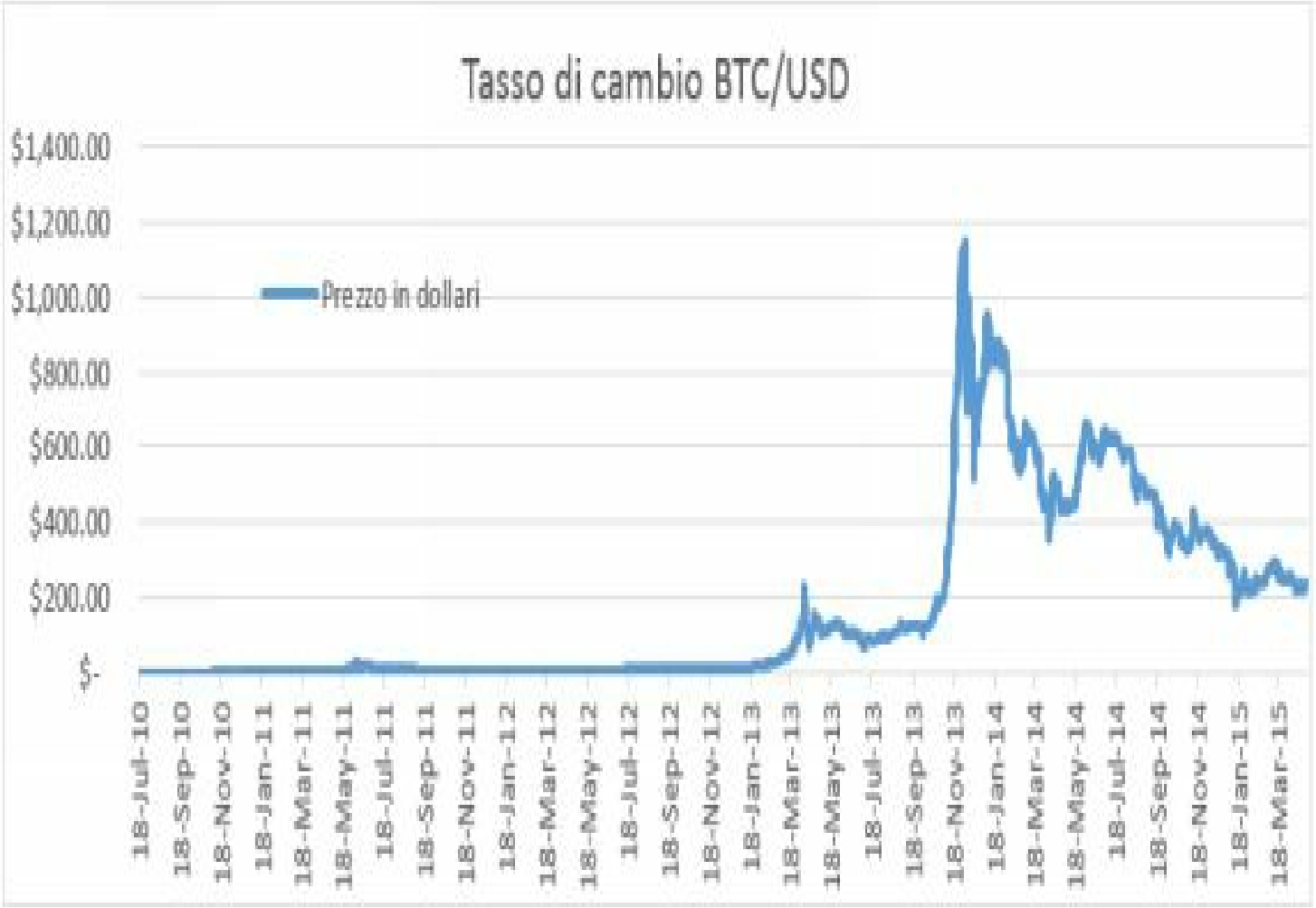


Figura 41: Serie storica BTC/USD. Fonte CoinDesk Bitcoin Price.

