CARATTERISTICHE E FUNZIONAMENTO DELLA MONETA IN RETE

BITCOIN

MARIAM AYOUBI

INDICE

INTRODUZIONE

La rivoluzione che più caratterizza il XX secolo è la rivoluzione tecnologica, la rivoluzione di Internet, ormai da più di 20 anni, che portò una grande ondata di innovazioni in diversi ambiti, dalla sociologia all'economia, dall'area scientifica all'area umanistica.

Negli ultimi anni si è assistito ad uno sviluppo in continua crescita delle più

avanzate tecnologie, dovute soprattutto alla scoperta e all'approfondimento delle scienze crittografiche.

E' proprio grazie alla scoperta della crittografia che si è assistito ad un'innovazione tecnologica anche in ambito economico; la creazione di innovative piattaforme di scambio monetario e lo sviluppo di nuovi strumenti di pagamento caratterizza l'economia di questi ultimi anni, la cosiddetta "economia digitale", basata su una nuova ricchezza, su opportunità di lavoro e business per tutti.

L’innovazione più interessante e potenzialmente la più importante, è da fissarsi precisamente nel gennaio dell’anno 2009 con l’avvento della prima criptovaluta, inventata dall’anonimo Satoshi Nakamoto ed oggi conosciuta con il nome di “bitcoin”.

L’idea della creazione di questa nuovo cripto-moneta scaturisce da una volontà sfrenata di creare un nuovo sistema di pagamento che non si basi sulla presenza di un ente terzo, e che gestisca in completa riservatezza tutte le transazioni. L’ideazione di una

criptomoneta decentralizzata, scaturisce anche dall'insostenibilità dei costi e delle spese di creazione delle monete tradizionali.

Il presente libro si propone di presentare gli aspetti innovativi della cripto-moneta, ideata da Satoshi Nakamoto, analizzandone le caratteristiche, le funzionalità, i vantaggi e gli svantaggi.

Il libro si articola in tre sezioni.

La prima sezione "Bitcoin: la prima cripto-valuta" è volta all'introduzione dell'argomento, con un breve excursus

storico che parte dai precursori della criptovaluta in questione ed arriva all' "era" delle cripto-monete ed al loro sviluppo nella società. In questo primo capitolo ci si soffermerà sulla presentazione di questa innovazione in campo economico, ovvero di questa moneta virtuale, evidenziandone le caratteristiche, il suo utilizzo e la sua gestione.

La seconda sezione "Architettura e funzionamento della rete Bitcoin" è volta alla presentazione dell'architettura della rete Bitcoin, ed alla spiegazione in

maniera approfondita del funzionamento di essa, illustrando la tecnologia e la struttura delle transazioni.

La terza, ed ultima sezione "Bitcoin nella realtà quotidiana", procede con un'analisi empirica della moneta e della relativa rete, volta a mostrarne i vantaggi e gli svantaggi derivanti dall'utilizzo della stessa. Gli ultimi paragrafi, in particolare, sono dedicati allo studio dei rischi di un eventuale fallimento della moneta in futuro.

L'opera, dunque, si propone come analisi dei risvolti sia positivi che

negativi che le valute digitali comportano nel sistema.

Jon Matonis, Executive Director della Bitcoin Foundation nella sua dichiarazione ufficiale in favore dei Bitcoin, asserisce quanto segue: “ *Quello che le persone devono comprendere è che non abbiamo più bisogno di affidarci a un re che si prenda il disturbo di coniare la nostra moneta. Il successo dei Bitcoin ha*

dimostrato a tutti, al mondo intero, che possiamo avere una valuta completamente decentralizzata”.

Capitolo 1
Bitcoin: la prima criptovaluta

1.1 Storia

1.1.1 Dalle radici di Bitcoin alla sua nascita

La nascita ufficiale del bitcoin si colloca nel gennaio del 2009, ma la nascita di questa criptovaluta, il suo funzionamento e soprattutto la sua ideazione affondano le proprie radici nel ben remoto 1982, con la pubblicazione di un articolo di un certo David Chaum, intitolato "Blind Signature for Untraceable Payments"[1], nel quale veniva introdotto un nuovo concetto, il concetto di "firme cieche".

Le “blind signatures”, ovvero le firme cieche, sono una sorta di firma digitale che viene apposta sul messaggio prima che quest’ultimo venga aperto e letto. Le blind signatures, ad oggi, sono utilizzate maggiormente nel sistema di voto elettronico (e-voting), in cui il firmatario e l’autore del messaggio sono differenti, e perciò non coincidono con la stessa persona.

Qualche anno più tardi, precisamente nel 1988, David Chaum pubblicava un paper intitolato “The Dining cryptographers problem: unconditional sender and recipient untraceability[2]”, nel quale per la prima volta si parlava dei concetti di “chiave pubblica” e

“chiave privata” (vedi capitolo 2).

Nel 1997, David Chaum in collaborazione con Stefan Brands, pubblicava un ulteriore articolo, intitolato “Minting Electronic Cash”, nel quale venivano discussi i problemi legati alla privacy online ed ai pagamenti in rete.

Ma chi è David Chaum?

David Chaum[3] è un noto crittografo, fondatore della DigiCash Inc[4] nel 1989 e famoso per aver sviluppato l’e-cash negli inizi degli anni ‘90, un’applicazione web cash con lo scopo di preservare l’anonimato dell’utente che ne fa uso, cosa che sarà ripresa qualche anno più tardi da Satoshi

Nakamoto nella presentazione della sua criptovaluta. La corporazione fondata da David Chaum nel 1989, la DigiCash Inc, vedeva la sua innovazione nei sistemi di transazioni monetarie online. Per la prima volta le transazioni erano anonime ed erano associate ad un codice crittografico del protocollo ideato dal suo fondatore.

La corporazione DigiCash Inc dichiarò bancarotta qualche anno più tardi, nel 1998, a causa del mercato, che si dichiarava conservativo e non pronto allo slancio economico all'interno di quel nuovo contesto virtuale che stava nascendo. Il sistema di pagamento elettronico, fondato da David Chaum e

con sede e gestione nella DigiCash, prevedeva un sistema centralizzato in quanto le transazioni monetarie in rete erano controllate dalla banca emittente, la DigiCash.

Nello stesso anno della pubblicazione del "Mintin Electronic Cash", Adam Back[5], un noto crittografo britannico, inventò l'Hashcash, un software che era in grado di prevenire lo spam via mail. Adam Back, ideando l'Hashcash, fu innovatore anche perché, nel prevenire lo spam via e-mail, veniva proposto un sistema di proof of work, usato da molti sistemi antispam e che sarà oggetto dell'attività di mining ideata da Satoshi Nakamoto (vedi cap.2).

Tutti questi crittografi ed esperti della cibernetica, vivevano in un periodo in cui vigeva un particolare clima culturale di ricerca e fascino del rapporto tra l'essere umano e la tecnologia. E' proprio in questo periodo della postmodernità, all'incirca verso la metà degli anni ottanta, che si viene a formare un movimento letterario ed artistico, i quali principi differivano dalle letterature a cui siamo abituati.

In questo clima nasceva il movimento dei Cyberpunk[6], un gruppo di attivisti che vedevano nelle tecnologie informatiche e nella cibernetica strumenti utili per il cambiamento radicale nella società.

Nel novembre del 1998, in una mailing-list dei Cyberpunk, una nuova figura, per molti versi vicina a ciò che concepirà Satoshi Nakamoto successivamente, pubblicò una proposta sotto il titolo “B-money, an anonymous, distributed, electronic cash system”.

L’autore di questo trattato è Wei Dai [7], un esponente del gruppo cyberpunk, e proponeva un sistema di interscambio di valore e stipulazione di contratti, che si basavano sull’uso di una moneta digitale che garantiva l’anonimato; la moneta in questione è denominata “b-money”.

Wei Dai proponeva due protocolli nel suo trattato di presentazione di questo sistema di pagamento anonimo e

distribuito.

Nel primo protocollo Wei Dai proponeva l'utilizzo di un proof of work, inteso come strumento per creare moneta online. Wei Dai riconosceva la presenza di un eventuale contratto con un ente terzo, con il fine di prevenire perdite.

Nel secondo protocollo spiegava come i partecipanti della rete potevano verificare che il proprio importo non fosse stato soggetto a inflazione. Definiva le linee di partecipazione alla rete asserendo che un totale di denaro era un requisito fondamentale per diventare server della rete, ma poteva essere perso se il server stesso si

rivelava un server “disonesto”.

Tutte queste scoperte, studi ed innovazioni crearono le basi per la nascita del bitcoin, che circa 10 anni più tardi, veniva presentato tramite un Whitepaper intitolato “Bitcoin: a peer-to-peer electronic cash system”[8], scritto da un anonimo firmato con il nome di Satoshi Nakamoto.

Ma chi è Satoshi Nakamoto?

Di questo personaggio, famoso per il suo innovativo progetto e per la sua mente geniale, non si conosce praticamente nulla, né se sia un uomo, un gruppo di persone o una donna. Si sono mossi molti studi intorno a questo personaggio, al fine di individuarne

l'identità ma non si è mai riusciti nell'intento.

Tuttavia, vi sono delle certezze: il software Bitcoin prima di essere stato attivato, sarebbe passato per un periodo di prova, il quale avrebbe permesso allo o agli sviluppatori di correggerne i vari bug del sistema, altrimenti risulterebbe impossibile spiegarsi il fatto che Bitcoin abbia funzionato alla perfezione sin dal primo giorno.

Ma perché Satoshi Nakamoto ha deciso di non svelare la propria identità?

La risposta potrebbe essere congiunta ad episodi passati, come per esempio il caso del Liberty Dollar[9], una moneta indipendente, il quale valore era

intrinseco e basato sul valore dell'oro e dell'argento; il Liberty Dollar terminò nel 2007, portando il fondatore all'arresto, per violazione dei principi della costituzione americana.

Satoshi Nakamoto, consapevole degli effetti che questa moneta avrebbe portato, preferì evitare tutto ciò e restare anonimo, ed il 1 novembre 2008 presentò la sua nuova criptomoneta utilizzando le seguenti parole:

"Ho lavorato ad un nuovo sistema di moneta elettronica che è completamente peer-to-peer, senza nessuna terza parte fidata".

La dichiarazione rilasciata da Satoshi Nakamoto è stata resa pubblica in una

mailing list[10], che contiene discussioni riguardanti lo sviluppo delle scienze e delle tecnologie crittografiche.

Il primo software Bitcoin fu rilasciato a gennaio del 2009, sotto il nome di "Bitcoin v0.1" e presentato come un sistema di trasferimento del denaro in maniera decentralizzata, distribuita, semplice e veloce.

Tuttavia, è da aggiungere che Satoshi Nakamoto dal 2008 al 2010 seguì e diresse il suo progetto "dietro le quinte", ovvero attraverso il suo blog, la sua casella di posta elettronica ed attraverso persone che lasciò visibili come parte integrante del progetto.

1.1.2 Lo sviluppo della criptovaluta dal 2009 ad oggi

Introduco la storia del Bitcoin, con un esordio contenente un frammento di testo, tradotto in italiano da Marco Nastasi, Michele Munaretto e Gabriele Maltinti, che ispirò Satoshi Nakamoto nella progettazione del suo "capolavoro":

"Mi affascina l'idea di Tim May di una società completamente volontaria e protetta per mezzo della crittografia. A differenza del tipo di comunità

tradizionalmente associato con la parola anarchia, in una cripto anarchia il governo ed i poteri forti non vengono eliminati, ma resi incapaci di imporsi. In questo tipo di comunità, la minaccia della violenza risulta nulla, poiché non è possibile imporre violenza su membri di una comunità da identificare contro la propria volontà. ..In questo articolo viene descritto un protocollo per cui tali servizi possano essere forniti da entità anonime ad entità anonime."

Bitcoin nasce ufficialmente il **3 gennaio 2009**, con l'uscita del

primo blocco Bitcoin, il "Genesis Block"[11] (o Blocco 0), che dette avvio all'attività di mining[12] e successivamente alla creazione di nuove unità di valuta virtuale.

Con il Genesis Block, o Blocco 0, vennero generati 50 BTC, precisamente alle ore: 18:15:05. Questi 50 BTC furono generati come ricompensa, e furono accreditati in un wallet bitcoin senza esser mai stati utilizzati e/o spesi. Ancora oggi risultano intatti.

Il **9 gennaio** nacque la prima versione di Bitcoin v0.1.

Il **12 gennaio** venne registrata nella Blockchain la prima transazione avente

come mittente Satoshi Nakamoto e come destinatario Hal Finney. Il primo blocco vedeva la transizione di ben 50 BTC.

Il **16 dicembre** uscì la seconda versione di Bitcoin v0.2.

Nel **2010** nacquero i primi mercati di cambio moneta (da valuta legale a valuta virtuale), ed a maggio dello stesso anno avvenne il primo acquisto di un bene "fisico", nel quale l'acquirente fu Laszlo Hanyecz che comprò una pizza facendo un pagamento di importo pari a 10.000 BTC.

Questo fatto non passò inosservato e ad oggi troviamo negozi virtuali come PizzaForCoins.com (link al sito www.pizzaforcoins.com), nati

appositamente con lo scopo di riprendere questo episodio e crearci un business, vendendo pizze in cambio di criptovalute.

Ad **agosto 2010** si verificò un bug, ovvero un'anomalia nel sistema, precisamente nel protocollo, che causò transazioni "anomale". Nel giro di poche ore le transazioni furono annullate dagli sviluppatori ed il bug fu risolto.

L'anno successivo, il **2011** fu caratterizzato da una serie di eventi che portò le autorità governative a considerare seriamente questo nuovo fenomeno. L'FBI aprì inchieste e definì con il termine "pericoloso" questo nuovo sistema di pagamento.

Di fatto, la maggior parte dei siti, che attuavano azioni illecite online, e anche il grande il mercato nero online del Deep Web accettavano pagamenti in Bitcoin, usufruendo della caratteristica dell'anonimato delle transazioni.

Negli **anni 2012 e 2013** si assistette all'ascesa sorprendente del numero dei mercati di cambio valuta, propriamente definiti con il termine "Bitcoin Exchange", nati con lo scopo di facilitare le procedure di pagamenti online e scambio della valuta.

Successivamente a ciò, si verificò anche un forte aumento di commercianti disposti ad accettare bitcoin.

Verso gli inizi di **aprile 2013** si

assistette all'ascesa del valore dei bitcoin; 1 BTC equivaleva a circa 100 $.

Nel **2014**, per la prima volta in Italia si parlava di Bitcoin, presso la sede della Camera dei Deputati a Montecitorio; questo episodio è considerato importante perché mostra come il sistema innovativo ideato da Satoshi, sia stato preso in considerazione dalle diverse autorità mondiali, le quali ne hanno discusso la diffusione e valutato le possibilità offerte.

Nello stesso anno i due colossi della tecnologia a livello mondiale Microsoft e Overstock.com scelsero di iniziare ad accettare pagamenti in Bitcoin.

Negli **anni successivi** il valore dei bitcoin (BTC) aumentò vertiginosamente passando da frazioni di dollaro ad oltre un migliaio di dollari, e al momento (ottobre 2017) è stabile attorno ai $ 4272.46[13], dimostrando di essere una moneta molto volatile ed instabile.

Il grafico sottostante mostra il valore BTC/USD a partire dalla data 28/10/2015 fino al 30/10/2017.

Grafico 1: grafico rappresentante il valore BTC/USD del biennio 2015/2017

1.2 Presentazione della rete Bitcoin

Nel novembre del 2008 venne pubblicato su Internet un Whitepaper, intitolato “Bitcoin: A Peer-to-Peer Electronic Cash System[14]”, che presentava questa innovativa criptomoneta, il bitcoin.

Il Whitepaper fu pubblicato da un anonimo, sotto il nome di Satoshi Nakamoto, il quale descrive un sistema per il trasferimento di denaro digitale

senza la presenza di un'unità organizzativa centrale che lo controlli e ne gestisca l'emissione.

Alla base della sua creazione, c'è la volontà di superare tutte le barriere e gli svantaggi che le monete tradizionali presentavano e tutto ciò avvenne tramite la rete Internet, ancora per molti versi libera da legislazioni rigide, vertenti su tutti i lati della vita virtuale.

La rete Bitcoin, infatti, nasce con l'obiettivo di permettere transazioni che non si basano sul controllo di un ente terzo e, in questo modo, garantisce:

- indipendenza del sistema di pagamento da terze parti;
- livello molto alto di riservatezza delle transazioni;
- mancanza di restrizioni e libertà di azione all'interno del sistema monetario.

L'innovazione di questa cripto-moneta risiede nella sua natura decentralizzata, nell'assenza di un ente centrale che garantisca la disponibilità delle parti coinvolte e verifichi le transazioni.

Per fare un esempio, la Banca Centrale Europea[15] (BCE) è l'ente centrale che controlla l'euro e la sua emissione nelle regioni dell'EuroZona, analogamente la Federal Reserve[16] (Fed) controlla il dollaro americano e la DigiCash controllava la moneta elettronica ideata da David Chaum, mentre in Bitcoin manca un soggetto adibito a tale controllo.

I sistemi di pagamento tradizionali e gli intermediari finanziari, ad esempio anche quelli nominati in precedenza, si basano sul concetto di fiducia, la quale

non può essere oggetto base del sistema monetario bitcoin.

"E' proprio il concetto di fiducia, che viene a mancare nei sistemi di pagamento elettronico, e viene sostituito da un lavoro crittografico, "cryptographic proof""", spiega Satoshi Nakamoto nell'introduzione del suo trattato "Bitcoin: A peer-to-peer electronic cash system".

Infatti, il fruitore di servizi erogati da una Banca o da un intermediario finanziario, fornisce fiducia a quest'ultimi sin dal momento della

sottoscrizione del contratto fino alla trasmissione online e deposito online di denaro. Tutti gli enti garanti della sicurezza di trasferimenti di denaro in rete richiedono come pre-requisito fondamentale la fiducia[17].

La rete Bitcoin, al contrario, non richiede la presenza di un terzo fiduciario ai suoi fruitori in quanto le transazioni avvengono direttamente tra le due persone interessate, e non vi è la presenza di un soggetto terzo, che eserciti un controllo.

Con l'avvento di Bitcoin la

certificazione fiduciaria è stata sostituita con la certificazione crittografica.

Infatti, l'unica condizione fondamentale al fine di poter usufruire dell'utilizzo del software Bitcoin è l'adesione ad un protocollo comune, ovvero ad un insieme di norme che regolano il funzionamento del sistema.

Il protocollo ed il software Bitcoin hanno natura libera e sono open-source[18], ovvero aperti a tutti coloro che vogliano apportarvi delle modifiche, al fine di migliorare il sistema.

La rete Bitcoin è un grandissimo

network, formato da nodi, collegati tra loro utilizzando un'architettura paritaria (o paritetica), conosciuta anche con il nome "peer-to-peer[19]", che garantisce sicurezza, autenticità, integrità dei file, riservatezza e anonimato.

Su ogni nodo della rete, risiede un dispositivo hardware su sui lavora il software Bitcoin, il quale permette al nodo, su cui poggia, di diventare soggetto attivo nel processo di gestione della moneta digitale in rete.

I nodi della rete Bitcoin rendono possibili le transazioni, ed il loro

aumento è direttamente proporzionale all'aumento della decentralizzazione, la quale assume sempre più valore; all'aumentare dei nodi in rete, aumenta la loro indipendenza.

Questo tipo di architettura paritaria permette maggiore flessibilità e velocità delle transazioni.

In sintesi, la rete Bitcoin garantisce un nuovo sistema di pagamento decentralizzato, gestito interamente dai nodi della rete, che lavorano a pari passo con appositi Software Bitcoin in essi installati, e aderendo quindi ad un

protocollo comune, permettono transazioni elettroniche in bitcoin (rappresentati anche con la sigla BTC).

1.3 Caratteristiche della rete Bitcoin

Nel luglio del 2014, il report dell'Autorità Bancaria Europea[20] (EBA), al fine di regolamentare e definire meglio il concetto di "moneta digitale", definiva ed introduceva il termine "Virtual currency" (ovvero

"moneta digitale") come *"una rappresentazione digitale di valore che non viene emessa da una banca o un'autorità pubblica, né necessariamente collegata ad una valuta fiat*[21], *ma è accettata dalle persone giuridiche come un mezzo di pagamento, che può essere trasferito, immagazzinato o scambiato elettronicamente".*

Qualche anno prima, nell'ottobre del 2012, la Banca Centrale Europea, nel report intitolato "Virtual Currency Scheme"[22], assegnava una nuova

definizione al termine criptovaluta[23], definendo il suo utilizzo come alternativo al denaro in alcune circostanze.

Secondo la Banca Centrale Europea, una criptovaluta è *"una rappresentazione digitale di valore, non emessa da una banca centrale, da un istituto di credito o dall'istituto di denaro elettronico, che in alcune circostanze può essere utilizzata come un'alternativa al denaro"*.

Ad oggi non vi è ancora una chiara definizione, che possa rappresentare ed

inquadrare meglio la criptovaluta in questione; la Banca Centrale Europea non inquadra i bitcoin all'interno della categoria "monete", perché li considera mancanti di alcune caratteristiche che la giurisdizione economica attribuisce alla moneta, ovvero manca di trasparenza, di garanzie giuridiche e di un controllo che ne disciplini l'uso.

La Banca Centrale Europea preferisce parlare di "sistema di moneta virtuale" o "schema di moneta virtuale" (definizione originale "Virtual Currency Scheme" oppure (VCS), piuttosto che di

moneta.

Le caratteristiche che contraddistinguono la criptovaluta bitcoin dalle valute legali sono soprattutto la sua natura decentralizzata e l'assenza di soggettazione a politiche monetarie.

La natura decentralizzata della rete Bitcoin risiede nel fatto che quest'ultima non ha alcuna autorità centrale che la controlli. Le transazioni sono controllate direttamente dai nodi del network presenti sulla rete in maniera distribuita e decentralizzata.

L’altra caratteristica fondamentale è l’assenza di soggettazione a politiche monetarie, dovuta al fatto che vi è la mancanza di un’autorità centrale e questo comporta l’impossibilità dell’aumento o della diminuzione del numero di valute in circolazione. La quantità di valuta in circolazione è stabilita a priori dal protocollo con un limite massimo di 21 milioni di unità.

L’assenza di un’autorità centrale e soggetti che fungono da intermediari nelle transazioni, favorisce anche dei bassi costi di commissione, con un costo

di commissione addebitato al mittente pari a circa 0.0001 BTC (circa 0.02 €).
Oltre alle caratteristiche sopra citate, è da aggiungere che i bitcoin non hanno corso legale; i bitcoin sono accettati come mezzo di pagamento volontario, a libera scelta e accettazione sia da parte dell'acquirente che da parte del venditore. I bitcoin non possono essere utilizzati come mezzo per pagare delle contravvenzioni che hanno ad oggetto una somma di denaro, previo consenso del creditore. In aggiunta, ogni utente è libero di gestire i propri bitcoin come

meglio desidera, nessun ente né autorità esterna ha il potere di bloccare un portafogli elettronico bitcoin, senza il consenso dell'utente stesso.

Satoshi Nakamoto, nell'introduzione all'innovativa rete di pagamento elettronico da lui ideata, spiega anche un'innovativa caratteristica di questo sistema, ovvero l'impossibilità nel risalire all'identità di colui che effettua una transazione.

Le transazioni di bitcoin garantiscono un alto livello di riservatezza, in quanto avvengono tra indirizzi pubblici, celati

da codici alfanumerici, dai quali è impossibile risalire alla reale identità della persona fisica che processa lo scambio della valuta.

Tutte le transazioni sono trasparenti, perché sono registrate in un registro aperto al pubblico, la Blockchain, che può essere visualizzato da tutti, ed irreversibili perché ogni transazione di bitcoin impiega in media 10 minuti per essere confermata e non può essere annullata, perciò è importante che l'indirizzo del destinatario sia corretto.

Accedendo al sito

www.blockexplorer.com si possono vedere tutte le transazioni in tempo reale ed è possibile conoscere anche quanti bitcoin possiede un determinato indirizzo bitcoin.

1.4 Bitcoin e le principali differenze con le valute legali

Le valute virtuali sono definite come monete digitali istituite e controllate generalmente dagli sviluppatori ed

accettate ed utilizzate tra i membri appartenenti a specifiche comunità virtuali.