In secondo luogo, non c'è stato un picco discendente fino ai valori "pre-bolla", ossia riportando i bitcoin ai valori infinitesimali degli anni 2010 – 2011, come riprova del fatto che si sia

trattata di mera speculazione. Questo elemento è fondamentale per trarre delle conclusioni: il valore dei bitcoin resta, infatti, elevato, nonostante i picchi speculativi degli ultimi due anni. In altre parole, gli utenti continuano ad usare BTC per le loro transazioni, i loro acquisti, e questo basta per affermare che ci sono senz'altro le premesse per ulteriori margini d'investimento in questo business.

Si può affermare quindi, che le speculazioni in realtà abbiano agevolato la diffusione della criptovaluta stessa, ma è solo la fiducia che gli utenti ripongono nei bitcoin a determinarne o meno il successo, a prescindere da

qualsiasi attacco speculativo. Riporre fiducia nei bitcoin significa abbracciare le caratteristiche innovative e peculiari del protocollo, ed il web dimostra come sempre più persone fanno parte di questo fenomeno in espansione.

7.2. QUANTO SONO RISCHIOSI I BITCOIN RISPETTO ALLE ALTRE VALUTE

Indubbiamente i bitcoin sono contraddisti da una notevole volatilità dei tassi di cambio, con tutti i pro e i contro che ne derivano. Ma siamo sicuri che le monete a corso legale si comportino così tanto meglio da minimizzare questo rischio? Il lettore può facilmente verificarlo su un qualunque sito riportante dati del *mercato valutario* (in gergo, Forex) e scoprire come negli ultimi mesi si sono

comportate alcune importanti valute internazionali:

- In meno di 12 mesi, l'euro si è deprezzato rispetto al dollaro del 24%, passando da 1€=1.39$ in data 08/05/2014 a 1€=1.055$ in data 16/03/2015

- Il 15 gennaio 2015 può essere definito lo "*shock del franco svizzero*". In seguito ad una repentina comunicazione della Banca nazionale svizzera che ha rimosso il blocco al cambio EUR/CHF (che manteneva ancorato il tasso di cambio ad un minimo di circa

1€=1.20CHF), in una sola giornata il franco si è apprezzato nei confronti dell'euro del 30%!

- Durante i primi mesi del 2015 il Rublo (la moneta russa) si è deprezzato nei confronti dell'euro di quasi il 100% rispetto all'anno precedente.

Questi esempi dovrebbero fornire ai lettori la consapevolezza che il mercato delle valute è estremamente volatile, e le relative fluttuazioni dei bitcoin dovrebbero essere tenute in considerazione nel mercato di appartenenza, implicitamente

caratterizzato da un alto grado di rischio.

7.3. I RISCHI NEL LUNGO TERMINE DEI BITCOIN

Quest'opera ha elogiato più volte la rivoluzione introdotta dal concetto di Bitcoin, ed è oramai stato ripetuto come, a prescindere da sviluppi nel lungo termine, *oggi* si possono fare - e molte persone stanno facendo - *utili* grazie a business sviluppati in bitcoin. Tuttavia, agli autori preme mantenere fede ai propositi che hanno accompagnato l'intera trattazione, ossia uno strumento pratico ed efficace nella comprensione del mondo Bitcoin. Si

tratterà in questo paragrafo, eccezionalmente, un orizzonte temporale sul lungo termine, per fornire ai lettori gli ultimi importanti tasselli per la comprensione del fenomeno nel suo complesso.

Come già accennato, immaginare un mondo in cui i bitcoin vengono scambiati *al pari* di altre valute a corso legale è, ragionevolmente parlando, fantascienza. Molti sono i limiti che rendono questo scenario improbabile. Tra questi, tuttavia, sicuramente non è presente la mancanza di legittimazione di un'entità sovraordinata, come molti erroneamente invece tendono a pensare.

La *fiducia* alla base dell'utilizzo di una moneta ha ben poco a che vedere con la presenza di un autorità sovraordinata. Il protocollo Bitcoin in realtà risolverebbe, e nasce principalmente per questa ragione, il problema della fiducia: è stato visto che la certezza dei pagamenti è garantita, e gli algoritmi su cui si basa il protocollo garantiscono assoluta sicurezza ed anonimato, nonché l'abbattimento dei costi di transazione.

Invece, il problema da superare risiede nel *numero totale massimo di bitcoin già stabilito*, che al momento è anche il fattore che più ne ha fatto la fortuna garantendo agli utilizzatori

l’assenza del rischio d’inflazione e l’aumento del valore unitario. Come visto nel Capitolo 1, all’aumentare della domanda di bitcoin, il loro valore non può fare altro che aumentare senza sosta. Sebbene per l’uomo della strada l’inflazione è un male perché erode il potere d’acquisto dei suoi risparmi, per un’economia in espansione è necessaria. Per questa ragione, se l’economia mondiale passasse esclusivamente attraverso i bitcoin, si assisterebbe ad una contrazione dei consumi, degli investimenti e conseguentemente dell’occupazione, in una spirale recessiva. Le scelte di consumo verrebbero posticipate e ridotte, poiché i consumatori sono consapevoli del fatto

che il semplice tesoreggiare della moneta è redditizio. Allo stesso modo gli investimenti si ridurrebbero, proprio in ragione del fatto che detenere bitcoin rappresenta un impiego redditivo a sé stante!

Inoltre, come insegna la teoria economica, "contrazione di investimenti e dei consumi" significa inevitabile aumento della disoccupazione, con le note conseguenze. Insomma, i bitcoin hanno elementi tali che, senza modificarne la struttura, non sono adeguati a soppiantare completamente le principali valute internazionali. Facendo un parallelismo, i bitcoin hanno le caratteristiche di un bene scarso quale

l'oro, e nonostante alcuni opinabili "visionari" auspichino un ritorno agli scambi tramite il *gold standard*[9], lo studio della storia da un punto di vista economico insegna che ciò non è possibile in una economia complessa come quella attuale.

Un altro problema considerevole è quello dei così detti "*zombie bitcoin*": portafogli contenenti bitcoin oramai andati persi o irrecuperabili, o comunque che non sono mai stati spesi. Questi, di fatto, diminuiscono di gran lunga il numero effettivo di bicoin in circolazione, e accelerando il fenomeno deflattivo. Risulta inoltre, tramite una analisi della

BlockChain, che la maggior parte dei bitcoin non circola nel sistema, anche in ragione del fatto che non tutti gli utenti prendono le dovute precauzioni per salvaguardare la loro criptovaluta, utilizzando gli adeguati sistemi descritti in quest'opera.

In aggiunta, i bitcoin non si può dire siano equamente distribuiti tra gli utilizzatori, infatti il 10% degli utenti possiede oltre il 90% dei bitcoin creati. Ma a ben vedere, non è forse una distribuzione della ricchezza comparabile a quella che contraddistingue la società moderna, con qualsiasi altro tipo di moneta di conto? Indubbiamente la risposta è affermativa,

non occorre quindi stupirsi troppo.

7.4. QUESTI SVANTAGGI SONO RILEVANTI?

È stato visto che, obiettivamente parlando, i bitcoin non sono i candidati ideali per sostituire completamente le principali valute internazionali, ma la considerazione che gli autori vogliono trasmettere ai lettori è che… *non è rilevante*!

In primo luogo, affinché questi problemi si concretizzino, la diffusione dei bitcoin dovrebbe essere capillare, ed i lettori possono tranquillizzarsi poiché, anche nel caso questo scenario

si verificasse (una diffusione capillare dei bitcoin), il lasso di tempo necessario è grande, *molto grande*. In altre parole, c'è tutto il tempo per investire, trarre guadagni, sviluppare il proprio business, tramite bitcoin.

In secondo luogo, un abile utilizzatore della criptovaluta acquisisce un "Know-how"[10] tale che riesce ad affrontare i dinamici cambiamenti intrinsechi delle innovazioni, quale appunto il fenomeno Bitcoin. Ed è questa la ragione per cui gli autori hanno deciso di affiancare a spiegazioni pratiche alcuni fondamenti di teoria del mondo Bitcoin, e allo stesso tempo contestualizzare il tutto grazie all'analisi

economica.

7.5. ALTRE CRIPTOVALUTE

È bene precisare che i bitcon non rappresentano l'unica criptovaluta attualmente disponibile sul web, anche se indubbiamente sono il punto di riferimento per tutte le altre.