Nella Sezione II della Banca d'Italia, la Comunicazione del 30 settembre 2015[24] afferma che le valute virtuali (VV) sono *"rappresentazioni digitali di valore non emesse da una banca centrale o da un'autorità pubblica. Esse non sono necessariamente collegate a una valuta avente corso legale, ma sono utilizzate come mezzo di scambio o detenute a scopo di investimento e possono essere trasferite, archiviate e negoziate*

elettronicamente. Le valute virtuali non sono moneta legale e non devono essere confuse con la moneta elettronica".

Similmente, qualche anno prima, nella relazione dal titolo "Virtual Currency Schemes", redatta dalla Banca Centrale Europea nel 2012 si parlava di tre modelli, o schemi, di Moneta Virtuale, riportati in modo grafico nella figura seguente:

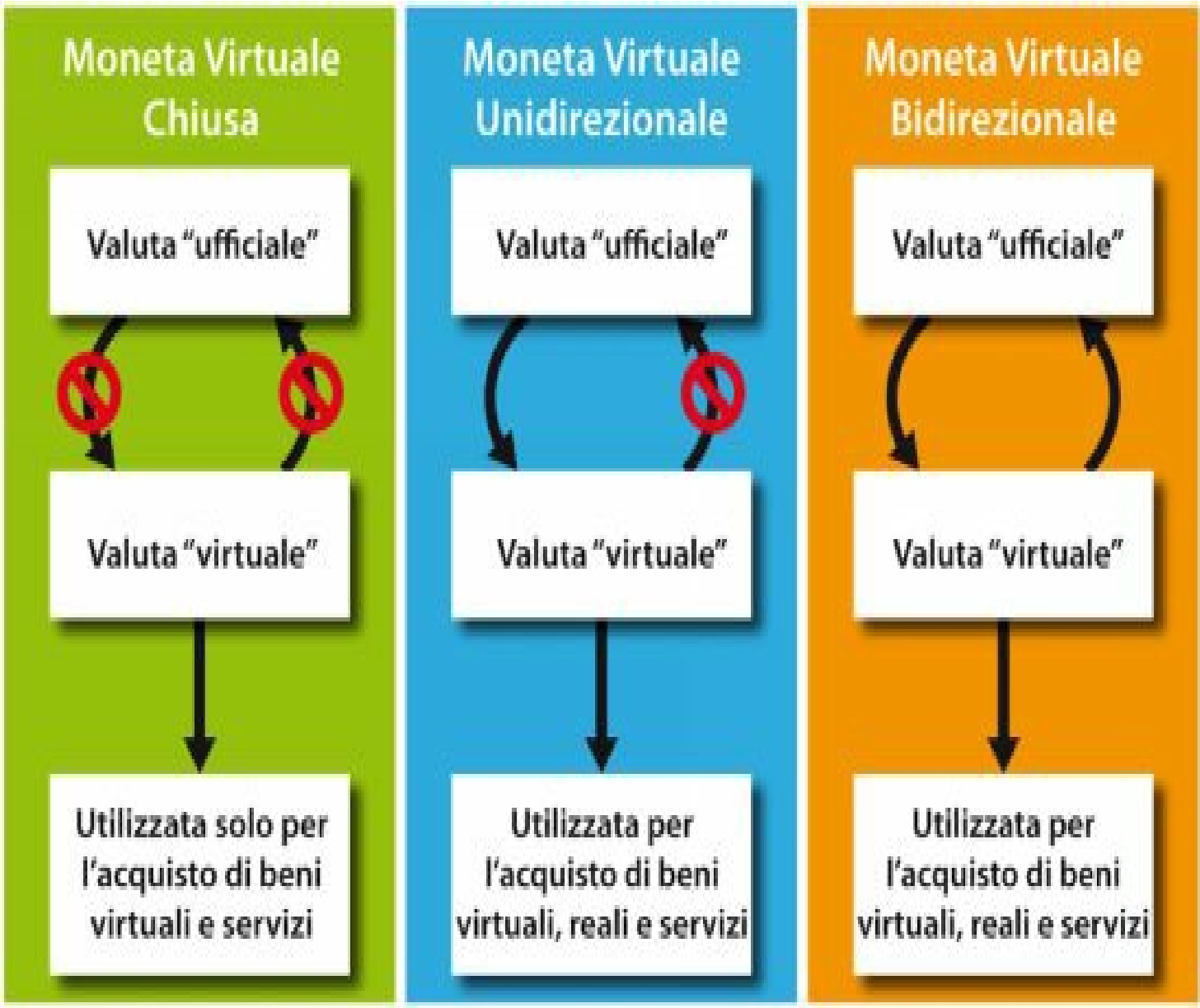


Figura 1: i diversi tipi di moneta virtuale (Report BCE, ottobre 2012)

Come si evince dalla **figura n.1** le

valute virtuali si differenziano in tre schemi[25]:

- **Schemi di valuta virtuale chiusi:** questo tipo di schemi generalmente non hanno alcun collegamento con l'economia reale e spesso sono definiti "in-game only" (ovvero valute dei giochi online). Gli utenti pagano una tassa d'iscrizione al gioco e guadagnano monete

virtuali, in base alla loro performance online. Le monete digitali guadagnate online possono essere spese solamente all'interno del gioco, acquistando beni e servizi virtuali offerti all'interno della comunità virtuale.

- **Schemi di valuta virtuale unidirezionale:** questo tipo di schemi permette l'acquisto della valuta virtuale

usando una valuta elettronica a corso legale, pagando uno specifico tasso di cambio, ma la valuta virtuale non può essere scambiata nuovamente in valuta reale. Le condizioni di conversione sono stabilite dallo schema del proprietario. Un esempio è offerto da Facebook Credits.[26] I crediti di Facebook possono essere acquistati utilizzando valuta reale e

spesi per applicazioni di Facebook e giochi.

- **Schemi di valuta virtuale con flusso bidirezionale:** questo tipo di schemi permette agli utenti la compravendita delle valute virtuali, pagando solamente le tasse di cambio vigenti nei paesi proprietari della valuta reale scambiata. La moneta virtuale, in questo tipo di

schema, è allo stesso piano di una normale valuta legale, per quanto riguarda la sua interoperabilità con il mondo reale. Questo tipo di schemi permette l'acquisto di beni, servizi digitali e reali con le valute virtuali.

I bitcoin e le altre criptovalute, definite con il termine Altcoins[27], fanno parte del terzo tipo di schema, ovvero lo schema di valuta virtuale con flusso bidirezionale, perché possono essere sia

acquistati che venduti in cambio di valute reali e permettono anche l'acquisto di beni e servizi reali.

La Direttiva 2009/110/CE[28] del Parlamento Europeo e del Consiglio del 16 settembre 2009 ribadisce che *"i modelli di moneta virtuale non devono essere confusi con la moneta elettronica, un equivalente digitale di denaro contante, memorizzato su un dispositivo elettronico o in remoto su un server"*; il Parlamento Europeo pone perciò su due piani diversi le monete virtuali e le monete elettroniche.

Le differenze tra le monete virtuali e le monete elettroniche sono molteplici. Di seguito sono riportate alcune differenze rilevanti:

- le transazioni delle monete virtuali non richiedono alcun costo di commissione (e se presente, si tratta di piccole frazioni di valuta), cosa molto comune nelle transazioni delle monete elettroniche, nelle quali una piccola percentuale viene addebitata al mittente da parte della Banca

garante;

- impossibilità da parte dello Stato o un'altra entità autoritaria di conoscere l'importo totale presente in un determinato portafoglio elettronico; quest'ultimo cela l'identità del possessore dietro codici alfanumerici, che saranno meglio spiegati nei prossimi capitoli. Contrariamente a quanto definito prima, nelle valute elettroniche tutte le Banche garanti dei servizi hanno libero accesso ai diversi conti dei propri clienti;

- le transazioni delle monete virtuali sono molto veloci rispetto alle transazioni di monete elettroniche. Il concetto di velocità delle transazioni è spiegato Franco Cimatti, esponente della Bitcoin Foundation Italia[29], con la seguente frase: *"ogni transazione deve essere data per buona dal 51% dei nodi della rete. I possessori dei registri controllano tutto, e questo garantisce una velocità delle transazioni impossibile per un istituto di credito"*;

- le valute virtuali sono state pensate per Internet ed hanno vita solo all'interno del contesto virtuale; le valute legali, invece, sono state create prima dell'avvento di internet e soffrono questo nuovo ambiente, per certi versi difettoso e contrario alla loro natura, che comporta ad esse molti problemi di aggiornamento e di sicurezza dei pagamenti.

1.5 Le valute virtuali

La rivoluzione di Internet ha interessato molti settori della vita umana, rivoluzionandola completamente.
Con l'avvento di Internet, e dei servizi apportati da esso, la vita quotidiana ha trovato facilitazioni in ogni campo, ed è cambiata la nostra percezione della società, dell'economia, della politica, che per certi versi si sono dovute "adattare" alle nuove necessità ed esigenze umane adottando un'ottica del

tutto innovativa, ovvero l'ottica della tecnologia.

L'avvento della tecnologia ha interessato anche l'ambito economico, in particolar modo le Banche che si sono dovute anch'esse "adattare" a quest'ondata di innovazione virtuale, permettendo e garantendo pagamenti online in moneta elettronica, transazioni e deposito di soldi in sistemi in rete adibiti a tale ruolo.

E' proprio in questo processo di transizione tra l'età pre-tecnologica e l'età tecnologica, che si vennero a

creare le valute virtuali, presentate come una possibile alternativa futura alle valute legali.

Le valute virtuali (VV) nascono come un mezzo di pagamento autonomo, non controllato da una banca centrale.

Infatti, esse sono prive di entità fisica e materiale; hanno vita soltanto all'interno della rete dove vengono generate, memorizzate e utilizzate.

Negli ultimi anni, con la scoperta e con la conoscenza sempre più approfondita delle scienze crittografiche, si vennero a creare un nuovo tipo di valute virtuali

che sfruttano la crittografia al fine di permettere transazioni in rete. Questo nuovo tipo di valute virtuali prende il nome di “criptovalute”.

La prima criptovaluta nacque nel 2009 e prende il nome di bitcoin, il cui codice valutario è indicato con la sigla BTC. Questa prima criptovaluta nacque con l’intento di garantire pagamenti veloci, anonimi e sicuri, direttamente tra due utenti.

Negli anni a seguire accanto al bitcoin, vennero create altre criptovalute virtuali che, prendendo esempio dal bitcoin, si

sono differite, dalla criptovaluta madre, per delle loro peculiarità e ad oggi le più diffuse sono: Ripple, Ethereum, Litecoin, Dash, NEO, NEM.

Tali valute sono definite anche con il termine "Altcoins" (abbreviazione di Alternative Coins), termine indicante tutte le criptovalute nate come alternativa al bitcoin.

Dal sito www.coinmarketcap.com sono registrati tutti gli Altcoins e sono mostrati i rispettivi valori, la rispettiva capitalizzazione e le caratteristiche, per le quali si contraddistinguono dalla

valuta madre.

1.6 Gestione dei bitcoin

Sono in continuo aumento le piattaforme online che, accanto ai metodi di pagamento tradizionali, accettano anche pagamenti in bitcoin.
A questo proposito sorgono spontanee le domande:

Come si ottengono i bitcoin?
I bitcoin si possono ottenere sia

attraverso il loro acquisto su piattaforme online che ne permettono l'acquisto, sia effettuando uno scambio di valuta con il proprio conto bancario.

Dove vengono custoditi i bitcoin?

Allo scopo di conservare il proprio contante digitale al sicuro, di poter ricevere ed inviare denaro digitale, è necessaria la creazione di un portafoglio elettronico, conosciuto con il termine inglese "wallet bitcoin", che possiede la stessa funzione e finalità di un portafoglio reale, ovvero la custodia del

denaro.

Come si trasferiscono i bitcoin da un portafoglio elettronico all'altro?
Per effettuare il trasferimento di contante digitale, si deve accedere al proprio portafoglio elettronico tramite un dispositivo elettronico, inserire l'importo da inviare e fornire un codice di riferimento al portafogli del destinatario.

Le risposte dettagliate alle precedenti domande saranno oggetto dei prossimi

paragrafi.

1.6.1 I portafogli elettronici di Bitcoin

I portafogli elettronici di Bitcoin, detti anche wallet bitcoin sono file in cui vengono custoditi i bitcoin di un determinato utente.
I wallet bitcoin offrono un'interfaccia intuitiva, che permette all'utente la visualizzazione del totale di bitcoin di cui egli dispone su tutti gli indirizzi che quest'ultimo possiede, in maniera

semplice, rapida e intuitiva. All'interno di un wallet bitcoin è possibile la visualizzazione della quantità di bitcoin nel portafogli, il relativo valore equivalente rispetto alle valute legali principali e le transazioni in entrata ed in uscita.

Tutti i wallet Bitcoin hanno tre sezioni principali :

- **saldo:** nella sezione "saldo" vi è il saldo attuale e lo storico di tutte le transazioni;

- **invia:** nella sezione “invia” si possono inviare i bitcoin dal proprio wallet ad un altro indirizzo bitcoin, conosciuto come bitcoin address;
- **ricevi:** nella sezione “ricevi” si produce il bitcoin address da passare alla controparte o il Qr-code da far scansionare per ricevere i bitcoin.

Tuttavia, i bitcoin sono memorizzati all’interno di un registro aperto, definito

con il termine “blockchain”[30], presente in rete come una sorta di lista di codici alfanumerici di 26-35 caratteri (Bitcoin address[31]), generalmente inizianti per i numeri 1 o per 3, ed assumono la dicitura della seguente stringa “1BvBMSEYstWetqTFn5Au4m4GFg7xJ[32]”.

Ogni bitcoin address, ovvero ogni indirizzo presente nella blockchain, è associato ad una chiave pubblica[33], la quale a sua volta è associata ad una chiave privata[34]. Questa associazione

di molteplici codici ha il fine di rendere impossibile risalire all'identità del proprietario dell'indirizzo; infatti, il meccanismo crittografico delle firme digitali[35], permette di spendere dei bitcoin di uno specifico indirizzo solo se si possiedono la relativa chiave privata. Al momento della creazione di un portafogli elettronico bitcoin, automaticamente vengono create cento coppie di chiavi private e pubbliche (dette anche key-pool), che permettono all'utente di utilizzare diversi indirizzi per spendere i propri bitcoin a proprio

piacimento, usufruendo di maggiori livelli di sicurezza.

Esistono diverse tipologie di portafogli elettronici[36] da poter scegliere, a seconda dei livelli di praticità, sicurezza e complessità desiderata:

- Wallet centralizzati (o Online wallet)
- Wallet decentralizzati (o Desktop/Mobile wallet)
- Wallet Hardware
- Wallet cartacei (o Paper wallet)

Wallet centralizzati (o Online Wallet): i wallet centralizzati, conosciuti anche come “online wallet”, sono siti web che custodiscono online i bitcoin di un determinato utente. In questo tipo di portafogli, l’utente fornisce le chiavi private del proprio indirizzo bitcoin a siti web, e quest’ultimi in cambio forniscono servizi di custodia online del denaro del cliente. Le chiavi private dell’utente, negli online wallet, vengono memorizzate all’interno di server online posti sotto la tutela dei fornitori del

servizio, i quali avranno accesso a tutti i trasferimenti dei loro clienti.

Questo tipo di portafogli non garantisce alti livelli di sicurezza, in quanto facilmente vulnerabile da parte di eventuali attacchi hacker al sistema.

Inoltre, l'online wallet richiede all'utilizzatore del sistema di "fidarsi", in quanto la piattaforma, nella quale sta depositando i propri risparmi, avrà il pieno controllo dei suoi fondi; tale tipologia di wallet, richiedendo la fiducia del fruitore del servizio, non rispetta una delle caratteristiche

principali della rete Bitcoin, ovvero la garanzia dell'anonimato.

Di fatti si richiede all'utente la conferma della sua identità, della residenza ed un eventuale motivazione/causale della transazione.

L'online wallet ha il vantaggio di essere veloce e facilmente accessibile, perché ci si può accedere direttamente dall'omonima applicazione e gestire in totale autonomia il proprio denaro.

Una delle piattaforme private che offrono questo tipo di servizi è Coinbase

(link al sito https://www.coinbase.com/?locale=it), fondata in California, negli Stati Uniti il 20 giugno del 2012.

Di seguito l'interfaccia della piattaforma Coinbase:

Figura n.2 : piattaforma online della società di scambio di beni digitali Coinbase

Coinbase offre servizi connessi all'assistenza reale e gestione del proprio conto; servizi non offerti dai wallet decentralizzati. Coinbase

presenta un'interfaccia molto semplice ed intuitiva ed, al fine di permettere l'inizio dell'attività di vendita/ricezione bitcoin e dunque la creazione del wallet, richiede l'inserimento dei seguenti dati personali e le seguenti azioni:

- inserimento dell'e-mail;
- conferma dell'indirizzo e-mail inserito;
- impostazione di una password sicura;
- inserimento del proprio numero di cellulare;

- verifica del numero di cellulare, attraverso l'inserimento di un codice ricevuto per SMS al numero indicato in fase di registrazione. Inoltre, ogni volta che viene effettuato l'accesso all'area personale, viene richiesto l'inserimento del codice ricevuto sul proprio numero;
- caricamento immagine fronte e retro di un documento;
- inserimento del metodo di pagamento prescelto.

Avendo testato personalmente la

piattaforma in questione, espliciterò meglio i passaggi che avvengono nella fase post creazione di un'area personale. Coinbase richiede la verifica e l'inserimento dei dati indicati precedentemente attraverso cinque passaggi, l'ultimo e quinto passaggio permette la possibilità di acquistare o vendere bitcoin.

La seguente immagine mostra l'interfaccia di configurazione dei dati personali richiesta da Coinbase e i passaggi da seguire al fine di completare il proprio profilo; i passaggi richiesti

sono l’inserimento di (vedi anche figura n.3):

- e-mail
- phone
- carica ID
- payment
- acquista

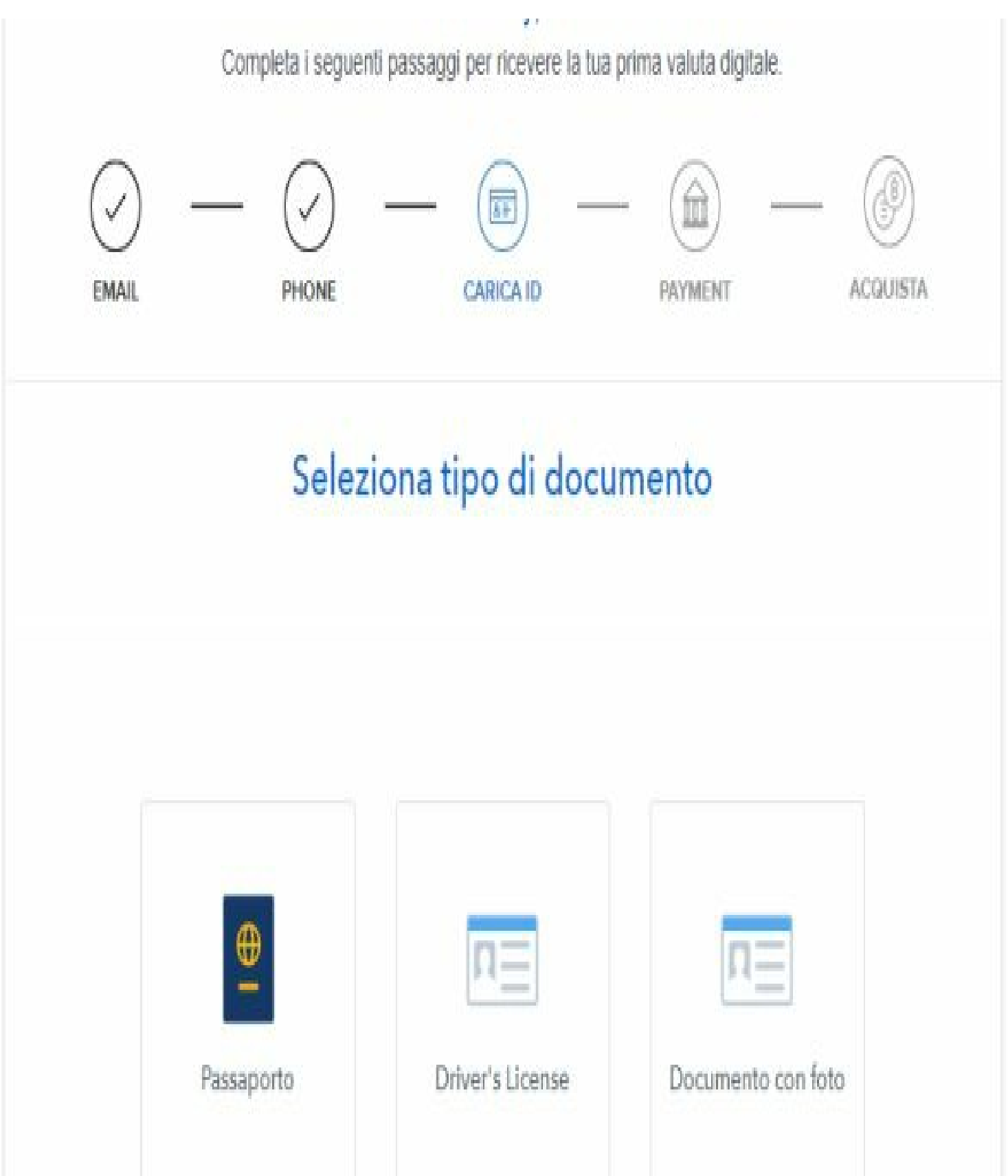


Figura n.3: la piattaforma Coinbase richiede i sopra indicati dati personali

prima di permettere l'acquisto di criptovaluta

Un'altra piattaforma che offre servizi di custodia di bitcoin online è Xapo (link al sito https://xapo.com/). Una piattaforma molto ben studiata, con grafica curata e coerente, che permette a chiunque di crearsi il proprio online wallet in pochi secondi attraverso pochi passaggi: cliccando su "Sign up", inserendo la propria e-mail, creando un Pin di 4 cifre ed una password.

Wallet decentralizzati (o Desktop wallet): questo tipo di portafogli elettronico richiede il download di uno specifico software, chiamato Software wallet, sul proprio computer. Le chiavi private dell'utente sono custodite all'interno dell'hard disk. I Wallet decentralizzati hanno il vantaggio di garantire un'elevata sicurezza e permettono agli utenti di gestire il proprio conto con totale

autonomia e controllo sul proprio denaro, senza la presenza di un ente terzo.

Nonostante ciò, è bene prendere le dovute precauzioni, e rendere il proprio computer immune da eventuali attacchi hacker al sistema operativo, aggiornandolo periodicamente, installando software antivirus ed effettuando costanti backup.

Il primo Desktop wallet creato fu Bitcoin core (scaricabile dal seguente link https://bitcoin.org/it/scarica),

conosciuto anche come Satoshi client, che fu attivato nel 2009, in concomitanza con la nascita del sistema Bitcoin. Satoshi client permette di inviare/ricevere bitcoin in tempo reale direttamente dal/sul proprio conto, accedere alla visione della mappa dei commercianti di bitcoin e richiedere assistenza.

Wallet decentralizzati (o Mobile wallet): sono applicazioni per Smartphone che consentono di avere

il proprio portafogli elettronico, sempre a portata di mano. Sono semplici, intuitivi, veloci e facilmente accessibili a differenza dei Desktop wallet, che richiedono la presenza del PC sempre a portata di mano, fattore di scomodità. Questo tipo di portafogli richiede il download solamente di una parte della blockchain. Fra i diversi Mobile wallet decentralizzati, i più conosciuti per sistemi Android sono i seguenti:

Figura n.4: mobile wallet per Android (fonte https://bitcoin.org/it/wallets/mobile/andr

Per i sistemi IOS invece troviamo:

Figura n.5: mobile wallet per IOS (fonte https://bitcoin.org/it/wallets/mobile/ios/)

Queste applicazioni per smartphone offrono interfacce utente e grafica molto ben studiate e ben impostate, garantendo un'elevata praticità d'uso e comodità.

Tuttavia, questo tipo di wallet non rispetta tutti i punti salienti, per i quali è nato Bitcoin, ovvero: trasparenza del codice sorgente, alti livelli di privacy e sicurezza e transazioni decentralizzate. I mobile/desktop wallet spesso richiedono una conferma delle transazioni da parte di un ente terzo, prima di permettere il deposito o il trasferimento dei bitcoin nel wallet di destinazione.