Brevemente, poiché non di competenza di questa trattazione, si citano alcune tra le più rilevanti:

- **Litecoin**: se i bitcoin possono definirsi l'oro delle criptomonete, i litecoin rappresentano l'argento.

Concepiti come una versione più "leggera" dei bitcoin, sia per quanto riguarda il *mining*, che la velocità di trasferimento (anche se il tempo per ricevere le "conferme" è più lungo). Risulta relativamente più semplice risolvere i blocchi logici per ottenere litecoin, ed il numero massimo è fissato a 84 milioni. Attualmente, risulta la seconda criptomoneta in ordine di capitalizzazione (al primo posto, inutile dirlo, risiedono stabilmente e con grande margine, i Bitcoin).

- **Peercoin**: in questo caso non è presente un numero massimo di

moneta in circolazione, ed il tasso d'inflazione è fissato all'1% annuale. Si tratta anch'essa di una moneta ispirata al protocollo Bitcoin, del quale condivide buona parte del codice. È al momento la quarta cripto moneta per capitalizzazione.

- **Dogecoin**: nasce con intenti ludici nel 2013, e conosce un improvviso successo grazie alla diffusione in alcune community, specialmente come "mancia" all'interno dei social network per gli utenti che promuovono i contenuti più interessanti o utili. Prevede

anch'essa un tasso d'inflazione programmato, grazie all'emissione annuale di nuovi dogecoin.

Per trovare ulteriori informazioni circa la capitalizzazione in dollari di tutte le cripto-valute, gli autori consigliano di vistare il seguente sito web:
http://coinmarketcap.com/currencies/dash

7.6. BITCOIN E LE ALTRE CYBER VALUTE

Si parta dal presupposto che il protocollo Biticoin è open-source[11], a dimostrazione del fatto che la competizione con le altre cripto valute non solo è possibile, ma per la natura stessa del protocollo incentivata.

Il protocollo Bitcoin è nato con un determinata logica: è basato sul fatto che il valore del singolo BTC è destinato a continuare ad apprezzarsi, dato il numero totale di bitcoin prestabilito e i costi di *mining* crescenti con progressione geometrica. Se così

non fosse, non avrebbe più senso la pratica del *mining* neanche per le grandi farm, e conseguentemente si sarebbe bloccata l'estrazione degli stessi.

Altre criptovalute sono nate con logiche diverse, ma tutte sono accumunate dal fatto di essere strettamente interconnesse nella loro quotazione con la quotazione dei bitcoin stessi. In altre parole, al centro di tutto il sistema di criptovalute ruota sempre il protocollo Bitcoin, che è il nucleo (e non il concorrente) di tutto questo ecosistema di cyber-moneta.

Inoltre, una soluzione ai problemi sul lungo termine dei bitcoin, potrebbe venire ovviata proprio da un

pool di criptovalute. Alcune di esse potrebbero infatti appoggiarsi ai bitcoin analogamente come fu stato per i sistemi aurei (con la differenza che in quel caso, c'era alla base un metallo prezioso[12]), arginando i problemi deflazionistici e creando un sistema di pagamenti e di trasferimento denaro innovativo e decentralizzato.

Tuttavia, queste sono al momento solo previsioni di possibili scenari. Comprendere i bitcoin *oggi* non solo permette di avere la possibilità di gestire il proprio business, ma consente anche di comprendere e di stare al passo con le evoluzioni e gli sviluppi futuri di un tema (le cripto valute) estremamente

affascinante e complesso.

GLI AUTORI

Alessandro Bersia

Laureato in Economia presso l'Università Bocconi di Milano, prosegue gli studi in Canada (Queen's University) e Paesi Bassi (Maastricht University) con una specializzazione in "Business Intelligence and Information Management". Gestisce e fornisce consulenza su progetti che includono Mobile App Developement, Artificial Intelligence, Blockchain Technology e Cloud Services. Sostenitore dell'*Open Innovation* come nuovo paradigma di innovazione e vantaggio competitivo, ha abbracciato con entusiasmo l'idea di

contribuire alla stesura di questo e-book sul mondo Bitcoin.