Wallet Hardware: sono

dispositivi hardware, aventi la forma di una pennetta USB, che contengono le chiavi private dell'utente. Vantano di un'enorme grado di sicurezza dati e trasferimento denaro, in quanto il pieno controllo del portafogli è in mano al proprietario. Questi dispositivi vengono collegati al computer ed appongono una firma digitale su tutte le transazioni, utilizzando le chiavi private dell'utente. L'utente, che utilizza questo tipo di

portafogli, dovrà semplicemente controllare l'esattezza dell'indirizzo del destinatario ed autorizzare l'avvio della transazione, attraverso l'inserimento di un codice PIN sul proprio hardware wallet. Nel caso in cui venissero commessi degli errori di battitura durante la trascrizione dell'indirizzo bitcoin del destinatario, il sistema individua che il bitcoin address immesso è errato e permette all'utente di

correggerlo, a meno che non si vada a trascrivere l'indirizzo bitcoin di un altro utente, in questo caso tutti i bitcoin inviati verranno persi in maniera definitiva.

Gli Hardware wallet sono i dispositivi di custodia delle chiavi private dell'utente più sicuri, perché anche se il computer è contraffatto, essi sono immuni da eventuali attacchi hacker e furto delle chiavi private in essi contenute. Uno dei più famosi Hardware wallet è Ledger, collegabile

direttamente al PC. E' usato come un supporto fisico per il deposito di bitcoin e si interfaccia con il PC principale. Altri esempi di Hardware wallet sono DigitalBox e Trezor.

La seguente immagine mostra i diversi tipi dell'Hardware wallet Ledger:

Figura n.6: diverse tipologie di hardware wallet Ledger

Wallet cartacei (o Paper wallet): sono supporti cartacei nei quali vengono custodite le chiavi private

dell'utente. Gli online wallet di solito forniscono la possibilità di stampare le chiavi private dell'utente in formato cartaceo creando in questo modo un wallet cartaceo (vedi figura n.7).

Una volta creato il proprio Paper wallet, la chiave pubblica è automaticamente eliminata dalla rete, ed il supporto cartaceo rimane l'unico elemento che la custodisce; è perciò consigliata la conservazione del supporto cartaceo in maniera adeguata. Questo tipo di wallet è certamente il più sicuro ed affidabile,

perchè estrapola qualsiasi tipo di codice associato all'utente dalla realtà virtuale, tenendolo in questo modo lontano da possibili cyber truffatori. Tuttavia, il paper wallet presenta anche degli svantaggi quali la possibile degradazione della carta nel corso degli anni con conseguente illeggibilità del codice o lo smarrimento del supporto cartaceo con conseguente perdita irreversibile di tutti i bitcoin presenti in quel determinato wallet.

Siti come https://www.bitaddress.org

[37] permettono la stampa delle proprie chiavi private e pubbliche su supporti cartacei, che possono essere anche stampati gratuitamente dal sito Bitcoinpaperwallet.com.

Figura n.7: Esempio di Paper Wallet

1.6.2 Ottenere i bitcoin

I bitcoin possono essere acquistati da molti servizi in rete; alcuni servizi hanno sede in uno stato ed oltre alla moneta

legale del proprio Paese, accettano anche monete da altri Paesi. Inoltre il Web è pieno di siti che forniscono servizi di compravendita di bitcoin in cambio di moneta legale o di criptovalute alternative, gli Altcoins. Prima di procedere all'acquisto di bitcoin online, bisogna tenere in considerazione diversi fattori, quali la percentuale di commissione che la piattaforma online stabilisce per vendere la criptovaluta, l'importo massimo acquistabile ed i tempi di erogazione di criptovalute.

Tali piattaforme sono definite market makers[38] ed hanno il compito di stabilire i tassi di cambio delle

principali valute tradizionali o di altre valute virtuali.

Una delle principali piattaforme online che consentono di acquistare bitcoin in rete è Coinbase, nominata in precedenza in merito al servizio di wallet elettronico che offre.

L'acquisto di criptovalute sulla piattaforma Coinbase può avvenire solamente previa registrazione sul sito, creando la propria area personale. Una volta effettuato l'accesso nella propria area personale, è possibile acquistare criptovalute direttamente cliccando sul link "Buy Bitcoin".

Nella sezione "Buy Bitcoin", tramite una grafica semplice ed intuitiva, sono

mostrati: il corrispettivo importo di un'unità di criptovaluta nelle diverse valute legali, l'ammontare delle spese di commissione e l'importo totale. Cliccando su "Continue", si verrà indirizzati nella pagina contenente le diverse modalità di acquisto accettate tra cui Paypal, Postepay, Bonifico SEPA ecc.

La seguente immagine mostra l'area "Buy Now" della piattaforma online di compravendita di criptovalute Coinbase.

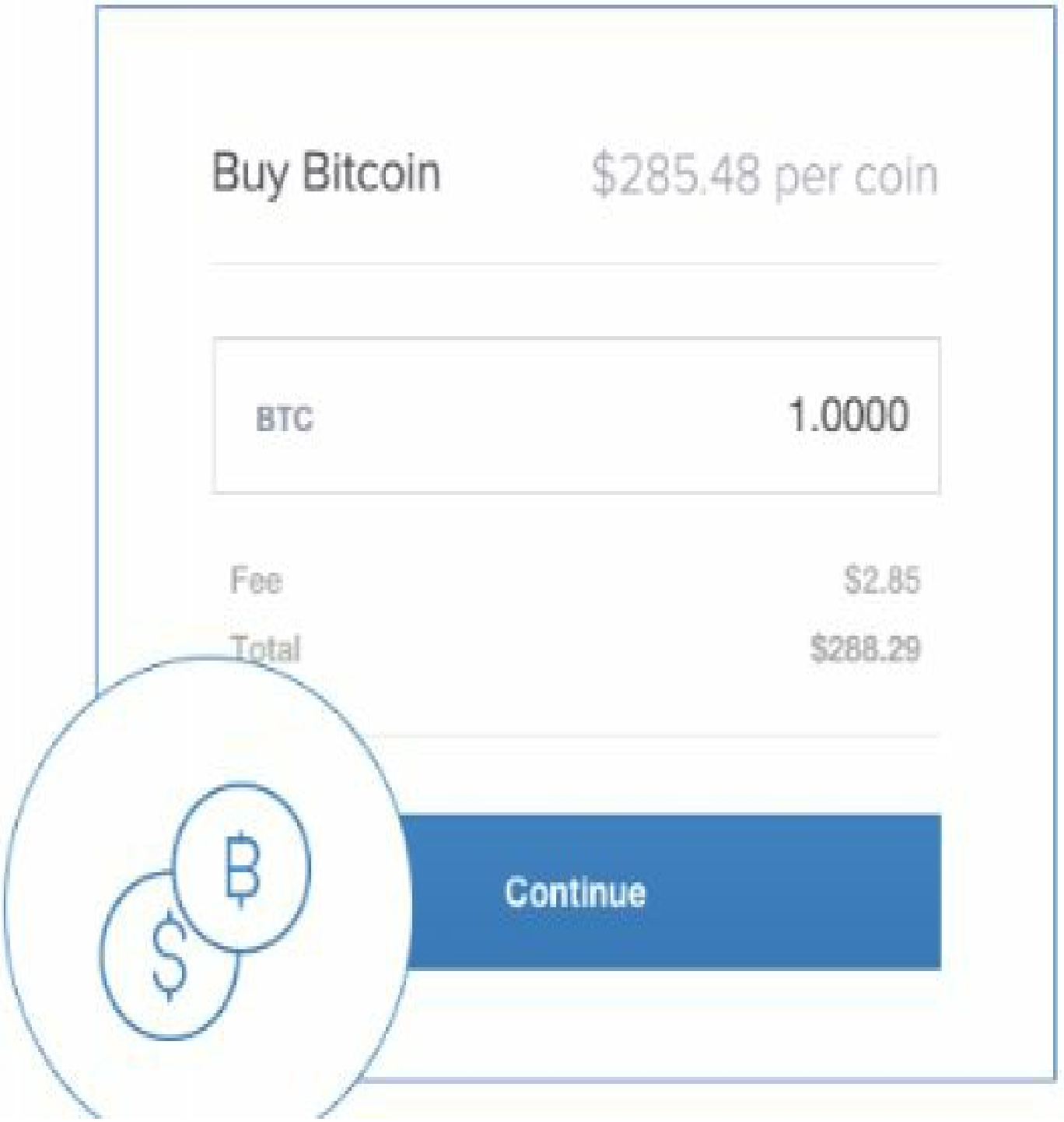


Figura n.8: area "Buy Now" del sito https://www.coinbase.com/home

Analogamente, si possono vendere

bitcoin direttamente dalla sezione "Vendi Bitcoin" scegliendo le diverse modalità di accredito previste dal sito.

Coinbase, tuttavia, oltre al bitcoin, permette la compravendita di altre due criptovalute: Ethereum e Litecoin (definite Altcoins).

Altre piattaforme internazionali di compravendita online di criptovalute sono Xapo, LocalBitcoins, Bitstamp.

In sintesi, per acquistare criptovalute online è sufficiente la registrazione sul sito, l'inserimento dell'importo da acquistare e verrà calcolata una percentuale di commissione che la piattaforme trattiene, generalmente pari al 0.20%.

Un altro metodo per acquistare i bitcoin è l'incontro fisico con l'acquirente stesso. localbitcoins.com è un sito che mette in contatto utenti privati che vogliono acquistare o vendere bitcoin, è soprannominato l' "eBay dei Bitcoin" o il "Subito.it dei Bitcoin". E' presente in 7.644 città e 240 paesi tra cui anche l'Italia.

Si possono incontrare persone disposte a vendere dei bitcoin anche attraverso bitcoin.meetup.com, un social network che raggruppa persone per aree di interessi, tempo libero e comunanze.

L'acquirente di bitcoin per acquistare criptovalute può scegliere di acquistarle utilizzando i diversi metodi di

pagamento online (per esempio tramite bonifico bancario, paypal, postepay ..), oppure accordando un incontro con il venditore ed effettuando un pagamento cash in contanti; è importante che nel luogo d'incontro vi sia un accesso libero ad Internet al fine di permettere le transazioni.

Un altro metodo per ottenere bitcoin sono i punti Automated Teller Machine[39] (ATM) che forniscono servizi di prelievo contanti o versamento contanti dal/nel proprio conto bitcoin; i bitcoin versati verranno convertiti nel valore rispettivo di valuta legale. Prima di prelevare o versare contanti presso un punto ATM bitcoin è

necessario eseguire il download del portafoglio elettronico (wallet bitcoin) sul proprio dispositivo hardware e generare un indirizzo bitcoin (bitcoin address) e il relativo QR Code da far scansionare all'ATM bitcoin.

Anche qui, sono previste spese di commissione che variano in ogni ATM.

Il primo ATM (Bancomat) bitcoin al mondo fu creato dalla Robocoin[40] USA, e venne installato presso la Waves Coffee House di Vancouver in Canada e cominciò a funzionare il 1º novembre 2013, effettuando circa 81 transazioni per un valore totale di 10.000 $.

Il primo ATM bitcoin in Italia (terzo in Europa dopo quelli di Helsinki e

Zurigo), ha cominciato a operare a Udine il 20 febbraio 2014 ed uno dei responsabili dell'installazione fu Luca Dordolo[41], che ribattezzò BTM per marcare la differenza con gli altri ATM tradizionali.

Attualmente ci sono 1610[42] Bancomat Bitcoin, di cui il 75% negli Stati Uniti. In Italia ci sono 11 Bitcoin ATMs (aggiornato al 30/09/2017).

Tuttavia, esistono anche molte applicazioni per Smartphone Android che localizzano gli ATM Bitcoin più vicini; una di esse è "Qui Bitcoin".

Secondo una ricerca condotta da coinatmradar, l'installazione di ATM Bitcoin nel mondo è in forte ascesa e se

ne contano circa 4 installazioni giornaliere, fornite dalla società Genesis Concept.

Genesis Concept è una società che gestisce le installazioni di ATM Bitcoin nel mondo e si occupa della fornitura dei POS Bitcoin a tutti gli imprenditori ed aziende che fanno parte di questa nuova realtà.

La seguente figura mostra un grafico contenente il numero di ATM Bitcoin installati dal 2013 al 2017.

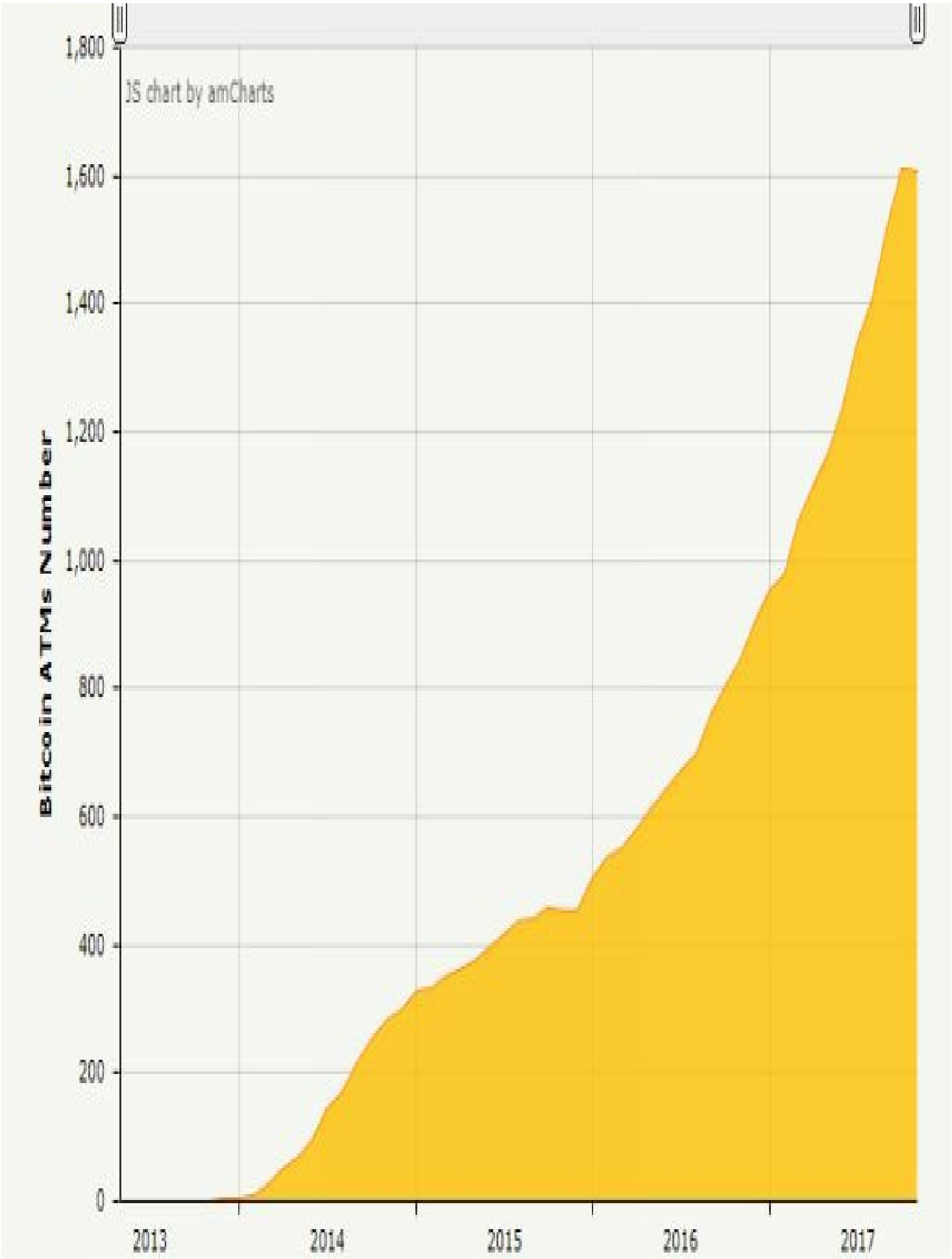

JS chart by amCharts
Bitcoin ATMs Number
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
2013
2014
2015
2016
2017

Figura n.9: Numero di Bitcoin ATMs installati nel corso degli anni

Il Bancomat Bitcoin funziona seguendo i seguenti passi:

a) **Registrazione**: ci si dovrà registrare al servizio, inserendo il proprio numero di cellulare e il codice che verrà inviato via sms dal sistema;

b) **Verifica identità:** si dovranno effettuare una scansione palmare, del proprio codice fiscale, della patente e una foto;

c) **Inserimento**

dell'indirizzo Bitcoin: si dovrà scansionare il Qr Code[43] associato al proprio wallet elettronico. Il wallet elettronico dovrà essere il medesimo verso il quale o dal quale si vorrà effettuare una transazione;

d) **Selezione dell'importo di denaro contante** che si vuole convertire in bitcoin. Se l'ATM è bidirezionale è possibile anche il procedimento inverso, ovvero la conversione dei bitcoin in valuta legale;

e) **Conferma:** stampa dello

scontrino di avvenuta operazione.

Tuttavia, il metodo più comune per ottenere bitcoin ed il primo utilizzato in assoluto è l'attività di mining, un'attività che viene svolta in rete da utenti definiti "miners", o semplicemente minatori. I minatori mettono a disposizione la potenza di calcolo del loro computer/hardware, con l'aiuto di un programma/software specifico, per svolgere dei complessi problemi crittografici, al fine di ricevere una ricompensa in bitcoin.

La rete ricompensa le attività di mining, al fine di incentivare i minatori a svolgere il proof-of-work richiesto,

mantenendo in questo modo l'integrità della Blockchain.

Andando avanti col tempo, queste attività di mining sono diventate sempre più complesse, perché i calcoli proposti (Proof-of-work) dal sistema hanno aumentato il loro grado di difficoltà, definito target, rendendo l'attività di mining poco redditizia.

I minatori, oltre al compito di produrre i bitcoin, hanno anche quello di confermare le transazioni effettuate dai vari fruitori del sistema.

Ma in cosa consiste la prova di lavoro fornita dal sistema?

La prova di lavoro, comunemente conosciuta con il termine Proof-of-

Work, consiste nella conversione di specifici dati offerti dal sistema in codici hash (vedi cap.2), che per essere validi devono coincidere e non superare il valore del target. Il target è un parametro essenziale che equivale al grado di difficoltà del proof-of-work, misurando la potenza di calcolo necessaria per la risoluzione di un problema di calcolo.

Esistono tre modi per svolgere l'attività di mining:

a) Minando in proprio (o solo-mining): acquistando degli hardware appositi, cioè che possiedono

un'elevata potenza di calcolo, in modo da riuscire a risolvere anche i problemi più complessi nel minor tempo possibile; questi tipi di hardware sono molto costosi.

b) Minando in comunità (o pool-mining): riunendosi in comunità e mettendo insieme la propria potenza di calcolo. Il profitto ricavato viene suddiviso in parti proporzionali alla potenza di calcolo offerta al sistema.

c) Minando in cloud (o cloud-mining): nel web vi

sono alcuni siti che mettono a disposizione dei computer, dotati di elevata potenza di calcolo ed in grado di minare. Questi computer, risiedono in server, che vengono messi in “affitto” dai siti cloud[44]. Lo scopo dei minatori è riuscire a risolvere problemi di calcolo nel minor tempo possibile, in maniera ripetitiva, e questo è possibile affittando parte della potenza di calcolo di un server, calcolata in GigaHash[45] (GH).

Navigando sul web, tuttavia, ci si rende conto che esistono un'infinità di modi

per guadagnare bitcoin gratis. Sono molti i siti che mostrano come guadagnare bitcoin gratis; uno di questi è proprio il sito www.guadagnarebitcoins.altervista.org.

Il sito, appena citato spiega che vi sono ad esempio siti e piattaforme online che permettono di guadagnare piccoli importi di bitcoin, in cambio di click e visite ai loro sponsor per un tempo prestabilito, altri in cambio di una semplice registrazione (sempre sulle piattaforme dei loro sponsor) o di un semplice download di applicazioni per smartphone. Si può guadagnare bitcoin gratis con:

a) **Faucet:** (detti anche "rubinetti") sono siti che pagano piccole frazioni di BTC per la risoluzione di captcha;

b) **Pay Per Action (PPA):** gli utenti vengono pagati per compiere una registrazione o un download;

c) **Pay Per Play (PPP):** gli utenti vengono pagati per giocare a giochi online;

d) **Paid To Click (PTC):** gli utenti vengono pagati per visitare sponsor[46] e fare il maggior numero di click.

1.6.3 Spendere i bitcoin

Nonostante vi siano ancora molti negozianti che non accettano pagamenti in bitcoin, un po' perché hanno timore di non saper rendicontare nel bilancio aziendale gli incassi in bitcoin, un po' perché fanno fatica a prendere confidenza con le nuove tecnologie emergenti, vi è comunque una crescita a livello di numero di aziende, negozianti, negozi fisici e virtuali che hanno aggiunto questa nuova e rivoluzionante forma di pagamento, accanto alle normali valute legali.

Oggigiorno, tra coloro che hanno deciso di adottare questa nuova forma di pagamento, troviamo anche piccoli commercianti che hanno iniziato ad accumulare criptovaluta con fini strategici, sperando in un futuro con valori molto alti.

E' l'esempio del famoso sito web statunitense di viaggi Expedia (www.expediainc.com/) che nel 2014 spiegò in una nota di aver preso accordi con la Coinbase[47], uno dei maggiori operatori della moneta virtuale, e di iniziare ad accettare i pagamenti in bitcoin solamente per prenotazioni riguardanti gli hotel. Expedia ha aggiunto, inoltre, che non svolgerà

attività commerciali trattando la moneta ricevuta in valuta virtuale ma la convertirà in valuta legale, come da accordi presi con la Coinbase.

Anche Microsoft Corporation[48], una delle più importanti aziende d'informatica al mondo, ha permesso l'acquisto di contenuti, quali applicazioni, giochi e video della sue piattaforme Windows, Windows Phone e Xbox in valuta digitale bitcoin.

Nella lista dei siti e piattaforme online che accettano pagamenti in bitcoin troviamo Wordpress, famosa piattaforma CMS (content management system) per la creazione di siti web e blog personali; Badoo, una famosa rete

sociale per incontri, conversazioni e chiamate in rete e molti altri.

Un buon punto di partenza per cercare un negozio che accetta bitcoin è il sito www.coinmap.org, un sito rappresentante una mappa con i negozi che accettano pagamenti in bitcoin. Il sito in questione si aggiorna continuamente, riportando in alto a destra il numero totale di attività commerciali nel mondo che accettano questa criptovaluta.

Secondo coinmap.org, al giorno d'oggi, in tutto il mondo sono 10.025 gli esercizi commerciali in cui ci si può recare ed acquistare beni o servizi in cambio di bitcoin (consultato il

03/10/2017).

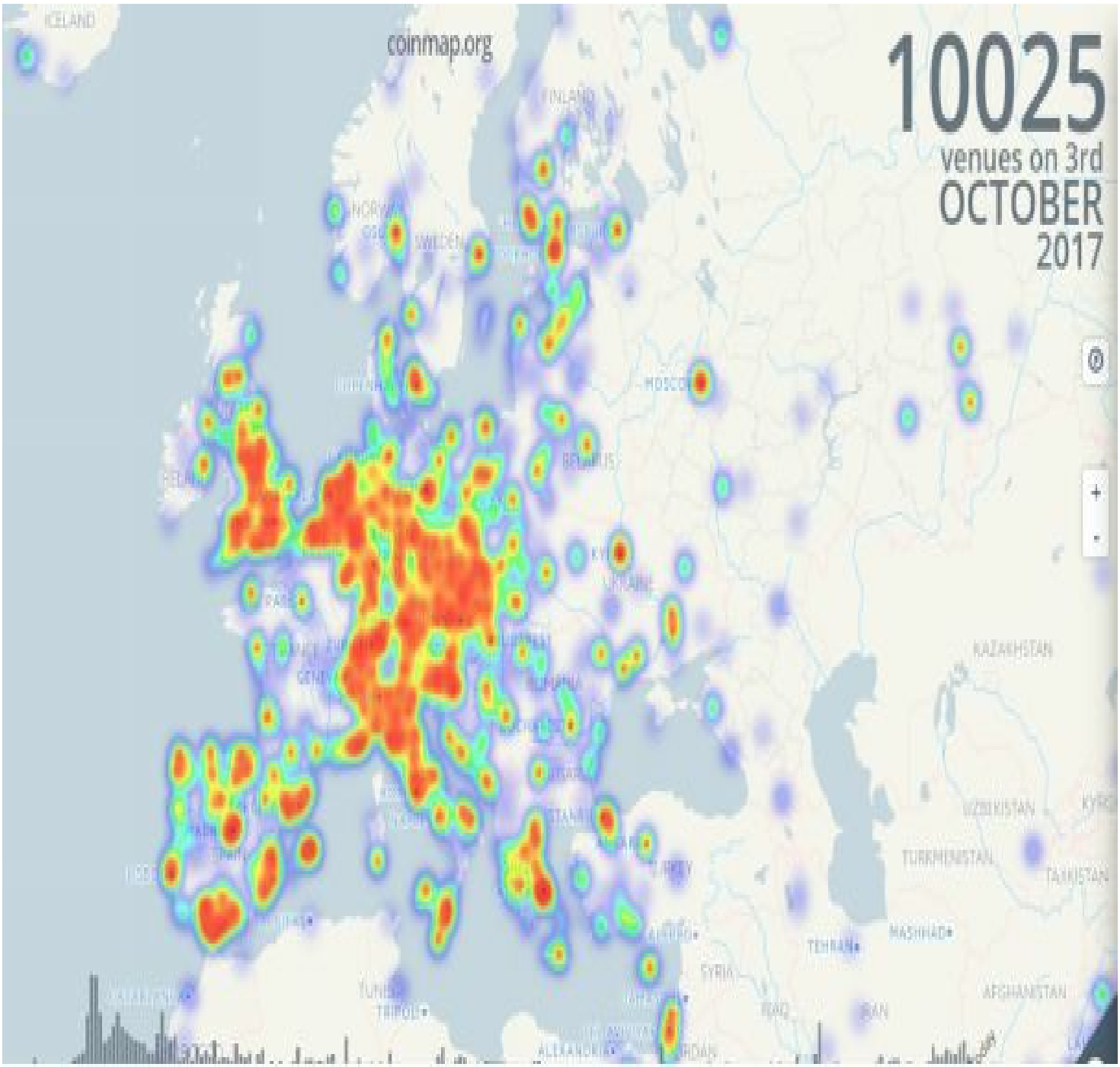


Figura n.10: Esercizi commerciali che accettano bitcoin nel mondo (fonte

coinmap.org)

Il sito coinmap.org permette anche la ricerca di una determinata via all'interno del suo database ed in più permette ad ogni utente di aggiungere e modificare la propria via, relativa alla propria attività commerciale in massima autonomia e indipendenza.

Per quanto riguarda i sistemi Android, una delle applicazioni più utilizzate per la ricerca di attività commerciali che accettano bitcoin è "Quibitcoin.it" (link al sito www.quibitcoin.it). Questa applicazione mostra gli ATM bitcoin più vicini, le attività commerciali bitcoin più vicine e filtra la ricerca per:

Vicino, Città, Categoria, Nome, Mappa, ATM e statistiche.

Il sito è ben strutturato e possiede una grafica semplice ed intuitiva, con un menu grafico a blocchi.

L'immagine seguente mostra la Homepage del sito www.quibitcoin.it.

Figura n.11: homepage del sito https://www.quibitcoin.it/

In Italia i siti che accettano i bitcoin sono riportati nel seguente sito: www.anycoindirect.eu/it/dove-spendere-bitcoin.

1.6.4 Le spese di commissione

Oggigiorno, possedere un conto corrente bancario implica delle commissioni e delle spese aggiuntive da pagare, ogni qualvolta ci si presta ad usufruire di un servizio offerto dalla Banca stessa. La maggior parte delle Banche di oggi prevedono una commissione di transazione, spesso una percentuale aggiuntiva al mittente del 5-10% circa dell'importo inviato. Chiaramente le

commissioni di transazione iniziano a diventare significative, nel momento in cui l'importo inviato è elevato.

In questo contesto, dove le spese per usufruire di servizi offerti sono in forte aumento, hanno ruolo importante i sistemi di pagamento decentralizzato, come ad esempio le criptovalute. Trasferire denaro in BTC, o un'altra criptovaluta, risulta essere un metodo alternativo valido, rapido ed economico rispetto ai sistemi di pagamento tradizionali. Bitcoin, infatti, è un sistema di pagamento molto economico, perché prevede dei costi di transazione bassi o quasi nulli. In Bitcoin il costo di commissione è invariato ed indipendente

dall'importo inviato; il pagamento di una tassa di commissione incentiva il lavoro svolto dai minatori e porta alla validazione della transazione in tempi brevi.

Analizzando e confrontando vari siti, si evince che le transazioni di bitcoin sono nettamente le più veloci ed economiche. La tabella seguente mostra, e mira ad evidenziare, le differenze di costo a livello di spese di commissioni di alcuni dei diversi sistemi di pagamento del mondo:

	WESTERN UNION FEE	PAYPAL FEE	PC

importi da 0,01€ a 50,00€	4,90 €	3,4% + 0,35 €	
Tempi di transazione	qualche minuto	qualche minuto	

Tabella n.1: costi di commissione nei sistemi di pagamento internazionali

Capitolo 2
Architettura e funzionamento della

rete Bitcoin

2.1 Introduzione

Questo capitolo esaminerà i processi di funzionamento della rete Bitcoin, presentandone dapprima l'architettura.

La rete Bitcoin è una rete paritaria, nella quale ciascun nodo svolge una duplice funzione: cliente/servente.

Le transazioni avvengono tra nodi paritari della rete e sono registrate all'interno di una sorta di "rubrica telefonica", chiamata Blockchain (catena dei blocchi). All'interno di questa

catena di blocchi, vi sono vari blocchi, all'interno dei quali sono registrate le transazioni della rete. La blockchain rappresenta l'organo innovativo e importante dell'intera rete.

I primi paragrafi sono volti alla definizione ed alla descrizione dei vari concetti e termini, propedeutici per la comprensione del funzionamento del sistema Bitcoin.

2.2 Chiavi private, pubbliche e indirizzi

Nella rete Bitcoin per poter inviare transazioni in valuta virtuale, bisogna

possedere una coppia di chiavi: chiave privata e chiave pubblica.

La chiave privata è una stringa di 256 bit integer, generata casualmente, che appone una firma digitale al messaggio in uscita. La chiave privata, in quanto segreta, deve essere conservata al sicuro e non deve essere persa, in quanto la sua perdita provocherebbe la perdita totale ed irreversibile di tutti i bitcoin presenti nel portafoglio elettronico.

La chiave privata può essere conservata in supporti cartacei, definiti paper wallet (vedi cap.1) o conservata online in software sicuri, che ne garantiscono la custodia.

Ad ogni chiave privata è associata una

chiave pubblica, che permette di verificare il messaggio in uscita e validarlo. La chiave pubblica deriva dalla chiave privata, ma non è un processo bidirezionale, ovvero una chiave privata non può derivare da una chiave pubblica.

La chiave pubblica è anch'essa un codice alfanumerico di 256 bit integer, generato da un particolare algoritmo, il ECDSA[49] (Elliptic Curve Digital Signature Algorithm).

Nella figura seguente vi è un'illustrazione grafica del processo di firma digitale apposta dalla chiave privata e validazione del messaggio da parte della chiave pubblica.

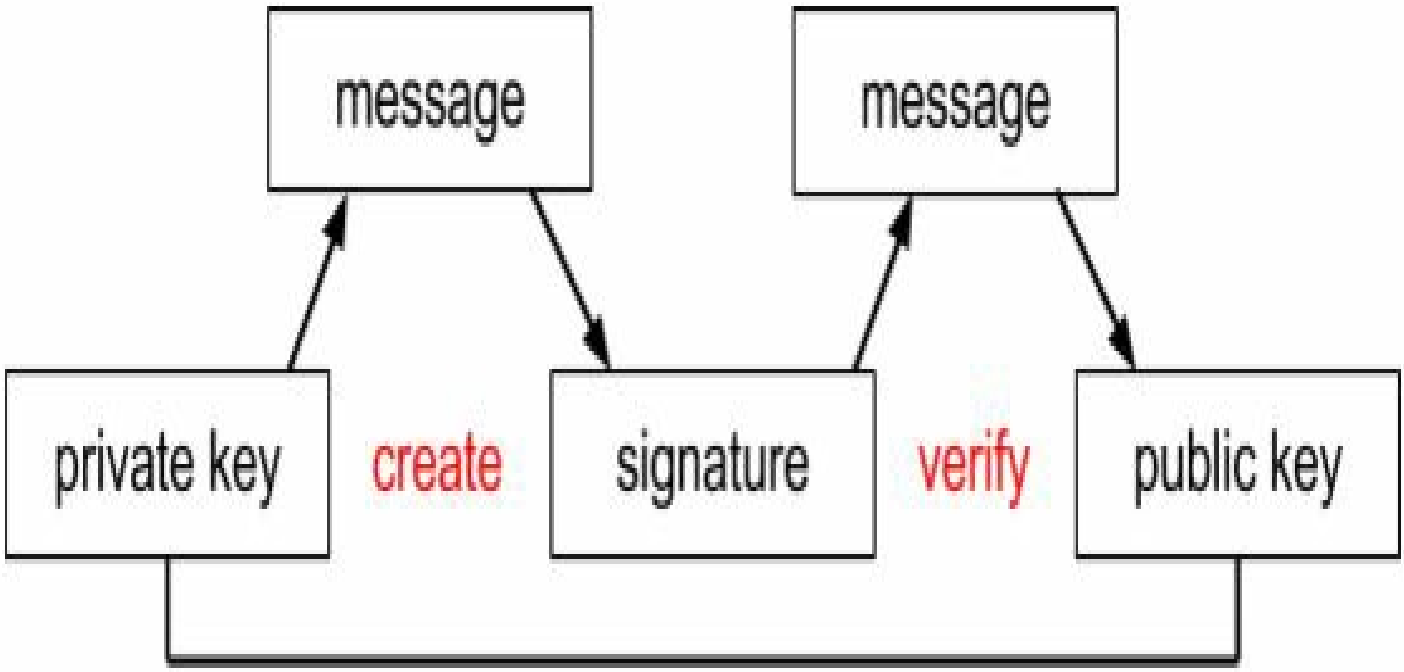


Figura n.12: ruolo delle chiavi private e pubbliche

Infine, dalla chiave pubblica viene creato l'indirizzo bitcoin, il cosiddetto address bitcoin[50], un identificatore di 26-35 caratteri alfanumerici, inizianti

con il numero 1 o il numero 3, e rappresenta l'indirizzo destinatario di un pagamento in bitcoin. E' possibile generare un indirizzo bitcoin, semplicemente cliccando su "New Address", dal software Bitcoin Core (presente il download su https://bitcoin.org/it/scarica) oppure accedendo direttamente da una piattaforma online con servizi legali alla criptovaluta.

2.3 La rete peer-to-peer

Come anticipato nell'introduzione, la rete Bitcoin è una rete paritaria (o paritetica), nella quale tutti i nodi risiedono nello stesso livello e svolgono la stessa funzione, ovvero quella di inviare richieste ad altri nodi della rete (svolgendo la funzione di client) e quella di ricevere richieste da altri nodi della rete (svolgendo la funzione di server). Non vi è dunque una gerarchia client/server, architettura presente per esempio nella rete web dove i vari dispositivi hardware connessi alla rete, svolgono funzione di client, ovvero di

fare la richiesta al server, il quale elabora la richiesta e fornisce una risposta, quale la pagina web di navigazione.

La natura paritaria dei nodi della rete Bitcoin, e dunque l'assenza di un server centrale che controlli la rete e le transazioni, confermano la natura decentralizzata del network, all'interno del quale tutti i nodi sono tra loro equivalenti.

La seguente figura mostra la composizione di un'architettura di rete peer-to-peer.

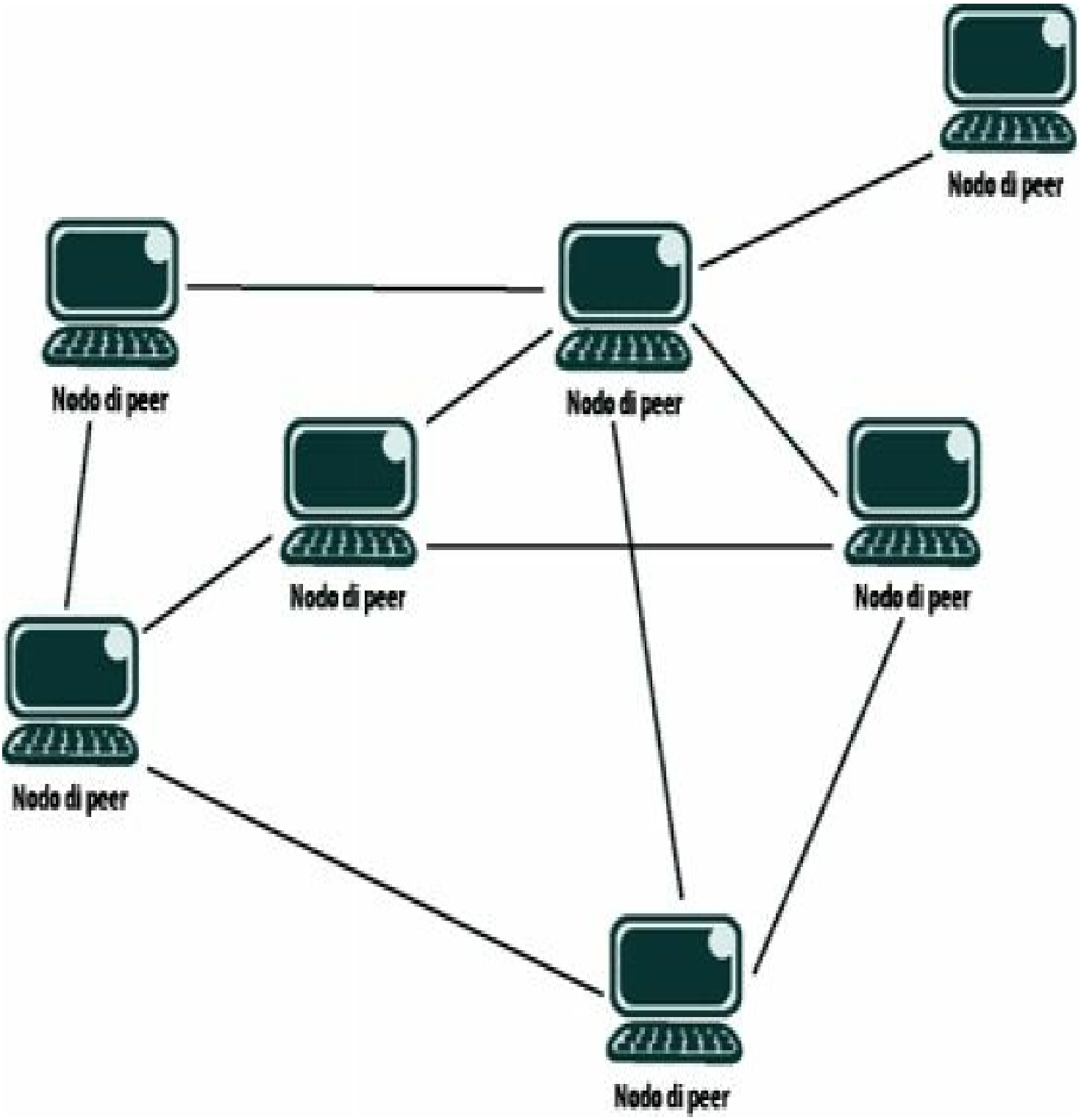


Figura n.13: esempio di architettura peer-to-peer

Ogni nodo, facente parte della rete Bitcoin, al momento della ricezione delle transazioni, le raggruppa all'interno di un unico blocco, a cui assegna una prova di lavoro (proof-of-work) da svolgere e risolvere. Questa prova di lavoro viene trasmessa a tutti i nodi della rete; quest'ultimi accettano il blocco solo se le transazioni in esso contenute sono state validate.

Una volta validato il blocco, ri-inizia il processo passando al blocco successivo della catena.

2.4 La Blockchain

La Blockchain, letteralmente catena di blocchi, è un sistema formato da blocchi collegati tra loro. All'interno di ogni blocco, vi sono le transazioni validate ed accettate dai nodi, che in questo ambiente svolgono la funzione di controllo, validazione e approvazione della correttezza di una determinata transazione, inserendola all'interno del blocco.

La Blockchain è definita anche come una

sorta di “rubrica telefonica”, perchè è pubblica e ciascun utente può vedere i blocchi e le transazioni in esso contenute. Il blocco, e di conseguenza anche le transazioni in esso contenute, una volta approvate dai nodi della rete, diventano immutabili ed immodificabili ed è questa la motivazione per la quale la Blockchain è considerata un sistema innovativo.

Tuttavia, bisogna aggiungere che nonostante la Blockchain sia aperta al pubblico e nonostante le transazioni siano consultabili da chiunque, vige un

rigido sistema di sicurezza che rende quasi impossibile risalire all'identità madre di colui che ha effettuato la transazione.

Le transazioni sono rappresentate da codici alfanumerici (bitcoin address), associati ad una chiave pubblica, associata a sua volta ad una chiave privata, appartenente solo ed esclusivamente al proprietario.

La figura seguente illustra metaforicamente una raffigurazione della catena di blocchi. Ciascun "gancio", rappresenta un blocco, all'interno del

quale vi sono le transazioni, rappresentate da codici alfanumerici univoci, bitcoin address.

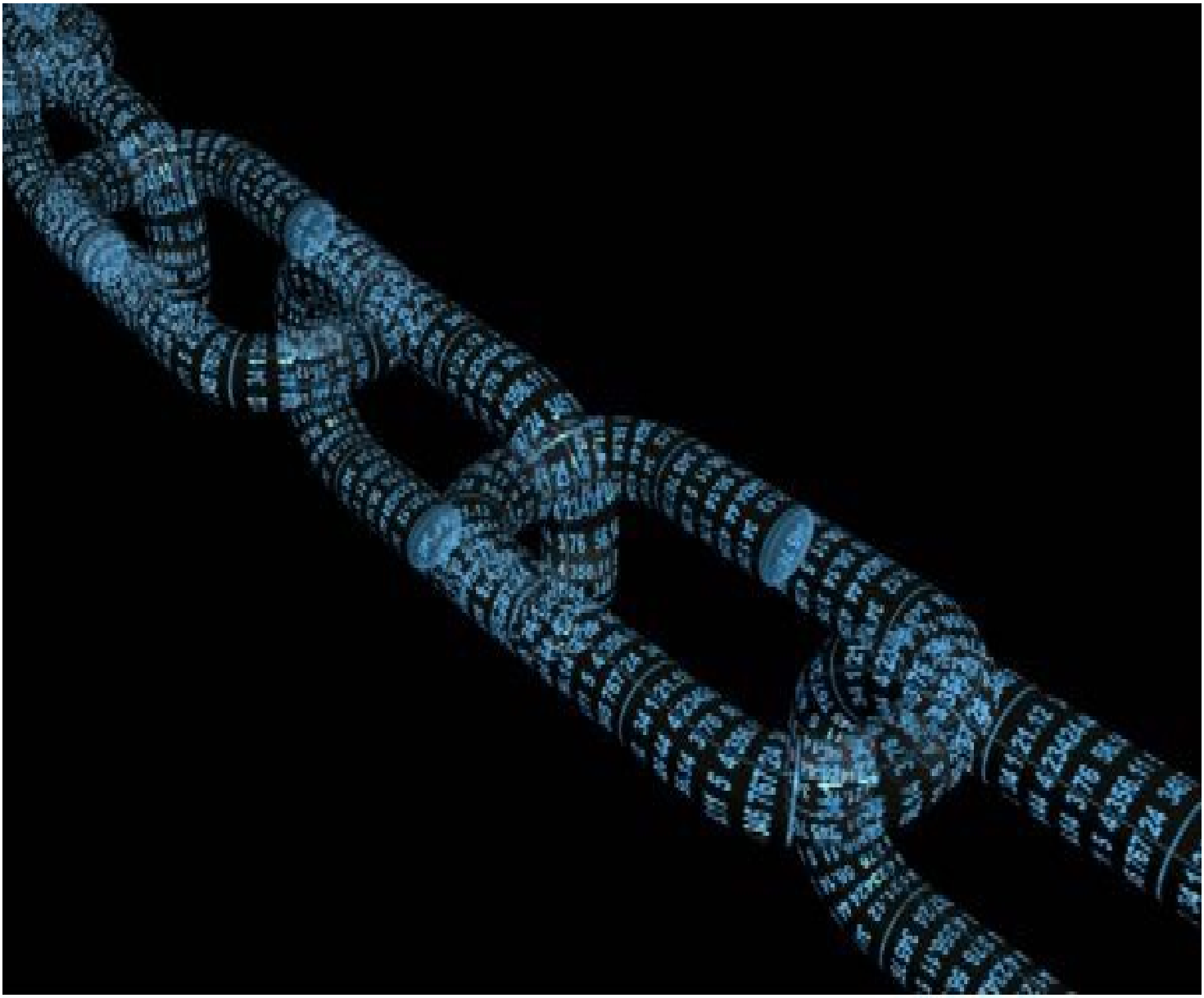


Figura n.14: esempio di blockchain

2.4.1 La struttura dei blocchi

Come si evince dal sito seguente www.blockexplorer.com, in Bitcoin tutto è registrato e aperto a chiunque. Tutte le transazioni avvenute dal 2009, dal Genesis Block (Blocco 0) ad oggi, sono registrate e presenti all'interno della Blockchain. Ogni blocco, come anticipato in precedenza, contiene le informazioni relative al blocco precedente, le transazioni eseguite e validate dai nodi ed altre informazioni che andremo a vedere meglio nel

presente paragrafo.

Nel sito www.blockexplorer.com, accedendo alla sezione “Latest Blocks”, è possibile consultare la lista di tutti blocchi della Blockchain, risalendo anche al blocco più remoto attraverso l’apposito link “See all blocks”.

Nell’anteprima di ogni blocco, sono specificate le seguenti informazioni: Height, Age, Transactions, Mined by e Size, come mostrato nella figura sottostante:

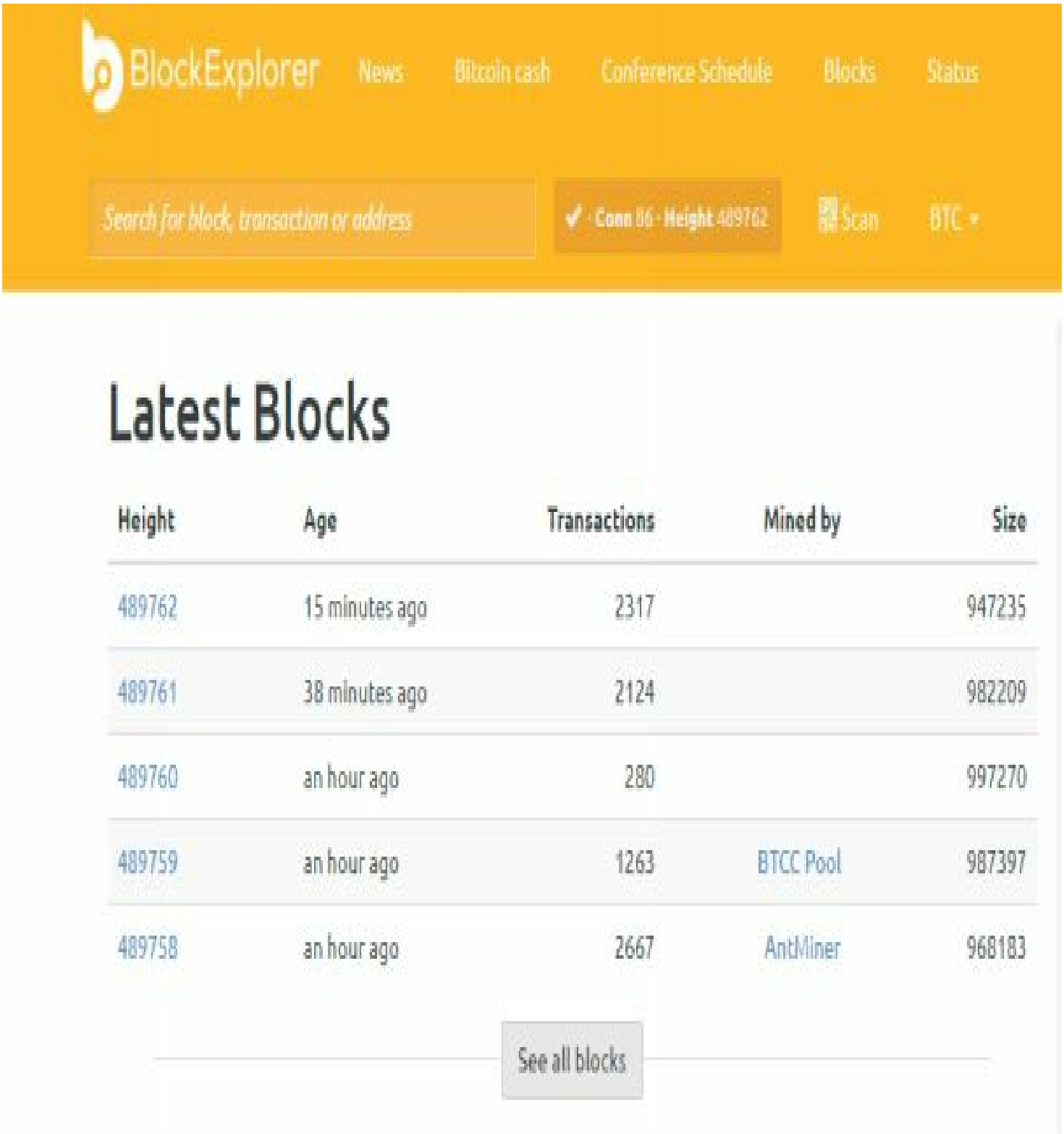


Figura n.15: schermata mostrante i diversi blocchi all'interno della

blockchain (consultato il 14/10/2017)

La voce “Height” mostra il numero progressivo di blocchi creati, dove il numero più grande equivale all’ultimo blocco creato nel tempo, ovvero al blocco più recente.