Giuseppe Silano

Laureato triennale in Ingegneria Informatica e laureando magistrale in Ingegneria Elettronica presso l'Università degli Studi del Sannio di Benevento, è sempre stato un amante del mondo elettronico, di quello informatico e delle ultime tecnologie. Crede che il futuro sia dei sistemi E*mbedded Low Cost*, quali Arduino. Sempre pronto a mettersi in gioco, ha deciso di collaborare alla stesura di questo e-book con l'obiettivo di informare il lettore su quello che crede possa essere

il futuro delle valute digitali: i Bitcoin.

Gli autori hanno collaborazioni attive con riviste informatiche nazionali (Win Magazine, EMC Elettronica).

Per comunicazioni di carattere commerciale, potete contattare gli autori all'indirizzo e-mail redazione@extremegeneration.it

Si ringraziano i lettori per tutte le segnalazione di refusi e omissioni, che possono far pervenire tramite il medesimo indirizzo e-mail.

Sommario

[1] Spese tenuta conto: rappresentano l'insieme dei costi che l'ente addebita al proprio cliente (sotto diverse forme) in funzione dei servizi offerti. Inoltre, si ricorda che anche l'imposizione fiscale (per esempio, imposta di bollo) è completamente esente nel protocollo Bitcoin.

[2] BTC: Verrà utilizzato da questo momento in poi come sinonimo per riferirsi ai bitcoin come valuta digitale (è l'abbreviazione con cui è indicato nei siti web di forex, come EUR per l'euro, USD per il dollaro statunitense, e così via).

[3] Questo significa che, essendo la commissione una percentuale (piccolissima) sulle transazioni elaborate dal miner, i suoi guadagni sono proporzionali al numero di transazioni stesse. Queste, tuttavia, sono aleatorie, perché soltanto la capacità di calcolo del processore del miner rapportata alla

complessità degli algoritmi da risolvere ne determina il numero effettivo a cui è possibile dare soluzione.

[4] In informatica, i pop-up sono degli elementi dell'interfaccia grafica, quali finestre o riquadri, che compaiono automaticamente durante l'uso di un'applicazione ed in determinate situazioni, per attirare l'attenzione dell'utente. Tipici pop-up sono quelli contenenti pubblicità e che compaiono nel browser durante la navigazione web.

[5] Un codice a barre bidimensionale, ossia a matrice, composto da moduli neri disposti all'interno di uno schema di forma quadrata. Viene impiegato per memorizzare informazioni generalmente destinate a essere lette tramite un telefono cellulare o uno smartphone. In un solo crittogramma sono contenuti 7.089 caratteri numerici o 4.296 alfanumerici. Il nome "QR" è l'abbreviazione dell'inglese "Quick Response" ("risposta rapida"), in virtù

del fatto che il codice fu sviluppato per permettere una rapida decodifica del suo contenuto.

[6] Sono dette fluttuazioni statistiche le discrepanze di valore che riguardano un evento estratto in un campione casuale (valore *osservato* o *attuale*) rispetto alla frequenza teorica dell'evento considerato in una popolazione infinita.

[7] FAQ: Frequently Asked Questions, Domande Risposte Ricorrenti.

[8] Distruptive technology: correlata al concetto di “distruptive innovation”, rappresenta una innovazione in grado di rendere obsoleta la tecnologia precedente, e conseguentemente con un elevatissimo potenziale di crescita.

[9] Gold Standard: la moneta a corso legale è basata sull’esistenza del metallo prezioso (oro), con il quale è – almeno in parte-

convertibile. Questo sistema non è funzionale ad una economia in espansione, poiché provoca deflazione e, conseguentemente, recessione. Nel 1971 gli USA abolirono la conversione in oro del dollaro, decretando la fine del sistema aureo.

[10] Know-how: competenza e conoscenza che fornisce un vantaggio rispetto ai competitor in un determinato business

[11] Open Source: il codice è disponibile per essere studiato da chiunque possieda conoscenze e tempo adeguati. È l'opposto dei sistemi chiusi, in cui il codice viene venduto e non è liberamente modificabile.

[12] Ricordiamo che la fine del sistema aureo (ossia la possibilità di convertire dollari in oro) è avvenuta soltanto nel 1971 con la fine degli accordi di Bretton Woods.