La voce “Age” indica quanti minuti, in direzione anti-oraria dall’ora attuale è stato creato quel determinato blocco.

La voce “Transactions” indica il numero di transazioni presenti nel blocco.

La voce “Mined by” indica il minatore che ha minato il blocco. Per esempio, in riferimento alla figura n. 15, il minatore

del blocco numero 489759 è la mining-pool BTCC https://pool.btcchina.com/.
La voce “Size” indica la memoria occupata dai dati di tutte le transazioni del blocco.

Tuttavia, cliccando su un preciso blocco ed accedendo all’interno di esso, possiamo consultare ulteriori informazioni relative ad esso. Per esempio, se clicchiamo sull’ultimo blocco della lista, il blocco numero 489762, ci apparirà la seguente schermata:

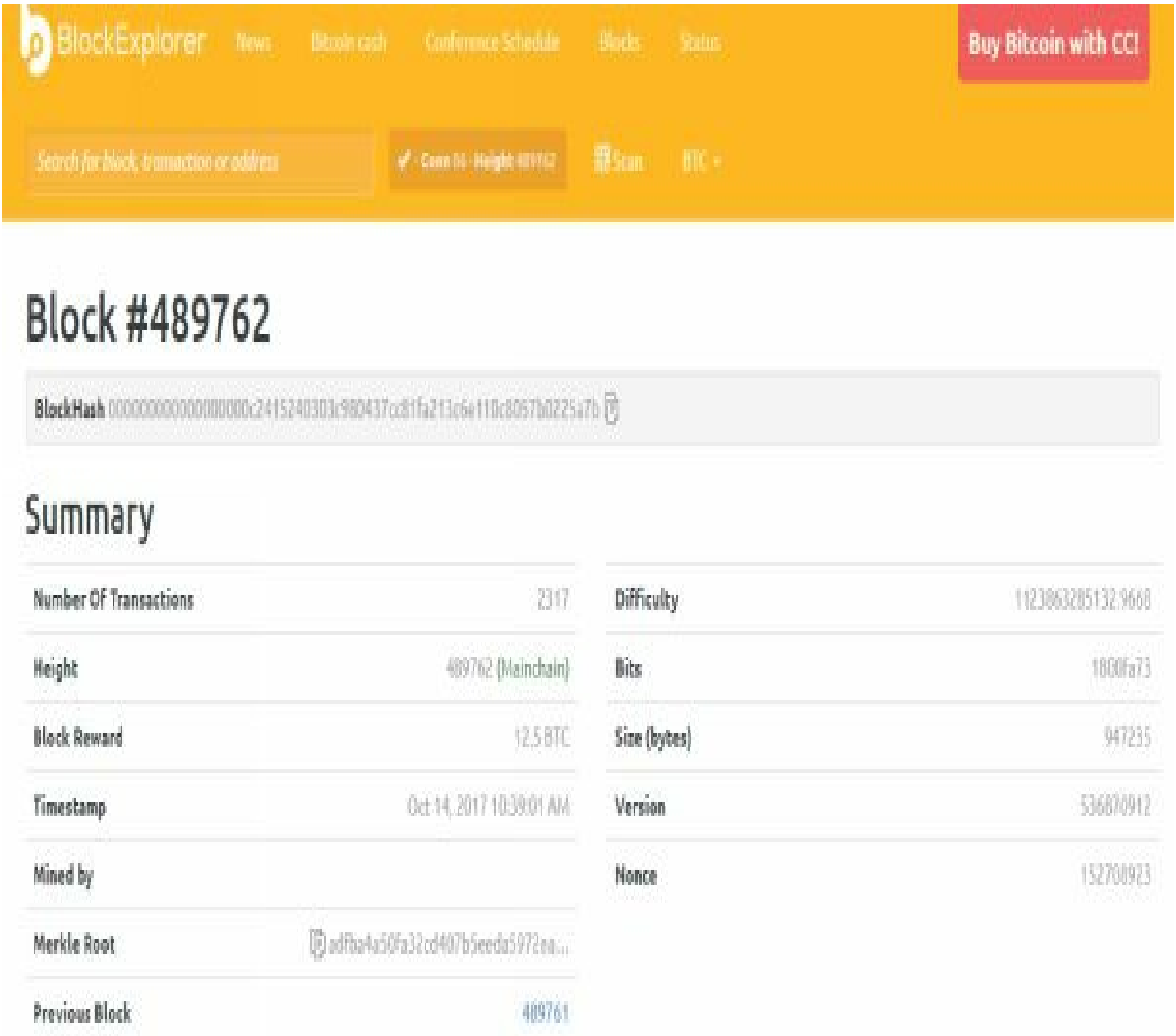


Figura n. 16: informazioni relative ad un blocco

Come si evince dall'immagine

soprastante, oltre alle informazioni indicate nell'anteprima dei blocchi, all'interno del blocco vengono indicate ulteriori informazioni: Block Reward, Timestamp, Merkle Root, Previous Block, Difficulty, Bits, Version e Nonce.
La voce "Block Rewards" indica il valore in bitcoin scambiato nelle transazioni del blocco.
La voce "Timestamp" indica la data e l'ora precisa in cui il blocco è stato risolto.

La voce "Merkle Root"[51] indica un codice alfanumerico, definito codice

Hash, che sintetizza tutte le informazioni riguardanti le transazioni comprese nel blocco.

La voce “Previous Block” indica il numero “Height” del blocco precedente. Come si può notare è indicato tramite un link, collegato al blocco precedente, al fine di poter visionare anche le informazioni riguardanti quest’ultimo.

La voce “Difficulty” indica il grado di difficoltà nella risoluzione del blocco ed è indicato con il termine “target”. La difficoltà è misurata calcolando il tempo di elaborazione necessario a risolvere

un determinato proof-of-work (prova di lavoro).

La voce “ Bits” indica l’unità di misura delle informazioni presenti nel blocco.

La voce “Version” indica il numero della versione del blocco. Per esempio la prima versione rilasciata da Bitcoin fu Bitcoin v0.

La voce “Nonce”, sta ad indicare un numero/campo utilizzato solo una volta (Number Used Once). Il Nonce è un numero casuale, utilizzato solo una volta nei protocolli di autenticazione ed assicura che i dati utilizzati nelle

transazioni precedenti non possano essere riutilizzati.

Oltre alle informazioni sopra indicate, all'interno del blocco, nella voce "Transactions" sono indicate anche le diverse transazioni in esso contenute, nella seguente composizione:

Previous Block 409761

Transactions

08ec1f4454d360f1067491533a6cabf0f1e72711b52b1dfab8eeb4e537a796cf4 mined Oct 14, 2017 10:39:01 AM

No Inputs (Newly Generated Coins)

1KfhE7w68haEthAswwryaoccDb6qcT6DbYY 15.28708758 BTC (U)

Unparsed address [0] 0 BTC (U)

1 CONFIRMATIONS 15.28708758 BTC

57248301 3bf27ac89d05d5beb8d36b598ac1a8501492fe0bcca8b2248fa41a54 mined Oct 14, 2017 10:39:01 AM

1RwW8UHma378n83znaQTXWBV3uf2nCGdu 1.446648 BTC

1NQPtUUV7MaVCkVwEbjL2UULYHTmkkKi7 1.410656 BTC (U)

1AecgtHedfA2gvXH6GiKLS2JGkfWfgyTC6 0.005 BTC (S)

FEE: 0.030992 BTC

1 CONFIRMATIONS 1.410656 BTC

03feb4a4702baf0918498bcff4dea9e61d0a829d3981896861804b916897e2e9 mined Oct 14, 2017 10:39:01 AM

13Dc4JosUWPE98BCbDtd64qx4ZwTiRzT3E3 0.06 BTC

1HgLwjYuHwSHwVdJzdrxmzqwFyeGuVj7K8 0.024056 BTC (S)

1AecgtHedfA2gvXH6GiKLS2JGkfWfgyTC6 0.005 BTC (S)

FEE: 0.030944 BTC

1 CONFIRMATIONS 0.029056 BTC

4ca1a7eb37c119c109b41ee620f4f138ca39a55293fc6301283dc5bd849d04f2 mined Oct 14, 2017 10:39:01 AM

Figura n.17: storico di tutte le transazioni, all'interno di un blocco.

La prima transazione di un blocco è definita "coinbase".
E' la coinbase che valida e ricomprende le transazioni successive dello stesso blocco, e perciò contiene la ricompensa dovuta al minatore che ha risolto il blocco.
La coinbase differisce dalle altre transazioni dello stesso blocco, poiché è priva di input; infatti nella rappresentazione della coinbase, nel

campo “input” appare sempre la scritta “No Inputs: Newly Generated Coins”.
Come si può vedere dalla figura n.17, per ogni transazione del blocco sono indicati il relativo valore di hash, gli inputs, gli outputs, il numero di conferme ottenute e il numero di bitcoin trasferiti.

2.4.2 La struttura delle transazioni

Satoshi Nakamoto, nel secondo paragrafo “Transactions” del trattato “Bitcoin: a peer-to-peer electronic cash

system", definisce il concetto di moneta elettronica come "una catena di firme digitali". Ogni utente della rete Bitcoin trasferisce la moneta elettronica all'utente successivo, apponendo una firma digitale sul codice hash della transazione precedente e sulla chiave pubblica dell'utente destinatario e aggiunge queste due informazioni alla fine della propria moneta. L'utente destinatario può verificare questi passaggi, ovvero le firme per verificare la catena di proprietà.

La seguente immagine, illustra i passaggi

di firme digitali che avvengono nelle transazioni di Bitcoin:

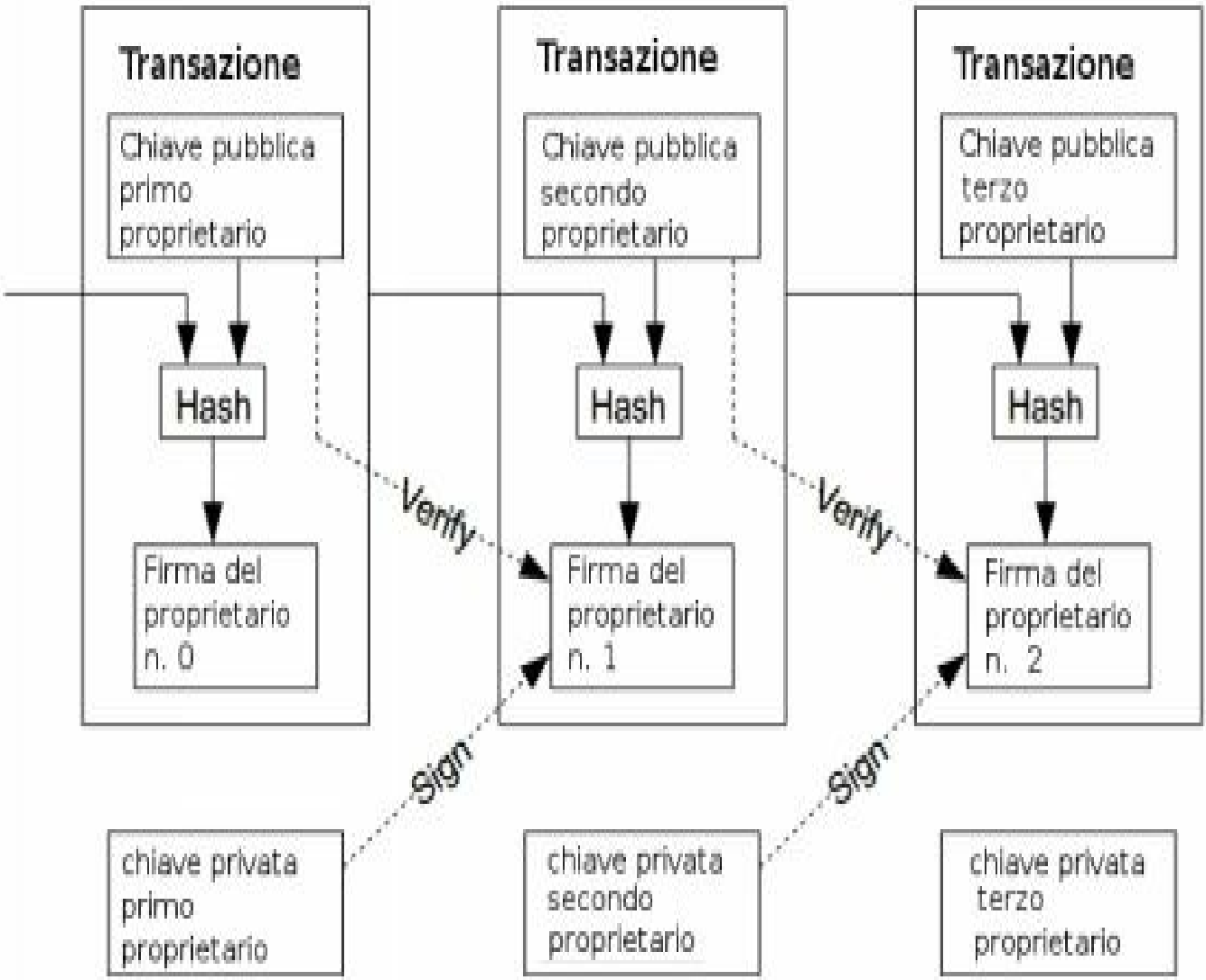


Figura n.18: transazioni di bitcoin (immagine fornita da Satoshi Nakamoto nel suo trattato)

L’utente destinatario, avendo accesso alla verifica della catena di proprietà, ha la prova che per la maggioranza dei nodi, e per l’esattezza da almeno il 51% di essi, la sequenza ricevuta è la sequenza cronologica valida.
L’utente, dunque, può verificare il pagamento di una transazione, disponendo di:

- intestazione del blocco della catena di proof-of-work più lunga (se non si dispone di essa, possono essere interrogati i nodi della rete

finché non si è sicuri di possedere la catena più lunga);

- ramo del Merkle Tree che collega la transazione al blocco, contenente la transazione da verificare.

Tuttavia, l'utente non può controllare la transazione da solo, ma collegandola ad un punto della catena, può verificare se vi sono stati aggiunti blocchi successivi al blocco che la contiene; se vi sono blocchi successivi vorrà dire che la transazione è stata verificata e validata.
Per ovviare al problema del double-

spending[52], in mancanza di un soggetto terzo che controlla l'emissione della moneta, questo sistema di pagamento elettronico in rete ha attivato la partecipazione attiva di tutti i nodi della rete; le transazioni devono essere dichiarate pubblicamente ed, affinché le transazioni siano valide, devono avere il consenso del 51% dei partecipanti della rete su un'unica sequenza cronologica.

Chiunque potrà vedere che qualcuno sta inviando una somma di denaro a qualcun'altro, ma senza informazioni che colleghino la transazione ad un utente

fisico.

Per fare un esempio, consideriamo che l'utente, che trasferisce denaro, sia uno studente immatricolato all'Università; ogni studente immatricolato all'Università possiede un codice che lo identifica, ovvero il numero di matricola.

Molto metaforicamente, possiamo pensare all'indirizzo bitcoin di una transazione come un numero di matricola, che cela l'identità del proprietario dietro un codice.

Nel sito www.blockexplorer.com è possibile accedere, tramite l'area "Latest Transactions", alla lista delle ultime transazioni.

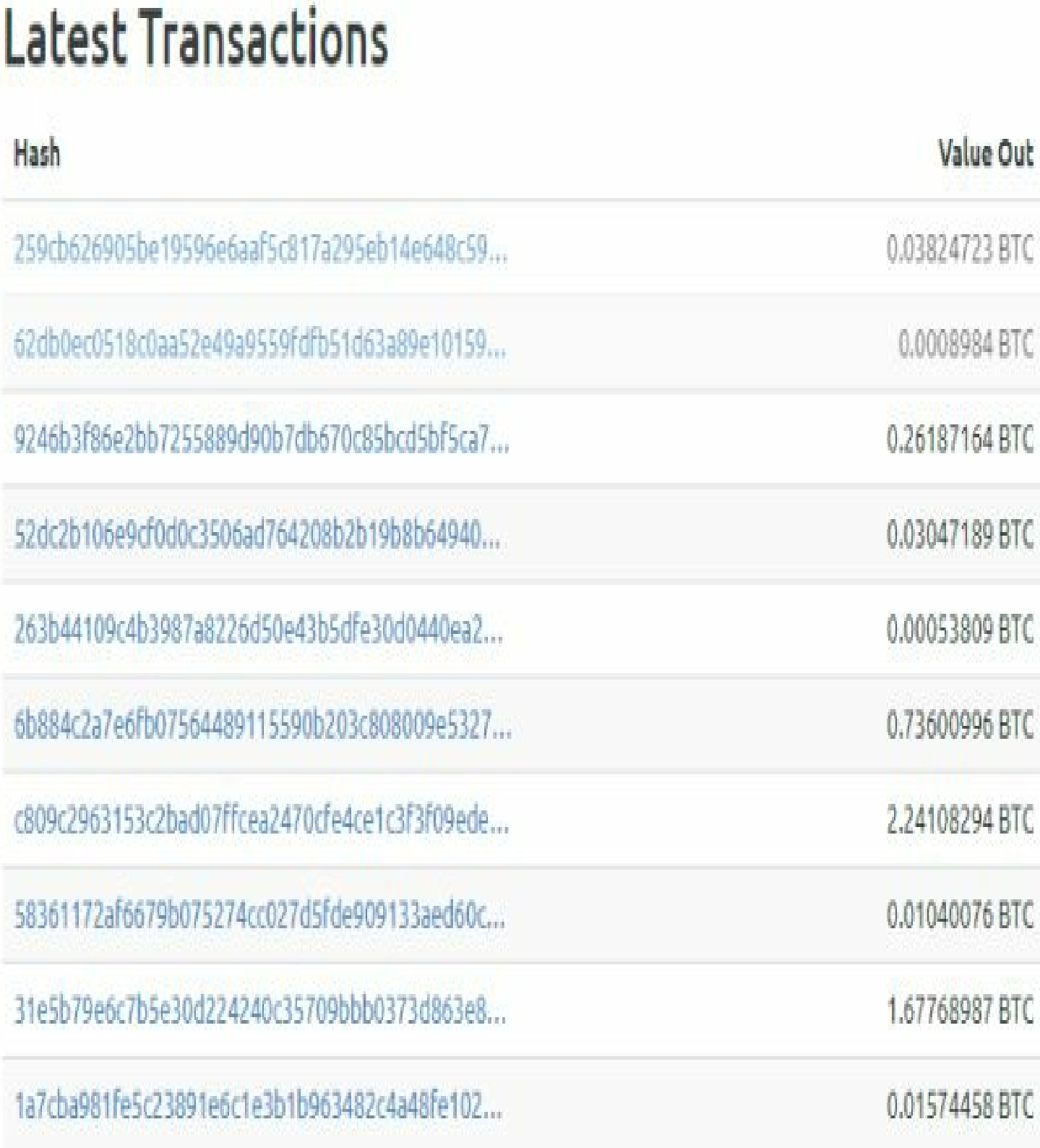


Figura n.19: lista delle transazioni della Blockchain

Nella schermata di anteprima, le transazioni sono rappresentate tramite un codice alfanumerico univoco, il Bitcoin address, ad ognuno dei quali corrisponde il valore “Value Out”.
Nel valore Value Out è indicato il valore di bitcoin in uscita.
Cliccando su un Bitcoin address casuale, si viene indirizzati all’interno della transazione stessa, della quale sono mostrate le seguenti informazioni:

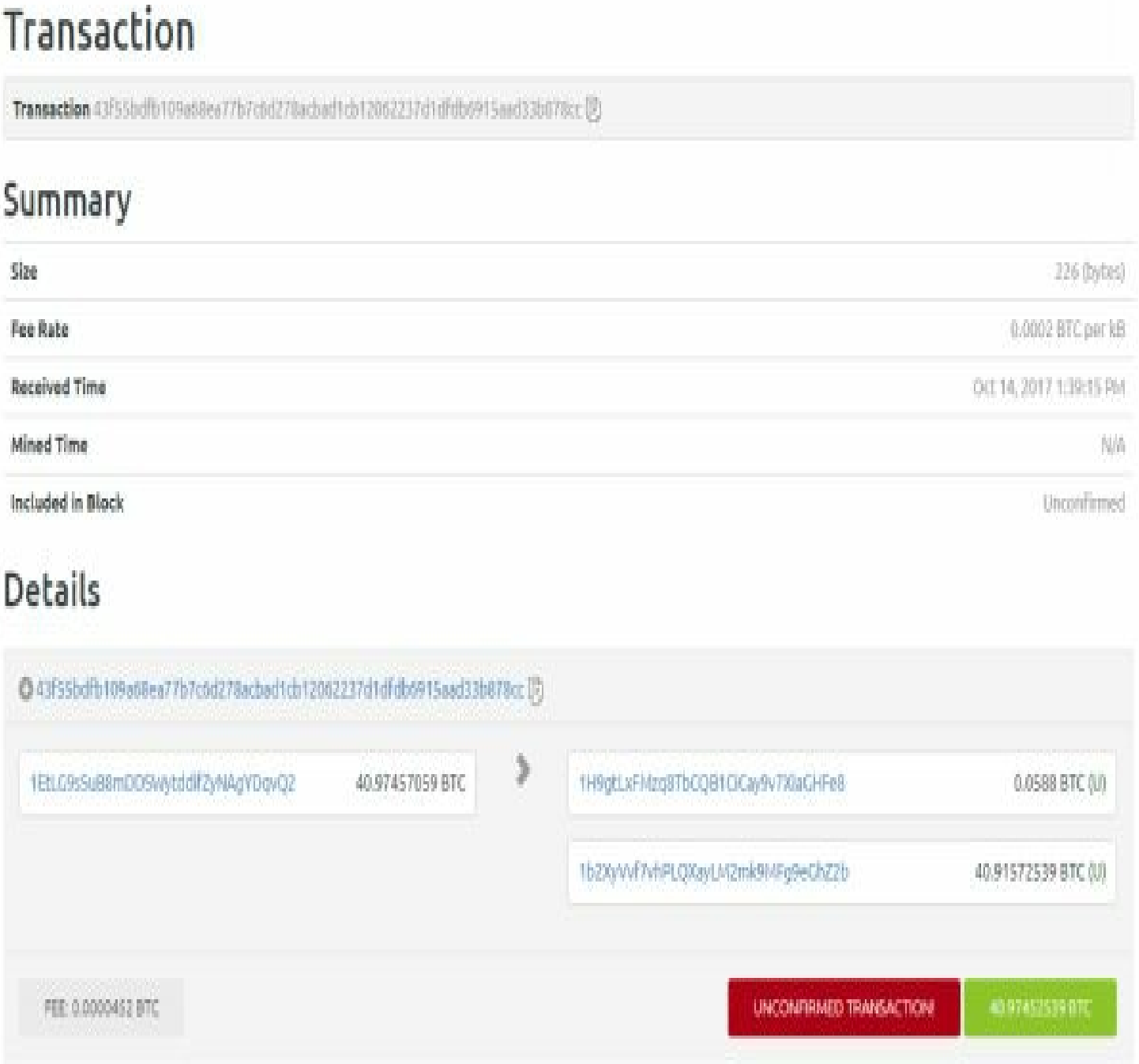


Figura n.20: schermata rappresentante una transazione

Le informazioni relative ad una determinata transazione sono suddivise in tre aree:

- **Transaction:** indica l'indirizzo bitcoin relativo alla transazione in oggetto;
- **Summary:** sintetizza le seguenti informazioni:
  1. Size: misura di memoria dei dati della transazione in termini di spazio occupato sul disco;
  2. Fee Rate: ammontare della commissione di transazione

attribuita al miner;

3. Received Time: data e ora della ricezione della presente transazione;
4. Mined Time: tempo speso nell'attività di mining;
5. Included in Block: numero del blocco in cui la transazione è memorizzata.

- **Details:** in questo campo si ha una panoramica delle transazioni in entrata, in uscita, delle conferme ricevute, del totale delle commissioni e del totale dei bitcoin

inviati all'utente destinatario. La figura n.20 mostra una transazione ancora non verificata e approvata dai nodi della rete con stato della transazione "unconfirmed transaction".

2.5 Funzionamento della rete Bitcoin

Come si evince dai paragrafi precedenti, la rete Bitcoin possiede un enorme

database distribuito tra i nodi della rete, che ne gestiscono il flusso di informazioni e le approvano. Questo database è chiamato blockchain, letteralmente catena di blocchi, nel quale vi sono registrate tutte le transazioni dal 2009 ad oggi, ovvero dalla nascita della rete Bitcoin ad oggi.

La tecnologia alla base di questa rete risiede nella sua natura crittografica.

In questo paragrafo si propone una spiegazione del funzionamento della rete Bitcoin, introducendo e spiegando il concetto principale di crittografia.

2.5.1 La crittografia

La crittografia (dal greco kryptòs graphìa letteralmente "scrittura nascosta") è la scienza che studia come cifrare e decifrare le informazioni. Questa scienza ha radici remote ed il suo utilizzo risale ai tempi dell'Antica Roma di Giulio Cesare.

Si parla del "Cifrario di Cesare", un metodo di cifratura utilizzato da Giulio Cesare, che consisteva nel sostituire in un testo ciascuna lettera con la lettera a

tre posizioni dopo nell'alfabeto. Questo metodo di cifratura non garantiva la segretezza delle informazioni, in quanto era possibile risalire al messaggio originale, utilizzando il metodo inverso e decifrando in questo modo il messaggio.

Nei sistemi informatici la crittografia è considerata un'innovazione che potrebbe portare importanti cambiamenti nello scambio e nella gestione delle informazioni online.

Lo scopo principale della crittografia è il mantenimento della segretezza dei

dati, assicurandone l'autenticità, l'integrità e la non ripudiabilità. Nella rete Bitcoin è fondamentale conoscere l'autenticità di un input, l'integrità delle transazioni, le quali non debbono subire alcuna modifica ed infine la non ripudiabilità dell'output.

Ne "Il manuale della crittografia. Applicazioni pratiche dei protocolli crittografici" dei due scrittori e crittografi Ferguson e Scheiner, si legge "*non esiste alcun modo noto per testare se un sistema crittografico è sicuro*".

Tuttavia, sappiamo con certezza, come

si legge in “Crittografia. Tecniche di protezione dei dati riservati” di Sgarro, che *“la sicurezza offerta da un sistema crittografico è affidata esclusivamente alla segretezza della chiave”*.

Infatti, nella rete Bitcoin la chiave privata è strettamente legata all’identità della persona che la possiede ed è la sola che permette di effettuare transazioni di bitcoin.

Il sistema crittografico è la base della rete Bitcoin, in cui tutte le informazioni sono occultate e cifrate da codici alfanumerici, definiti Hash.

2.5.1.1 Le funzioni Hash

Il valore di Hash è un valore, o codice univoco alfanumerico, di lunghezza fissa che indica ed identifica un input di testo. Dato un input di testo, propriamente detto “messaggio di testo” di qualsiasi lunghezza, è possibile ricavare da esso e calcolare il valore di Hash, propriamente detto “messaggio digest”, utilizzando specifici algoritmi per la conversione.

Gli algoritmi per la conversione più

comuni sono i seguenti: MD5 Hash, SHA1 Hash, SHA256 Hash, SHA384 Hash, SHA512 Hash e RIPE MD160 Hash.

Il sito www.convertstring.com/it/Hash pemette la conversione online di qualsiasi stringa di testo, in codice Hash, proponendo per la codifica diversi algoritmi.

Facendo un esempio, la stringa di testo “messaggio di prova” restituisce il seguente valore Hash, codificato con algoritmo MD5 Hash: F80F5016E59A05FAA85CAC2B32024

La seguente immagine mostra quanto appena descritto:

MD5 Hash

▸ Opzioni di ingresso

Incollare il testo da MD5 hash qui:

messaggio di prova

Generare MD5 Hash!

Copia il messaggio MD5 digest da qui.

F80F5016E59A05FAA85CAC2B32024A01-

Figura n.21: esempio di conversione in valore Hash di un messaggio di testo.

Il valore di Hash, o messaggio digest, identifica ed è strettamente legato al messaggio di testo dato in input. La sola modifica di un carattere nel messaggio di testo di input, comporterebbe il totale cambiamento del messaggio digest di output; due input diversi non potranno mai avere lo stesso valore di Hash, o messaggio digest.

La conversione da "messaggio di testo" a "messaggio digest" è un'operazione

unidirezionale: è possibile conoscere il "messaggio digest" di qualsiasi "messaggio di testo", ma è quasi impossibile conoscere il "messaggio di testo" di un "messaggio digest".

2.5.1.2 Crittografia asimmetrica

La crittografia asimmetrica, definita anche crittografia a chiave pubblica o crittografia a coppia di chiavi o crittografia a chiave pubblica/privata, si basa sull'utilizzo di entrambe le chiavi

(le keypair, ovvero chiave pubblica e chiave privata) nell'invio di un messaggio cifrato o una transazione. E' necessario conoscere la chiave pubblica dell'utente destinatario, per potergli inviare un messaggio cifrato, ovvero un messaggio digest.

L'utente destinatario utilizzerà la propria chiave privata per la decodifica del messaggio ricevuto.

L'immagine seguente illustra il meccanismo di cifratura/decifratura appena descritto:

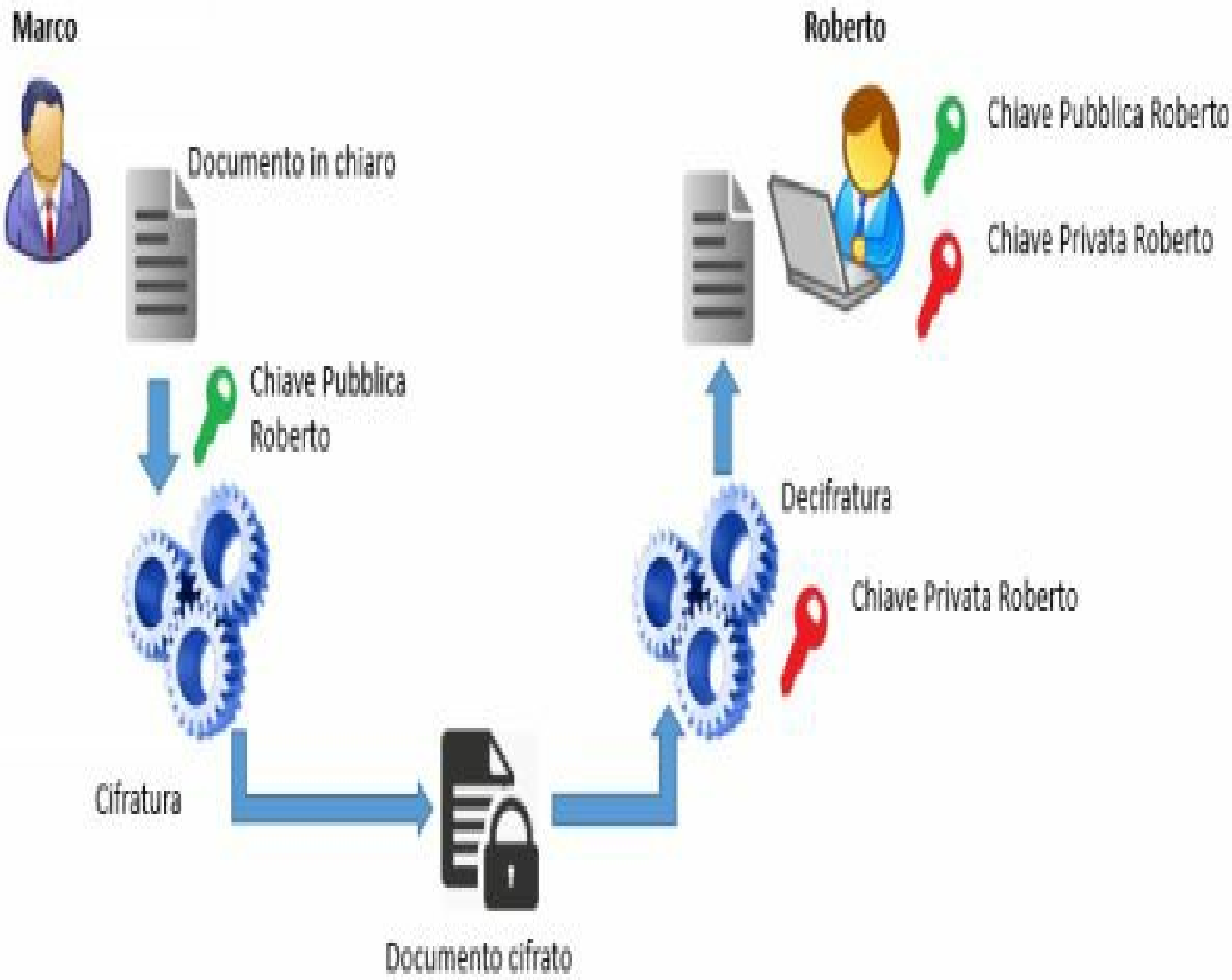


Figura n.22: illustrazione del funzionamento della crittografia asimmetrica, a chiave pubblica

Facendo riferimento alla figura n.22, Roberto è il destinatario del messaggio cifrato e possiede due chiavi: chiave pubblica (rappresentata in verde) e chiave privata (rappresentata in rosso). Marco è il mittente del messaggio di testo, e per cifrare il messaggio utilizza la chiave pubblica di Roberto.
Roberto riceve il messaggio cifrato, inviatogli da Marco, e per accedere alle informazioni in esso contenute e procedere alla decifrazione del messaggio, utilizza la propria chiave privata.

Questo è il meccanismo di crittografia asimmetrica.

Dunque, gli algoritmi di cifratura a chiave pubblica richiedono l'utilizzo della chiave pubblica per cifrare il messaggio e l'utilizzo della chiave privata per decifrare il messaggio ed a differenza degli algoritmi a chiave privata, non richiedono alcun utilizzo di un canale sicuro per lo scambio iniziale di una o più chiavi utili per la codifica/decodifica. In questo meccanismo, chiunque può cifrare un messaggio utilizzando la chiave

pubblica di un utente destinatario, ma solamente il possesso della chiave privata, associata alla chiave pubblica del destinatario, può decodificarlo. Questo sistema di crittografia garantisce alti livelli di sicurezza in quanto è quasi impossibile risalire alla chiave privata, partendo dal possesso di una chiave pubblica.

Gli algoritmi di firma a chiave pubblica sono RSA o DSA[53] (Digital Signature Algorithm).

2.5.1.3 Crittografia simmetrica

La crittografia simmetrica, propriamente definita crittografia a chiave privata, ha origini remote e risale ai tempi di Giulio Cesare, il quale era solito utilizzare cifrari per occultare testi di sua proprietà. La crittografia simmetrica è una tecnica di cifratura che consiste nel cifrare un messaggio di testo, utilizzando diversi algoritmi di cifratura, i cosiddetti cifrari. Il destinatario potrà accedere alla decifratura del messaggio soltanto se possiede la chiave, utilizzata

per la cifratura del messaggio stesso.
Questo tipo di crittografia presuppone che mittente e destinatario siano i soli a possedere la medesima chiave, la cosiddetta chiave simmetrica, che in questo sistema funge sia da chiave per cifrare il messaggio, che chiave per decifrare il messaggio.
L'immagine seguente mostra il meccanismo di crittografia simmetrica:

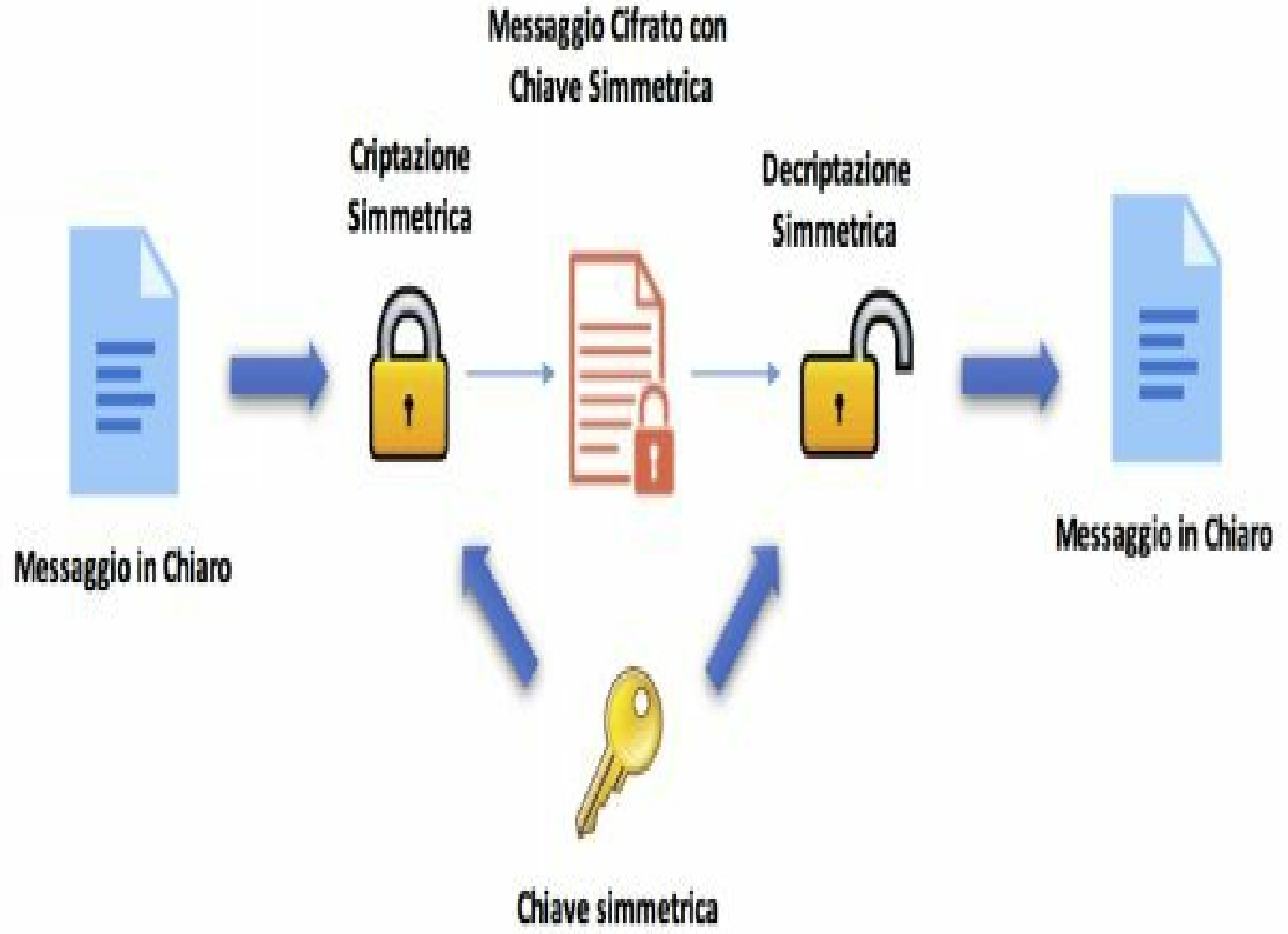


Figura n.23: illustrazione del funzionamento della crittografia simmetrica, a chiave privata

Come si evince dall'immagine soprastante, la chiave simmetrica è la

sola che cifra e decifra il messaggio di testo e viene scambiata tra mittente e destinatario, utilizzando un canale di scambio sicuro.

Consideriamo **P**, il messaggio di testo originale, crittato con la chiave simmetrica **k**, utilizzando un algoritmo di crittografia simmetrica **s**, la funzione di crittografia simmetrica sarà la seguente, dove **C** rappresenta il messaggio cifrato:

$$S\ (P,\ k) = C$$

L'utente destinatario in questo sistema di crittografia a chiave privata è in possesso della chiave simmetrica **k**, ed una volta ricevuto il messaggio cifrato **C**, utilizza un algoritmo di decrittazione simmetrica **D**, presentando la chiave simmetrica **k** in suo possesso. La funzione risultante darà come risultato **P**, il messaggio di testo originale:

$$D(C,k) = P$$

Gli algoritmi di firma a chiave privata

sono: AES (Advances Encryption Standard), DES (Data Encryption Standard) e 3DES (Triple DES)[54].

Capitolo 3
Bitcoin nella realtà quotidiana

3.1 L'ecosistema Bitcoin

Le transazioni in Internet risalgono ai primi anni settanta del secolo scorso con la nascita del primo sistema elettronico che consentiva il trasferimento di informazioni e dati in un formato

elettronico; questo sistema è L'Electronic Data Interchange (conosciuto anche con l'acronimo EDI). L'Electronic Data Interchange consentiva il trasferimento di informazioni in formato elettronico tramite reti di telecomunicazioni private ed era utilizzato maggiormente dalle grandi aziende.

Con l'avvento di Internet, tra la fine degli anni Ottanta e l'inizio degli anni Novanta, si assistette ad una rivoluzione dell'EDI, la quale comportò notevoli conseguenze a livello economico,

sfociando nella cosiddetta “new economy”[55].

Come evidenzia Giorgio Lener nel suo articolo “Il commercio elettronico”, in questo nuovo ambito di totale cambiamento innovativo legato alla diffusione delle tecnologie informatiche, moltissime aziende si sono del tutto “trasferite” online, facendo del commercio elettronico la sola fonte di guadagno.

E’ in questo contesto di evoluzione continua, e di new economy, nata con l’avvento di Internet e basata sul

trasferimento del commercio tradizionale in commercio elettronico, e sull'utilizzo sempre più frequente delle monete elettroniche anziché le monete tradizionali, che ebbe luce un nuovo ecosistema: l'ecosistema delle criptovalute.

Come già accennato, le criptovalute nascono come conseguenza della scoperta e dell'approfondimento delle scienze crittografiche, e nascono in un contesto di scoperta di una realtà parallela alla realtà fisica, nella quale la prima valuta crittografica creata e la più

diffusa è proprio il bitcoin.

Un sito interessante è www.bitsblockchain.net, il quale mostra una panoramica delle più diffuse criptovalute presenti oggi ed il loro reale equivalente in bitcoin.

Le criptovalute prese in considerazione dal sito Bits Blockchain Explorer sono ATMC, BTC, XRP, DOGE, LTC ed ETH.

Il presente sito, oltre a fornire un'equivalenza tra Altcoins e Bitcoin, fornisce anche l'equivalente di 1 BTC in EUR (Euro) e USD (Dollaro

americano); 1 BTC= 4641,08 EUR e 5486,46 USD (aggiornamento al 15 ottobre 2017).

L'immagine sottostante mostra la barra superiore del sito Bits Blockchain Explorer, nella quale vi sono le equivalenze tra le criptovalute e le valute legali con il bitcoin (BTC):

Figura n.24: sito Bits Blockchain Explorer e l'ammontare dei BTC nelle

diverse valute/criptovalute

I principali attori e gestori di questo ecosistema sono i minatori. I minatori svolgono il ruolo maggiore all'interno della rete Bitcoin e sono loro a tenerla in vita.

Attraverso la risoluzione dei Proof-of-Work, prove di lavoro fornite dalla rete, ed attraverso il mettere a disposizione la potenza di calcolo dei propri dispositivi hardware, i minatori aumentano la produzione di blocchi, cercando di aggiudicarsi la ricompensa.

Ad ogni emissione di un nuovo blocco viene emessa una quantità stabilita di bitcoin, che sarà la ricompensa del minatore che per primo ha prodotto il blocco.

La quantità di nuovi bitcoin emessi ad ogni produzione di un nuovo blocco è fissata. Originariamente venivano generati 50 BTC ad ogni produzione di un nuovo blocco, e questa quantità prevedeva un dimezzamento ogni 210.000 nuovi blocchi (ovvero ogni 4 anni).

Il primo dimezzamento si è verificato

nel 2012 e la ricompensa equivaleva a 25 BTC.

Il secondo dimezzamento si è verificato nel 2016 e la ricompensa attuale equivale a 12,5 BTC, fino al 2020 nel quale la ricompensa sarà circa 6 BTC, e così via fino ad esaurimento delle ricompense. Infatti, il futuro di Bitcoin dipende dalla diffusione che questa criptovaluta riuscirà ad ottenere ed alla sua adozione come forma di pagamento, in quanto i minatori in assenza di ricompensa non saranno spronati a continuare la loro attività di mining.

Altri attori che gravitano intorno ai minatori in questo ecosistema sono gli usufruitori della rete Bitcoin, coloro che possiedono portafogli elettronici Bitcoin e svolgono attività di compravendita online; gli sviluppatori, coloro che contribuiscono al miglioramento del sistema Bitcoin, risolvendo di volta in volta bug e falle del sistema ed infine le piattaforme online, che fungono da intermediari, fornendo servizi e opportunità di investimento sulla criptovaluta.

3.2 I vantaggi

Il protocollo Bitcoin nacque con l'obiettivo di permettere pagamenti in rete anonimi, celeri e decentralizzati. Oltre a questo aspetto, la sua natura decentralizzata e la sua natura crittologica fecero emergere numerosi vantaggi.

E dunque alla domanda "Perchè utilizzare Bitcoin?", risponderò presentando i vantaggi di questo nuovo e "rivoluzionario" sistema.

Il sistema Bitcoin permette:

- **Transazioni veloci ed efficienti:** essendo un sistema di pagamento decentralizzato, con nessun ente terzo che lo controlli, lo gestisca e ne emetta moneta, i pagamenti in Bitcoin non prevedono costi di commissione. Le transazioni di Bitcoin sono economiche e potrebbero prevedere un costo

aggiuntivo di circa 0.02 €, valido per transazioni di ogni importo. Inoltre, la velocità delle transazioni è dovuta dal lavoro dei nodi, che controllano e validano tutte le transazioni ed i blocchi in un tempo breve;

- **Transazioni trasparenti ed accessibili:** essendo un sistema basato sull'utilizzo della crittografia, tutte le transazioni e tutti i movimenti all'interno della rete

sono resi pubblici, e sono celati dietro un codice alfanumerico che offusca l'identità della persona proprietaria. Chiunque ha accesso alla consultazione delle transazioni in rete, ma risulta quasi impossibile associare una transazione ad una persona fisica, in quanto vige un sistema rigido e complesso che garantisce la sicurezza e l'anonimato delle transazioni (vedi cap.2).

Inoltre, Bitcoin garantisce un alto livello di accessibilità perché è facile da usare; chiunque può crearsi un indirizzo Bitcoin ed iniziare ad inviare e ricevere denaro in rete, senza sottostare a limiti imposti dalle autorità;

- **Transazioni anonime e sicure:** come asserito in precedenza, ciascuna transazione in Bitcoin è anonima e celata da un

codice alfanumerico, definito codice Hash. La rete Bitcoin garantisce alti livelli di sicurezza, in quanto ad ogni utente vengono assegnati tre valori Hash: la chiave privata, la chiave pubblica e l'indirizzo Bitcoin. La chiave privata non deve essere resa nota a secondi, ed è la sola che permette di effettuare transazioni in rete. La chiave pubblica e l'indirizzo Bitcoin permettono di ricevere

denaro; il mittente per poter trasferire denaro deve essere in possesso della chiave pubblica o dell'indirizzo bitcoin del destinatario, e non potrà mai venire a conoscenza della chiave privata associata ai codici di cui dispone;

- **Transazioni con micro importi:** la rete Bitcoin garantisce la possibilità di inviare e ricevere pagamenti con importi molto

ridotti, a differenza di altri sistemi di pagamento che impongono una soglia minima nelle transazioni;

- **Transazioni previo consenso:** in Bitcoin tutte le transazioni prima di essere validate e confermate dai nodi, devono ricevere il consenso di almeno il 51% dei nodi della rete. Il consenso ad una transazione avviene tramite l'apposizione di una firma digitale

alla transazione stessa. Questo sistema è utilizzato come garanzia dell'onestà della transazione stessa, in quanto blocca tutte le transazioni considerate sospette o disoneste;

- **Democrazia nella rete:** la rete Bitcoin avendo una natura open source, è aperta a tutti gli sviluppatori ed esperti di informatica permettendo loro di poter apportare modifiche e miglioramenti al sistema.

Nonostante ciò, la modifica deve passare prima sotto il consenso del 51% dei nodi della rete, i quali dovranno approvare il passaggio alla versione successiva.

Considerando i vantaggi sopra definiti, moltissime aziende e piccole imprese potrebbero innovare il loro ecosistema di guadagni adottando ed accettando pagamenti in Bitcoin. Particolare rilievo potranno assumere le compagnie No-Profit, nel mostrare il loro

organigramma sempre più trasparente e le donazioni potranno essere visibili al pubblico, incentivando sempre più persone a donare.
Inoltre, permettendo pagamenti minimi che non prevedono alcuna soglia da superare, in caso di disastri naturali, le persone saranno motivate maggiormente ad inviare una piccola donazione a favore dei colpiti, senza dover sottostare a soglie da rispettare e costi aggiuntivi da pagare.

3.3 Gli svantaggi

Nonostante i numerosi vantaggi e le buone prospettive future in un'eventuale adozione della valuta virtuale, vi sono altrettanti rischi e svantaggi. Sono molte le autorità comunitarie che hanno votato a sfavore di una possibile adozione delle valute virtuali accanto alle solite valute legali. Tra queste autorità comunitarie, l'Autorità Bancaria Europea (EBA) e la Banca Centrale Europea (BCE) nel 2014 esortarono apertamente le autorità nazionali a impedire l'uso delle valute virtuali perché individuarono numerosi profili di rischio che potrebbero derivare dall'utilizzo delle stesse.

Nel rapporto dell'EBA, pubblicato il

giorno 4 luglio 2014, furono identificati 70 fattori di rischio e l'Autorità Bancaria Europea, rivolgendosi alle autorità di vigilanza nazionali, indicò di scoraggiare le istituzioni di pagamento online, gli istituti di credito e le istituzioni di e-money ad accettare valute virtuali come pagamento legittimo.

Ad oggi la situazione fiscale e legale del possesso di moneta virtuale Bitcoin non è omogeneo in tutto il mondo, non esiste una legge o una regolamentazione che definisca la legalità e l'illegalità della compravendita, detenzione e attività di mining delle criptovalute. Sono ancora molti i paesi che non si sono dichiarati né a favore né a sfavore, molti che ne

vietano il possesso ed altri che ne permettono soltanto l'attività di mining.

Le organizzazioni mondiali e statali sono turbati dalla caratteristica più importante delle criptovalute: l'anonimato delle transazioni. Se in una transazione non si potrà più risalire al mittente, saranno effettuate molte attività illegali senza che le autorità statali puniscano il colpevole.

Nell'Unione Europea vige l'avvertenza da parte dell'Autorità Bancaria Europea, di vietare l'utilizzo delle criptovalute nelle nazioni facenti parte dell'Unione. Tuttavia, è libero lo scambio di criptovalute e le attività di mining e la compravendita online di bitcoin sono legali.

Nel 2015, la Banca d'Italia emanò una regolamentazione con il titolo "Avvertenza sull'utilizzo delle cosiddette valute virtuali", nel quale afferma quanto segue *"in Italia, l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale"*. Chiara è la situazione in Cina, dove la "People Bank of China" (PBOC) mediante l'avviso "Precautions against the risks of Bitcoin"[56] del dicembre 2013, ha dichiarato pubblicamente che la compravendita dei bitcoin è legale tra individui aventi la cittadinanza cinese,

ma vietata per le banche e le altre istituzioni finanziarie.

Negli Stati Uniti, invece, la criptovaluta è considerata come un "prodotto ibrido", in quanto ricalca le caratteristiche sia della valuta legale che di una commodity[57] e può comportarsi come una sostituta alle valute legali.

Nel presente paragrafo ci si propone di elencare i possibili svantaggi, legati all'utilizzo della criptovaluta come forma di pagamento in rete.

La rete Bitcoin presenta i seguenti svantaggi:

- **Fluttuazioni del prezzo:** il prezzo della valuta Bitcoin è altamente instabile ed imprevedibile. Questa instabilità di prezzo scoraggia gli usufruitori della criptovaluta, perché è altamente sconsigliato accumulare quantità di Bitcoin per lunghi periodi, in quanto il prezzo totale potrebbe variare da un momento all'altro a seconda del lavoro dei nodi;

- **Limiti all'anonimato:** tutte le transazioni della rete Bitcoin sono pubbliche e facilmente accessibili da chiunque. Avendo accesso alle transazioni, si ha accesso anche ai diversi indirizzi Bitcoin, dai quali è facile risalire al portafogli elettronico associato e conoscerne i movimenti. E' proprio per questa motivazione, che è consigliato cambiare indirizzo

bitcoin, ogni qualvolta si voglia inviare del denaro nella rete Bitcoin;

- **Irreversibilità delle transazioni:** una volta inviato il denaro è impossibile annullare la transazione e riavere il denaro. E' importante, perciò, assicurarsi della correttezza dell'indirizzo Bitcoin inserito. Nella rete Bitcoin non sono previste garanzie a tutela del fruitore del servizio e perciò non è possibile

chiedere né un annullamento della transazione né un rimborso, in quanto non vi è un ente terzo garante della gestione della rete;

- **Vulnerabilità della sicurezza:** in Bitcoin, il possesso della chiave privata è il solo modo che permette di spendere il denaro contenuto nel wallet bitcoin associato. Molti utenti si affidano a terzi, per quanto concerne la custodia

della chiave privata, conservandola online in siti web appositi o nel proprio hard disk. Questi sistemi di custodia delle chiavi private, purtroppo, non sono immuni da attacchi criminali e molto spesso si verificano episodi di furto delle chiavi private a causa di attacchi hacker a questi servizi.

3.4 Critiche al Bitcoin

Nonostante Bitcoin sia un sistema innovativo in continua scoperta ed in continua ricerca di trovare implicazioni empiriche adeguate, vi sono tuttavia molti voti a sfavore di questo nuovo ecosistema. Se da un lato vi sono le nazioni e le autorità ancora incerte sul da farsi e lontane da un'eventuale presa di posizione, dall'altro vi sono esperti e qualificati che criticano questo sistema, cercando di "aprire" gli occhi alla gente. Uno dei personaggi più famosi

che lanciò pesanti critiche al sistema monetario Bitcoin fu Paul Krugman, oggi docente di Economia presso l'Università di New York.

Paul Krugman, si fece conoscere per il suo radicale scetticismo nei confronti del sistema di pagamento Bitcoin ed in una possibile adozione delle criptovalute in generale, accanto alle valute legali.

Egli condanna apertamente la natura instabile del Bitcoin, considerato da egli come il diavolo[58], affermando che un'economia non può basarsi su un

sistema di pagamento instabile, soggetto a continue fluttuazioni irregolari di prezzi alti e bassi.

Egli asserisce, nel suo trattato “The conscience of a Liberal”[59], che una moneta deve fungere sia da mezzo di scambio sia da mercato stabile di valuta, ed aggiunge che la gran parte degli economisti moderni, non rispondono mai alla domanda “Ma la rete Bitcoin è un mercato stabile di valuta?”, ma preferiscono deviare dalla domanda, e rispondere mostrando quanto è vantaggioso l’utilizzo della moneta

Bitcoin come mezzo di scambio.

Di seguito un estratto scritto da Paul Krugman nel suo blog[60]:

"At the end of 2013, I wrote a post titled "Bitcoin is evil," riffing off Charlie Stross's "Why I want Bitcoin to die in a fire." Charlie and I both keyed in on the obvious ideological agenda: Bitcoin fever was and is intimately tied up with libertarian anti-government fantasies."

Per Paul Krugman la rete Bitcoin è una

rete anti-sociale, perché non dipende da alcun ente che gestisca l'emissione di moneta; per questa sua espressione, Krugman fu definito contradditorio da molti economisti che risposero a questa provocazione mostrando la natura libertaria della moneta digitale.

Gli amanti del Bitcoin - aggiunge Krugman - amano la natura anonima e libertaria della rete Bitcoin, abusando del proprio potere di generare denaro; una sua frase è " *allo stesso tempo è molto particolare, poiché i bitcoin hanno un valore evocato dal nulla. A*

differenza di oro e banconote il valore di questa moneta digitale deriva dalla convinzione che gli altri la accettino come metodo di pagamento"[61].

Egli è scettico anche per quanto concerne l'economia Americana, la quale è vista dai suoi occhi come ormai in crisi e fallita, diretta verso la rovina, senza alcuna via d'uscita. Ironicamente in un suo scritto egli afferma che gli unici esseri che potranno salvare l'economia Americana saranno gli alieni, utilizzando i loro poteri magici!

Altre critiche alla rete Bitcoin sono state

mosse da studiosi ed esperti in materia che vedono i pagamenti in bitcoin come un mezzo pericoloso che permette di compiere un giro di affari illeciti.

Questi esponenti criticano il sistema Bitcoin, appellandosi e presentando l'esempio del Deep Web, una parte del Web accessibile solo da specifici browser, non indicizzati e non accessibili da alcun motore di ricerca.

Il Deep Web rappresenta il 99% dei siti del mondo, la cui maggior parte di essi sono siti di compravendita di materie e prodotti illegali e fornitura di servizi

online vietati dalla legge; in questo spazio virtuale vi è un'economia parallela alla nostra, denominata "mercato nero digitale" in cui vengono esercitate azioni di compravendita illecite.

E' proprio attraverso il Deep Web che i pagamenti in bitcoin sono i favoriti da coloro che acquistano o forniscono servizi illegali, perché possono portare a termine il loro operato in totale anonimato e senza che qualcuno mai riesca a trovarne traccia.

Ma, come asseriscono Marco Nastasi,

Michele Munaretto e Gabriele Maltinti nel loro “Bitcoin: manuale alla portata di tutti sull’oro del 21° secolo”, il bitcoin è solo un mezzo attraverso il quale queste azioni illecite vengono compiute, e criticare e condannare l’utilizzo del bitcoin è come condannare l’uso di un fucile perché utilizzato da terroristi, senza mettere in considerazione che un fucile può essere anche utilizzato da un normale cacciatore.

3.5 Attacchi alla rete Bitcoin e possibili vulnerabilità della rete informatica

La rete Bitcoin proprio per la sua natura decentralizzata è considerata dagli hacker uno dei bersagli principali. In questo paragrafo si esamineranno i principali tipi di attacco alla rete Bitcoin e la vulnerabilità di questa rete.
Negli ultimi anni, non sono stati pochi i furti delle chiavi private e del rispettivo

ammontare Bitcoin ad esse associato.

Nella storia dei Bitcoin i furti più importanti sono avvenuti rispettivamente nel febbraio del 2014, con un furto alla MtGox [62]giapponese di ben 450 milioni di dollari in BTC, e nell'agosto del 2016, con un furto alla Bitfinex[63] giapponese di ben 65 milioni di dollari in BTC.

Anche quest'anno (marzo 2017) gli hacker hanno preso di mira un sito della Corea del Sud con sede a Seul, accedendo a ben quattro portafogli elettronici ed effettuando un furto con un

importo di ben 5.5 milioni di dollari.
Questi episodi causarono dei forti crolli del valore della valuta ed aumentano la natura instabile della criptovaluta.
La figura seguente mostra le percentuali degli attacchi informatici che hanno mirato al furto del denaro agli utenti (rapporto del 2015).

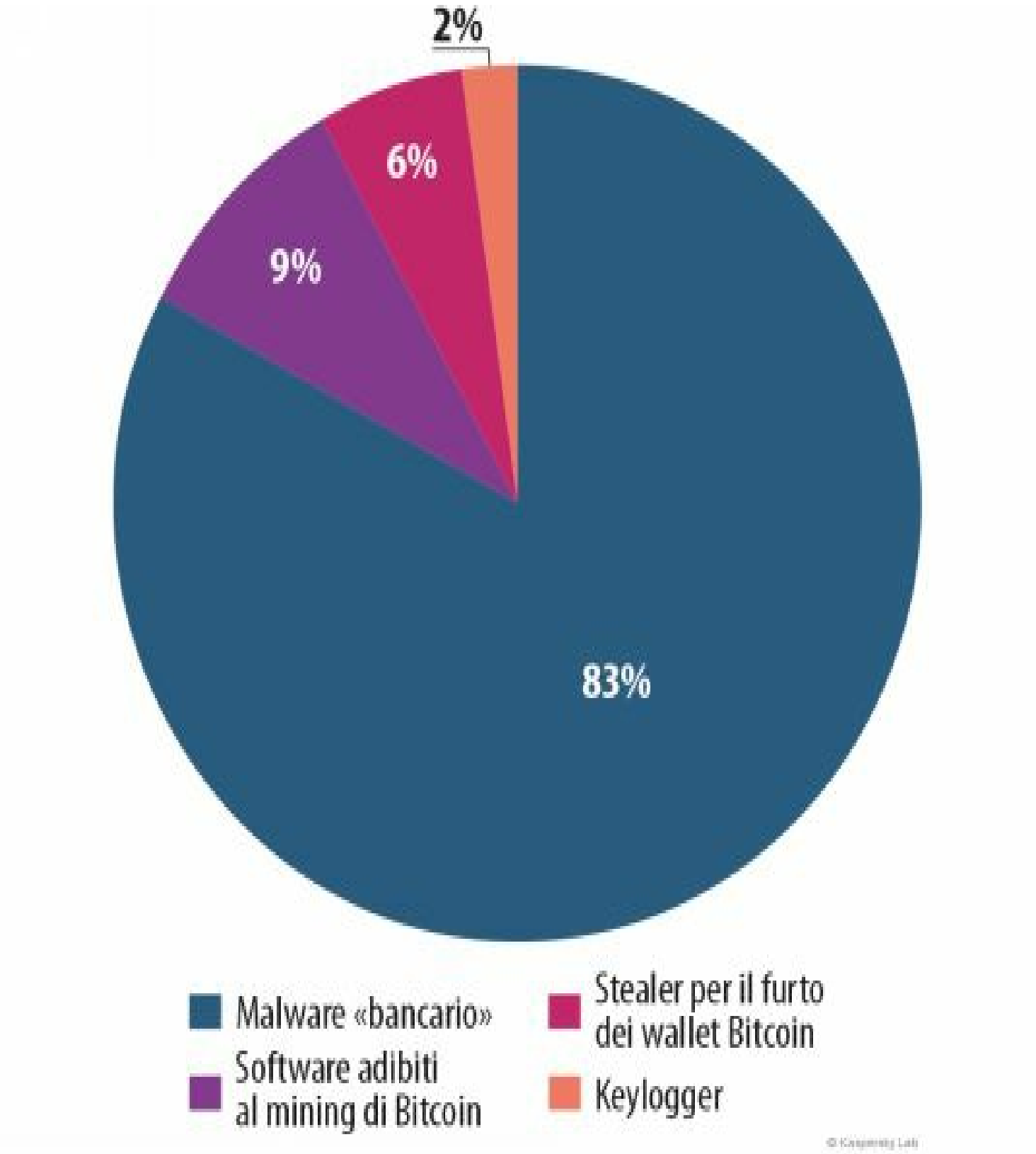


Figura n. 25: ripartizione degli attacchi più comuni legati al furto del denaro

degli utenti - Rapporto secondo semestre del 2015 “Evoluzione delle minacce informatiche”[64]

Come si può evincere da quanto detto e dall’immagine soprastante, uno degli attacchi prediletti dagli hacker è il furto di portafogli elettronici con conseguente possesso dell’importo in BTC in essi contenuti. La perdita delle monete virtuali non sono coperte da alcuna assicurazione e sono irreversibili ed è proprio questo il limite principale per chiunque voglia intraprendere un intero

business fondato sui bitcoin.

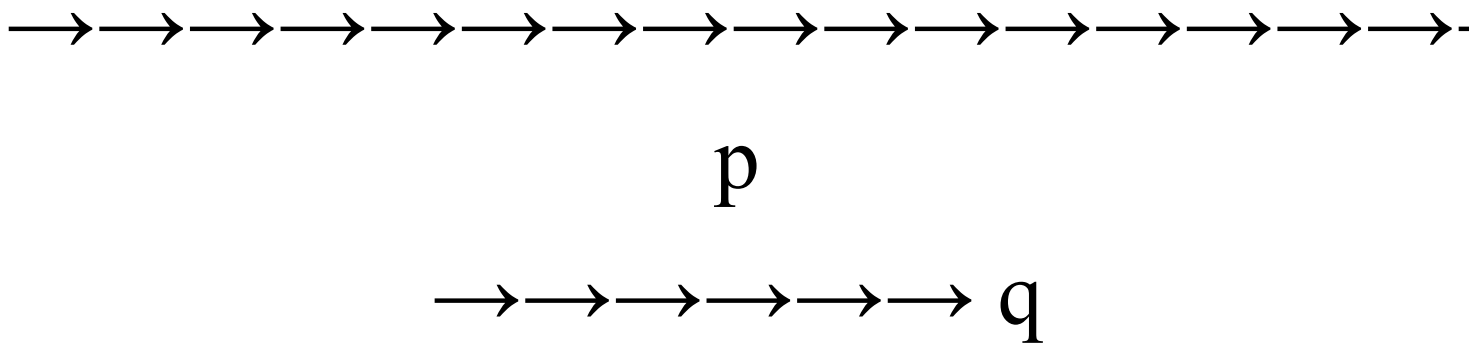
Una delle vulnerabilità della rete Bitcoin è il possesso di almeno il 51% dell'intera rete e potenza di calcolo. Chi possiede il 51% dell'intera rete e dell'intera potenza di calcolo è in grado di gestire le transazioni a suo piacimento, generando false transazioni ed accettandole a suo piacimento. Questo sistema continuerebbe fino a quando la forchetta dei nodi onesti non riuscisse a conquistare il 51% dell'intera rete, limitando la creazione di nodi disonesti.

Ma qual'è la probabilità che un nodo disonesto riesca ad impossessarsi del 51% dell'intera rete?

Come asserisce Satoshi Nakamoto, nel suo trattato "Bitcoin: A peer-to-peer electronic cash system", la probabilità che un hacker recuperi un certo svantaggio è analoga al teorema della *rovina del giocatore*[65]. Supponiamo che un giocatore in svantaggio, possiede una dotazione illimitata di fondi e può giocare infinite volte per cercare di raggiungere il pareggio.

Quanta probabilità ha di farlo?

(consideriamo il giocatore in svantaggio come l'attaccante (q) ed il giocatore in vantaggio come la catena di nodi onesti(p)).



p= probabilità che un nodo onesto trovi il blocco successivo, incrementando la sua lunghezza

q= probabilità che un nodo

disonesto trovi il blocco successivo,

incrementando la sua lunghezza

qz= probabilità che il nodo disonesto recuperi z blocchi di svantaggio

$$qz = 1 \text{ se } p \leq q$$

$$qz = (q/p)^{z} \text{ se } p > q$$

Si evince che all'aumentare di p, la probabilità (qz) diminuisce e si nota di conseguenza che l'attaccante ha poca possibilità di riuscire ad avere il

possesso del 51% dell'intera rete e se non effettua un balzo fortunato, la probabilità diventa minima al limite del nullo.

Ma, poiché la rete è aperta, se l'attaccante riuscisse a possedere una potenza di calcolo superiore al resto della rete, riuscirebbe a produrre più blocchi e di conseguenza ad impossessarsi del 51% della rete.

Poiché non vige alcun controllo nella rete Bitcoin, nessuno potrebbe vietare che tutto ciò accada e/o appellarsi ad una legge e considerare questo atto come

illecito.

Tuttavia, il nodo disonesto potrebbe decidere di rimanere onesto, avendo il pieno controllo su tutti gli altri nodi della rete e riuscendo ad aggiudicarsi una ricompensa giornaliera, dovuta alla risoluzione del Proof-of-Work prima degli altri nodi. E' da considerare che far fallire il sistema, causerebbe un crollo enorme di valuta e non sarà una mossa nemmeno a favore dell'attaccante, che ne potrebbe risentire delle perdite di valore della valuta.

Un altro attacco piuttosto comune è

l’attacco a collisione, che si viene a creare nel momento in cui due stringhe di testo, di lunghezza variabile producono lo stesso valore di Hash. Questo evento può capitare, in quanto i valori di Hash sono codici alfanumerici, di lunghezza finita e definita e potrebbero crearsi disfunzioni al momento della conversione da messaggio di testo a messaggio digest (valore di Hash).

In questo caso, l’attaccante potrebbe generare un indirizzo Hash uguale all’indirizzo Hash di un altro utente, e

ricevere lo stesso importo di denaro del reale possessore del codice Hash.
Un altro tipo di attacco, ed è il più comune, è legato al problema del double-spending[66]. Consideriamo due utenti **x** e **y**:

x= attaccante che vuole far credere a **y** di aver effettuato il pagamento, per poi in un secondo momento invertirlo a sé stesso;

y= destinatario del pagamento.

y, ignaro delle dinamiche a cui andrà

incontro, genera un nuovo paio di chiavi (chiave privata e chiave pubblica) e fornisce la chiave pubblica a **x**, per permettere a quest'ultimo di effettuare il pagamento.

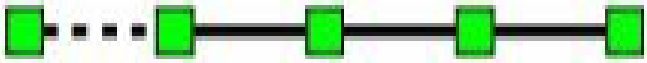
Una volta che **x** effettua il pagamento, invia la transazione in rete, e parallelamente a ciò, inizia a creare una catena parallela più lunga, che contiene una versione alternativa della sua transazione (una transazione verso **z**).

Al termine di questo processo, si creerà una biforcazione della blockchain (fork) dove sarà considerato valido e riceverà

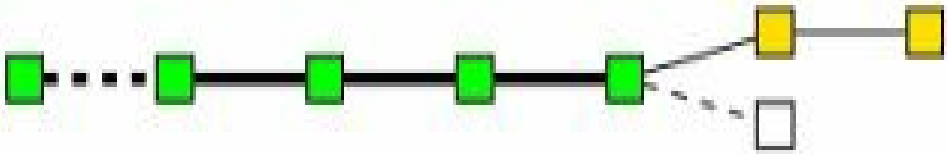
conferme il blocco che contiene transazioni confermate.

Visto che la transazione di **x** a **y**, è stata sostituita con una transazione di **x** a **z**, contenute in una catena più lunga, la transazione di **x** a **y** non avendo ricevuto conferme, non è valida perché farebbe riferimento ad un input già speso (input di **x**).

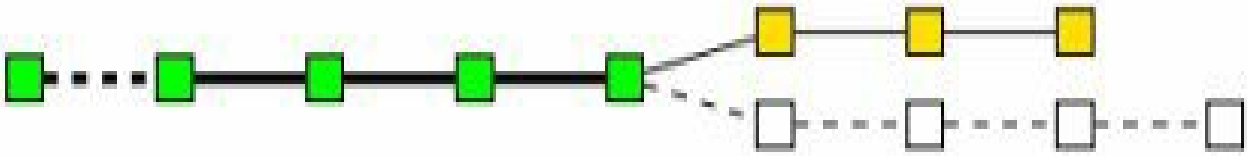
Di seguito, un'immagine mostrante come avviene questo tipo di attacco:



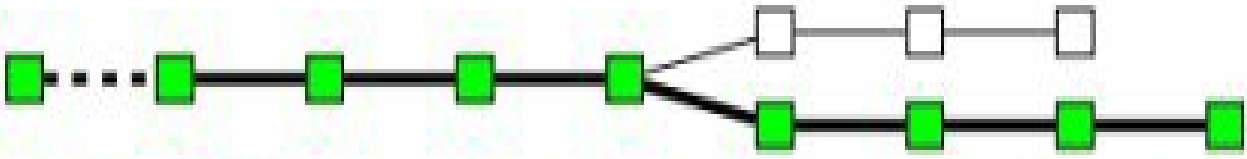
(a) Initial state of the blockchain in which all transactions are considered as valid.



(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.



(c) The attacker succeeds in making the fraudulent branch longer than the honest one.



(d) The attacker's branch is published and is now considered the valid one.

Figura n.18: illustrazione dell'attacco double spending. I passi che portano un attaccante a "camuffare"una transazione.

3.6 Prospettive future

La rete Bitcoin, essendo stata pre-limitata ad una quantità massima di 21 milioni di BTC come ricompensa, ha una vita limitata.
L'attività di mining, oggigiorno, è portata avanti grazie alla ricompensa che i minatori ricevono per il loro lavoro e per la potenza di calcolo che mettono a disposizione, tenendo in vita questo grande ecosistema.
Come anticipato nei paragrafi

precedenti, questa ricompensa viene dimezzata ogni 4 anni, e di conseguenza ad oggi ricevere una ricompensa potrebbe rivelarsi un'attività assai ardua, per i seguenti motivi:

- bisogna acquistare dispositivi hardware appositi per l'attività di mining, con una grande potenza di calcolo, in modo da riuscire a risolvere i proof-of-work, che la rete genera. Questi dispositivi hardware sono molto costosi;
- bisogna riuscire a risolvere il

proof-of-work prima che qualche altro nodo della rete trovi la soluzione;

- bisogna che le transazioni di un determinato blocco siano tutte confermate e validate dai nodi della rete, al fine di ricevere la ricompensa;
- la ricompensa è minima e diminuisce di anno in anno, fra qualche anno sarà prossima allo 0;

Si stima che in futuro, in assenza di ricompensa, il lavoro dei minatori non

sarà incentivato a continuare e, con l'abbandono dell'attività di mining, la vita di Bitcoin sarà prossima alla fine.
L'unica possibilità che la rete Bitcoin ha di vita è quella di imporsi come moneta di scambio, al pari delle altre monete, vantando in questo modo degli stessi diritti di quest'ultime ed essendo considerata un legittimo mezzo di scambio a livello internazionale.
In questo paragrafo, si propone di presentare le previsioni, viste sia da un occhio pessimista che da un occhio ottimista, riguardanti la vita futura di

Bitcoin.

3.6.1 Il Bitcoin potrà sostituire le valute legali?

La valuta digitale bitcoin per poter sostituire le valute legali, deve innanzitutto poter soddisfare le caratteristiche delle valute legali, quali:

- stabilità del valore della valuta;
- moneta intesa come mezzo di pagamento;
- rapporto prezzo/beni e servizi

stabile e facile da inquadrare.

La valuta virtuale bitcoin, essendo un sistema monetario decentralizzato e non soggetto a nessun controllo sull'emissione da parte delle Banche Centrali, non può soddisfare il primo prerequisito, ovvero quello riguardante la stabilità del prezzo. Infatti l'instabilità di questa criptovaluta è stata la causa principale delle critiche mosse da Paul Krugman, presentato in precedenza.

In Bitcoin il valore della valuta è

fortemente instabile e cambia notevolmente più volte nell'arco della giornata. Avendo natura instabile, è anche difficoltoso stabilire un prezzo fisso ad un determinato prodotto, bene o servizio, in quanto vi deve essere un bilancio tra il prezzo ed il servizio offerto, e per poter stabilire tale bilancio si dovrebbero modificare più volte nella giornata i prezzi dei beni in vendita.

L'unico requisito che questo nuovo sistema di pagamento potrebbe soddisfare è l'essere utilizzato come

mezzo di pagamento. Molti al giorno d'oggi sono i negozi sia fisici che virtuali, che accettano pagamenti in bitcoin, prendendo le dovute precauzioni.

Parallelamente all'aumento dei negozi fisici e virtuali che accettano bitcoin, sono in aumento utenti che scelgono di crearsi un portafoglio elettronico e gestirlo in totale autonomia, usufruendo di alti livelli di privacy, bassi costi di commissione e transazioni veloci e sicure.

In riferimento a quanto esposto, la valuta

digitale Bitcoin non potrà sostituire facilmente le valute legali in quanto non soddisfa a pieno i requisiti base e le caratteristiche base di una moneta reale.
Anche dal punto di vista degli istituti finanziari, degli enti garanti dei servizi di pagamento e dei gestori dell'emissione di moneta, risulterebbe molto pericoloso accettare di trasferire un'intera economia ad un sistema decentralizzato, dove ogni azione è lecita e dove non vige alcun controllo né garanzia.
Tuttavia, se Bitcoin non viene accettato

come mezzo di pagamento e non riuscisse a conquistare un largo consenso a livello internazionale, il suo futuro potrebbe rivelarsi prossimo ad una fine.

Inoltre, se ciò dovesse accadere il futuro di Bitcoin, vedrà l'abbandono dell'attività di mining, la quale una volta esaurito l'ammontare della ricompensa prestabilita, i minatori non avranno scopo di continuare la loro attività, senza la ricezione di una minima remunerazione al loro lavoro.

Un'alternativa all'abbandono

dell'attività di mining, potrebbe verificarsi in una sua concentrazione nelle mani di pochi, in questo caso il destino di Bitcoin sarà da imputarsi ad un mero dirigersi verso un potere non più decentralizzato, ma nelle mani di pochi.

D'altro canto, la situazione attuale vede sempre più paesi coinvolti in questo ecosistema e molte aziende vedono nelle criptovalute, in particolar modo nel bitcoin un'opportunità da approfondire e sfruttare al meglio per ciò che ci riserverà nel futuro.

Le autorità governative si vedono ancora avvolte nel dubbio riguardo alla legislazione adatta da apportare in questo ambito e sono timorosi nell'accettare un ecosistema, che vede transazioni, wallet elettronici e detenzioni di denaro anonimi.

E' un sistema vasto, comprendente vari ambiti e necessita di una legislazione omogenea che ricopra tutti gli ambiti del bitcoin, che sia anche valida per tutti i paesi, chiara e lontana da ambiguità.

La possibilità per le istituzioni statali potrebbe essere di fare a meno della

peculiarità base del bitcoin, ovvero la garanzia dell'anonimato, ed imporre a tutte le piattaforme online ed i siti di exchange che offrono servizi di custodia del denaro online, di richiedere i dati personali al fine di offrire e garantire il servizio.

CONCLUSIONI

La passione e l'amore per questa materia mi ha portato ad approfondire un tema molto attuale, di cui spesso non se ne parla o non se ne parla abbastanza. Ad oggi, argomenti come "cos'è il bitcoin?" o "cos'è la crittografia?" vengono un po' trascurati dalle istituzioni governative ed autoritarie e non vengono considerati argomenti importanti, al punto da presentarne le caratteristiche ed il funzionamento;

trovare articoli che ne parlino, e trovare del materiale, come analisi, grafici e statistiche attuali è un lavoro assai arduo visto il poco interesse da parte delle istituzioni ad interessarsi a questa materia.

Il presente libro nasce dall'obiettivo di portare maggior chiarezza riguardo il sistema Bitcoin, senza entrare nei dettagli tecnici e matematici, mantenendo una mera presentazione del sistema, basata su uno studio ed un'analisi accessibile a chiunque voglia accedere ad una conoscenza preliminare

di questo vasto "cripto-ecosistema".
Il libro dunque, ha attuato uno studio ed un'analisi trasversale, basata sullo studio della materia da più punti di vista, quali quello sociologico/umanistico, economico/scientifico, informatico/tecnologico.
Le diverse piattaforme esposte nel corso della tesi, sono state testate, analizzate e riportate nella presente tesi, al fine di garantire maggiore chiarezza sul tema e sul funzionamento dei relativi servizi offerti in rete.

Il libro ha dapprima presentato gli aspetti “esteriori” del sistema Bitcoin, presentandone le caratteristiche, l’innovazione apportata, la differenza dalle valute legali ed accenni alla storia, ripercorrendo gli aspetti salienti dalla nascita della criptovaluta ad oggi.

Il lavoro, ha proseguito nei capitoli successivi, presentando il funzionamento della moneta in rete, il sistema alla base delle transazioni, analizzando di volta in volta la grafica e le funzionalità dei siti e delle piattaforme utilizzate per lo studio.

Nel corso dello studio, sono stati trattati anche temi riguardanti il futuro di questa moneta virtuale, analizzando sia i riscontri positivi che negativi, prendendo in considerazione gli attuali vantaggi e svantaggi.

In conclusione, asserisco che il sistema Bitcoin potrebbe rivelarsi un gran punto di svolta per molti imprenditori ed aziende, che potrebbero vedere la possibilità di poter basare un intero business su un sistema del tutto decentralizzato, senza costi di commissione, imposte da parte dello

Stato e con pagamenti celeri e sicuri da parte dei clienti, d'altra parte sarà una questione ardua la considerazione di questa cripto-valuta come un metodo di pagamento legale a tutti gli effetti da parte delle autorità statali.

Bibliografia

Chaum David “Blind signatures for untraceable payments” - Springer Verlag - 1982

Chaum David “The dining cryptographers problem: unconditional

sender and recipient untraceability” - Springer Verlag - 1988
Lener Giorgio “Il commercio elettronico” - “Comunicazione digitale e comunicazione in rete” di Zuanelli Elisabetta - ARACNE editrice S.r.l. - maggio 2012
Nastasi Marco, Munaretto Michele, Maltinti Gabriele “Bitcoin, Manuale alla portata di tutti sull’oro del 21° secolo” - Independently published - 3 ottobre 2017
Satoshi Nakamoto “Bitcoin: a peer-to-peer electronic cash system” -

Independently published - 1 novembre 2008
Tombolini Antonio “Bitcoin Manifesto: una cpu un voto” - Antonio Tombolini Editore - 14 dicembre 2015

Sitografia

Agi - Cosa muove davvero Bitcoin e perché è impossibile fermarlo - https://www.agi.it/innovazione/1345617/news/2017-01-03/

Altcoins

- http://www.investopedia.com/

Autorità Bancaria Europea

- https://www.eba.europa.eu/la

B-money –

BitcoinWiki - https://en.bitcoin.it/

money

Bitcoin - Wikipedia -

https://it.wikipedia.org/wiki/Bit

Bitaddress.org

- https://www.bitaddress.org/bit

Bitcoin Address – Bitcoin Wiki

- https://en.bitcoin.it/wiki/Addre

Bitcoin ATM map

- https://coinatmradar.com/

Bitcoin.org

- https://bitcoin.org/it/wallets/m

Bit Connect -

https://coinmarketcap.com/

Bits Blockchain

- https://www.bitsblockchain.ne

Block Explorer

- https://blockexplorer.com/

Blockchain – Wikipedia

- https://it.wikipedia.org/wiki/Bl

Chaum David – Wikipedia

- https://en.wikipedia.org/wiki/I

Chiave privata – Wikipedia

- https://it.wikipedia.org/wiki/Cl

Chiave pubblica – Wikipedia

- https://it.wikipedia.org/wiki/Cl

Cloud computing – Wikipedia

- https://it.wikipedia.org/wiki/Cl

Coinbase

- https://www.coinbase.com/?locale=it

Coinmap.org

- https://coinmap.org/#/map/50.

Comunicazione del 30 gennaio 2015 – Banca d'Italia

- https://www.bancaditalia.it/pubblicazioni/vigilanza/2015-01/20150130_II15.pdf

Costa Pier Francesco – Bitcoin aspetti tecnici, economici e politici di una crittovaluta

- http://amslaurea.unibo.it/7313/

Criptomining

- http://cryptomining-blog.com/tag/gigahash/

Criptovaluta – Wikipedia

- https://it.wikipedia.org/wiki/Cr

Critiche di Krugman Paul

- http://formiche.net/2013/04/15

stronca-il-bitcoin/

Crittografia asimmetrica – Wikipedia

- https://it.wikipedia.org/wiki/Cr

Crittografia simmetrica – Wikipedia

- https://it.wikipedia.org/wiki/Cr

Cyberpunk – Wikipedia

- https://it.wikipedia.org/wiki/Cy

DigiCash – Wikipedia - https://en.wikipedia.org/wiki/D

Direttiva 2009/110/CE del Parlamento Europeo e del Consiglio - http://eur-lex.europa.eu/LexUriServ/LexUri=OJ:L:2009:267:0007:0017:i

Double Spending – Wikipedia - https://en.wikipedia.org/wiki/D spending

Dove spendere Bitcoin

- https://anycoindirect.eu/it/dove spendere-bitcoin -

https://blog.comprarebitcoin.info/dove-spendere-bitcoin/

ECSA – Bitcoin Wiki

- https://en.bitcoin.it/wiki/Ellipti

Evoluzione delle minacce informatiche

- https://securelist.it/it-threat-evolution-q2-2015/58672/

Expedia Inc.

- http://www.expediainc.com/

Facebook Credits – Wikipedia

- https://en.wikipedia.org/wiki/F

Firma digitale – Wikipedia

- https://it.wikipedia.org/wiki/Fi

Fornaro Andrea - Il Potenziale dei Bitcoin: un sistema monetario alternativo - http://tesi.eprints.luiss.it/13433/andrea-tesi-2014.pdf

Foundation Italia Bitcoin-

https://www.bitcoin-italia.org/parere-su-quanto-espresso-dalla-banca-ditalia/

Guadagnare Bitcoin fratis

- http://guadagnarebitcoins.alter

Krugman Paul – Bitcoin is antisocial and impractical

- https://cointelegraph.com/news/krugmans-bitcoin-is-antisocial-and-impractical-argument-is-

flawed -

Krugman Paul – Bitcoin is evil - https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/ https://thinksteroids.com/community/threads/krugman-bitcoin-is-an-evil-libertarian-long-con.134359055/ http://bitcoin-vs.s3.amazonaws.com/krugman-bitcoin.html

Krugman Paul -

http://formiche.net/2013/04/15/stronca-il-bitcoin/

Local Bitcoins - https://localbitcoins.com/

Meetup - https://www.meetup.com/it-IT/topics/bitcoin/

Moneta legale – Wikipedia - https://it.wikipedia.org/wiki/Mo

New Economy – Wikipedia - https://it.wikipedia.org/wiki/Ne

Open source – Wikipedia

- https://it.wikipedia.org/wiki/O

Peer-to-peer – Wikipedia

- https://it.wikipedia.org/wiki/Pe

to-peer

People's Bank of China

- https://www.btcchina.com/pag

Qui Bitcoin

- https://www.quibitcoin.it/

Robocoin

- http://www.robocoinkiosk.it/

Storico delle quotazioni del Bitcoin

- http://valutevirtuali.com/bitcoi

quotazioni-storico/

Virtual Currency Schemes – Ocober 2012

- https://www.ecb.europa.eu/pu

Xapo - https://xapo.com/

Zen Alberto – Bitcoin analisi tecnica ed economica

- http://dspace.unive.it/bitstream/1184046.pdf?sequence=2

---

[1] Documento originale https://taler.net/papers/chaum-blind-signatures.pdf

[2] Documento originale http://www.cs.cornell.edu/people/egs/herbivore

[3] fonte https://en.wikipedia.org/wiki/David_Chaum

[4] DigiCash Inc: è una corporazione fondata da David Chaum nel 1989 con sede ad Amsterdam. La DigiCash Inc è una corporazione di pagamenti elettronici. fonte https://en.wikipedia.org/wiki/DigiCash

[5] fonte https://en.wikipedia.org/wiki/Adam_Back

[6] Cyberpunk: corrente letteraria e artistica che si sviluppò nel nord Europa verso la metà degli anni ‘80. fonte https://it.wikipedia.org/wiki/Cyberpunk

[7] Wei Dai è l’ideatore del sistema b-money. fonte https://en.bitcoin.it/wiki/B-money

[8] Documento originale https://bitcoin.org/bitcoin.pdf

[9] Liberty Dollar: moneta privata prodotta negli Stati Uniti, con valore legato all’argento e all’oro

[10]Mailing list: nel sito http://www.metzdowd.com/mailman/listinfo/cry vi è la possibilità di visionare la mailing list, previa autenticazione tramite e-mail e password

[11] Genesis block (o Blocco 0): è il primo blocco Bitcoin

[12] Mining: attività che permette agli utenti connessi tramite specifici dispositivi, di risolvere dei proof of work e di avere una

ricompensa finale in valuta virtuale.

[13] fonte http://valutevirtuali.com/bitcoin-quotazioni-storico/

[14] "Bitcoin: A Peer-to-Peer Electronic Cash System": https://bitcoin.org/bitcoin.pdf presente sul Web il documento originale che descrive le funzionalità della moneta ideata da Satoshi Nakamoto.

[15] Banca Centrale Europea: la Banca centrale europea (BCE) è la banca centrale di tutti coloro che hanno adottato l'euro (19 Stati membri dell'Unione europea). fonte https://www.ecb.europa.eu/ecb/html/index.it.htm

[16] Federal Reserve: è la Banca Centrale degli Stati Uniti d'America. fonte https://it.wikipedia.org/wiki/Federal_Reserve_S

[17] fonte "La relazione di fiducia tra la banca ed il cliente" - C. SALVATORI - L. CRISIGIOVANNI - F. ANELLI - N. PAGNONCELLI-

http://www.assbb.it/contenuti/news/files/quader

[18] Open source: software in cui gli autori rendono pubblico il codice sorgente al fine di rendere possibili modifiche e miglioramenti da parte di sviluppatori. fonte https://it.wikipedia.org/wiki/Open_source

[19] Peer-to-peer: modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client-server, ma sono nodi paritari che possono fungere sia da clienti che da servienti. fonte https://it.wikipedia.org/wiki/Peer-to-peer

[20] Autorità Bancaria Europea (EBA): è un'autorità che assicura la stabilità finanziaria nell'UE e garantisce l'integrità, l'efficienza e il regolare funzionamento del settore bancario. fonte https://www.eba.europa.eu/languages/home_it

[21] Valuta fiat: è la moneta legale ed ha valore solo perché appartiene ad un'autorità, uno

stato. La moneta legale, o valuta fiat, non ha un valore intrinseco e non è coperta da riserve di altri materiali. fonte https://it.wikipedia.org/wiki/Moneta_legale

[22] Virtual Currency Scheme: https://www.ecb.europa.eu/pub/pdf/other/virtual

[23]Criptovaluta: (crittovaluta o criptomoneta) è una valuta paritaria, decentralizzata digitale la cui implementazione si basa sulla crittografia per convalidare le transazioni ed emettere nuova moneta. fonte https://it.wikipedia.org/wiki/Criptovaluta

[24] Si veda al riguardo https://www.bancaditalia.it/pubblicazioni/bollett vigilanza/2015-01/20150130_II15.pdf

[25] fonte “Virtual Currency Schemes” - BCE - pagina 13-14 - https://www.ecb.europa.eu/pub/pdf/other/virtual

[26] Facebook Credits: era una valuta virtuale che permetteva agli utenti di Facebook di

acquistare beni e servizi all'interno di giochi online e applicazioni all'interno della comunità di Facebook. I Facebook Credits furono eliminati nel 2012. fonte https://en.wikipedia.org/wiki/Facebook_Credits

[27] Altcoins: sono criptovalute alternative al bitcoin, lanciate successivamente alla nascita dei quest'ultima. fonte http://www.investopedia.com/terms/a/altcoin.as

[28] DIRETTIVA 2009/110/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 16 settembre 2009 concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE. fonte http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:it:PDF

[29] Bitcoin Foundation Italia: è un'associazione

che si propone di difendere, diffondere e promuovere l'utilizzo della criptovaluta bitcoin in Italia; link al sito https://www.bitcoin-italia.org/

[30] Blockchain: è una base di dati distribuita, introdotta dalla valuta bitcoin che mantiene in modo continuo una lista crescente di record. fonte https://it.wikipedia.org/wiki/Blockchain

[31] Bitcoin address: stringa alfanumerica di 26-35 caratteri, che rappresenta una possibile destinazione per un pagamento in bitcoin. fonte https://en.bitcoin.it/wiki/Address

[32]fonte https://en.bitcoin.it/wiki/Address

[33] Chiave pubblica: è una chiave crittografica associata, utilizzata in un sistema di crittografia asimmetrica ed è associata ad una chiave privata. fonte https://en.bitcoin.it/wiki/Address

[34] Chiave privata: è una chiave crittografica, utilizzata in un sistema di crittografia asimmetrica ed è associata ad una chiave

pubblica. Il possesso della chiave privata permette l'invio/ricezione dei bitcoin associati ad essa. fonte https://it.wikipedia.org/wiki/Chiave_privata

[35] Firma digitale: schema matematico per dimostrare l'autenticità di un messaggio o di un documento digitale inviato su un canale digitale non sicuro. fonte https://it.wikipedia.org/wiki/Firma_digitale

[36] fonte http://dspace.unive.it/bitstream/handle/10579/611184046.pdf?sequence=2

[37] Bitaddress.org https://www.bitaddress.org

[38] Market makers: è un intermediario finanziario che pubblica i prezzi di acquisto e di vendita dei titoli quotati in borsa e di suo possesso permettendo a tutti gli altri investitori di comprare o vendere a quei prezzi.

[39] Automated Teller Machine: è il sistema per il prelievo automatico di denaro contante dal

proprio conto corrente bancario attraverso l'uso di una carta di debito nei distributori collegati in rete telematica

[40] Per approfondire, consultare il sito http://www.robocoinkiosk.it/

[41] Luca Dordolo: uno degli autori del libro "Bitcoin: Manuale alla portata di tutti sull'oro del 21° secolo"

[42] fonte https://coinatmradar.com/ ultima consultazione 30/09/2017

[43]Qr Code (Quick Response Code):codice a barre bidimensionale di forma quadrata, impiegato per memorizzare informazioni digitali ed essere letto mediante smartphone (Fonte: wiki/Codice_QR)

[44] Sito cloud: indica un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità on demand attraverso Internet a partire da un

insieme di risorse preesistenti e configurabili. fonte https://it.wikipedia.org/wiki/Cloud_computing

[45] GigaHash (GH): è una parte della potenza di calcolo del server. E' un'operazione che inizia come un investimento in mining privato e successivamente offre un servizio di cloud mining. fonte http://cryptomining-blog.com/tag/gigahash/

[46] fonte http://guadagnarebitcoins.altervista.org

[47] Coinbase: società di scambio di beni e servizi digitali, fondata nel 2012 e con sede a San Francisco, in California. https://it.wikipedia.org/wiki/Coinbase

[48] Microsoft Corporation: ha sede a Washington, negli Stati Uniti ed è una delle più grandi produttrici di software al mondo per fatturato. fonte https://it.wikipedia.org/wiki/Microsoft

[49] ECDSA: algoritmo crittografico utilizzato dalla rete Bitcoin per garantire che i fondi, ovvero i bitcoin, possono essere spesi solamente dai veri e propri proprietari. fonte https://en.bitcoin.it/wiki/Elliptic_Curve_Digital

[50] Bitcoin address: stringa alfanumerica, associata ad un utente. fonte https://en.bitcoin.it/wiki/Address

[51] Merkle Root: è un codice alfanumerico, facente parte del Merkle Tree, che sintetizza tutte le informazioni delle transazioni del blocco. Il Merkle Tree è un albero dove ogni foglia è etichettata da un codice contenente i dati di un blocco; il Merkle Tree sintetizza i codici hash delle transazioni e i hash della catena. fonte https://en.wikipedia.org/wiki/Merkle_tree

[52] Double spending: è un problema che causa la stessa spesa di soldi più di una volta. fonte https://en.wikipedia.org/wiki/Double-spending

[53] fonte https://it.wikipedia.org/wiki/Crittografia_asimm

[54] fonte https://it.wikipedia.org/wiki/Crittografia_simme

[55] New economy: fase di sviluppo legato alla diffusione delle tecnologie informatiche e digitali dell'ultimo secolo. fonte https://it.wikipedia.org/wiki/New_economy

[56] fonte https://www.btcchina.com/page/bocnotice2013

[57] Commodity: prodotto primario o materia prima che costituisce un fondamentale oggetto di scambio internazionale (es. caffè, petrolio, carbone ..)

[58] In un noto trattato di Paul Krugman si legge la frase "Bitcoin is Evil" perchè manderà in rovina l'intera economia mondiale.

[59] The conscience of a liberal - Paul Krugman https://krugman.blogs.nytimes.com/2013/12/28

is-evil/

[60] https://cointelegraph.com/news/why-krugmans-bitcoin-is-antisocial-and-impractical-argument-is-flawed

[61] http://formiche.net/2013/04/15/krugman-stronca-il-bitcoin/

[62] MtGox: è un Bitcoin Exchange con sede a Tokyo, in Giappone.Nata nel 2010, tra il 2013 ed il 2014 gestiva più del 70% delle transazioni di bitcoin.

[63] Bitfinex: è un Bitcoin Exchange, società di Hong Kong.

[64] https://securelist.it/it-threat-evolution-q2-2015/58672/

[65] Teorema della rovina del giocatore: date le dotazioni iniziali di entrambi i giocatori e una probabilità del 50% di perdita/vincita per entrambi, il presente teorema calcola la probabilità che un giocatore ha di vincere una serie di scommesse fino ad esaurimento

dotazioni dell'avversario. http://www.ripmat.it/mate/l/ld/lde.html

[66] double spending: è un errore che si verifica nei sistemi di pagamento digitali e causa un'anomalia nel sistema delle transazioni, lo stesso importo viene speso più di una volta. https://en.wikipedia.org/wiki/Double-spending