



UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA “GIORGIO FUÀ”

Corso di Laurea triennale in Economia e Commercio

**IL FENOMENO DELLE CRIPTOVALUTE: ANALISI DELLA
LORO ATTUABILITÀ**

THE PHENOMENON OF CRYPTOCURRENCY: ANALYSIS OF THEIR VIABILITY

Relatrice:

Prof.ssa Caterina Lucarelli

Rapporto Finale di:

Cristiano Marini

Anno Accademico 2021/2022

*Alla mia famiglia,
a Giulia
e a tutti i miei amici*

INDICE

Introduzione.....	3
Capitolo 1 – Le criptovalute.....	4
1.1. Caratteristiche e funzioni.....	4
1.2. La blockchain.....	7
1.3. Modelli di moneta virtuale.....	10
1.4. Tipi di criptovaluta.....	12
1.5. Regolamentazione.....	14
Capitolo 2- Il Bitcoin.....	19
2.1. Caratteristiche e funzioni.....	19
2.2. Exchange e commissioni.....	22
2.3. I rischi del bitcoin.....	25
2.4. Regolamentazione.....	28
2.5. Pareri e prospettive della BCE.....	30
Conclusion.....	33

INTRODUZIONE

Con l'avvento della tecnologia sono venute alla ribalta le cosiddette criptovalute, che sono entrate a gamba tesa all'interno del sistema finanziario. In questo testo si andrà ad analizzare il panorama dello stato attuale, delle prospettive, dell'inquadramento normativo, e dell'effettiva attuabilità di quest'ultime all'interno del mercato globale.

Nel primo capitolo si esplorerà cosa sono le criptovalute, quali sono le loro principali funzioni e caratteristiche, la tecnologia fondamentale sulla quale si appoggiano che viene denominata blockchain; si andrà poi ad elencare una lista delle criptovalute più importanti e conosciute. Si conclude con una panoramica generale sulla regolamentazione di esse e i diversi approcci possibili, facendo riferimento alle realtà dei vari paesi Europei e non solo.

Nel secondo capitolo si andrà a trattare il bitcoin che è stata la criptovaluta più mainstream negli ultimi anni, elencandone le principali caratteristiche, i suoi utilizzi più comuni, le funzioni e i relativi rischi connessi: dal suo utilizzo o dalla mancanza di una inquadratura legale e finanziaria; si entrerà poi più nel dettaglio esaminando un eventuale quadro normativo in cui possa essere inquadrata. Infine, si tratterà il punto di vista della BCE sulle criptovalute e sui bitcoin, analizzando il documento da essa pubblicato dove all'interno si può trovare i pareri e le prospettive future riguardo i determinati approcci da adottare.

Capitolo 1

LE CRIPTOVALUTE

1.1. Caratteristiche e funzioni

Il termine criptovaluta è composto da due parole: cripto e valuta. Letteralmente, valuta nascosta. “Si tratta di una moneta digitale in cui le transazioni che vengono effettuate sono verificate e registrate da un sistema decentralizzato che utilizza la crittografia piuttosto che da un’ autorità centralizzata”.¹

Le criptovalute sono staccate dal controllo diretto del governo o della banca centrale, il controllo di ognuna funziona attraverso una *blockchain*, che svolge il ruolo di database pubblico per le transazioni finanziarie. La tecnologia *blockchain* verrà poi ripresa in seguito.

Le criptovalute sono nate per poter superare i limiti delle banche, ovvero il fallimento che provoca una perdita di denaro da parte degli investitori che a sua volta porta ad una grande perdita di fiducia, e per superare i limiti della moneta tradizionale.

Lo scopo fondamentale delle criptovalute è quindi quello di facilitare le transazioni e i trasferimenti confermando la sicurezza tramite la chiave privata o pubblica.

¹ Oyelude, A., 2022, *Cryptocurrency: the future money here now...*, Library Hi Tech News.

Attraverso questo sistema è così possibile ridurre al minimo le spese di transazione rispetto alle commissioni previste dalle istituzioni finanziarie convenzionali.

Le criptovalute vengono conservate in portafogli virtuali che sono chiamati “*wallet*” che possono essere sia *software*, collegati direttamente alla rete e che permettono di immagazzinare numerose valute virtuali; sia *hardware*, collegati solamente quando è necessario svolgere una transazione, come ad esempio le *chiavette usb*.

Si possono così definire questi “*wallet*” come un servizio di *home banking* personale che consente quindi ai possessori di conservare le varie monete virtuali, ma anche di effettuare trasferimenti con altri utenti, ricevere ed effettuare pagamenti, monitorare lo storico in ordine cronologico di tutte le transazioni avvenute e compiere acquisti online sui siti che accettano pagamento in valute virtuali.

Il portafoglio virtuale deve essere collegato ad un indirizzo chiamato “*address*” o anche chiamato chiave pubblica che viene generato automaticamente quando si installa il *wallet* nel computer.

Una volta generato l’indirizzo, che è composto da un insieme di lettere e numeri (stringa alfanumerica in termini tecnici), viene generata una *password* o chiave privata che consente di installare “questo” conto anche su altri “*wallet*”.

La chiave pubblica funziona similmente ad un indirizzo e-mail, quindi può essere condivisa con altre persone in totale sicurezza.

Per chiave privata si intende invece una combinazione di numeri di formato diverso con il fine di separare un utente dagli altri così da creare un codice personale per ogni individuo. Quest'ultima identifica l'identità dell'utente aiutandolo nel commercio con le criptovalute.

In fondo la moneta nasce in primis come mezzo di pagamento e il bitcoin, insieme alle altre valute, vogliono porsi come alternativa ai mezzi di pagamento tradizionali. La criptovaluta non esiste in forma fisica, ma si scambia e si genera in modo esclusivo in via telematica, anche per questo è definita moneta "virtuale".

La criptovaluta, può essere scambiata in modalità *peer-to-peer*, ovvero laddove ci sia un consenso tra i partecipanti relativi a quella determinata situazione, è possibile effettuare l'operazione tra i due dispositivi senza la necessità di essere regolati da intermediari.

Le criptovalute hanno costi di transizione minimi questo è dovuto al fatto che non hanno bisogno di edifici fisici per esistere; quindi, non hanno bisogno di scaricare sulle commissioni: i salari per i dipendenti, le bollette o gli affitti. Permettono inoltre di ridurre i tempi per le transazioni transfrontaliere e velocizzare i trasferimenti di attività finanziarie.

Le monete virtuali poggiano su una forte base fiduciaria, fiducia spontanea che si instaura tramite l'incontro tra domanda e offerta; lo schema che consente di creare queste monete è distribuito nella rete e quindi non appartiene a nessun soggetto singolo, sono così create da un ampio gruppo di partecipanti privati.

Le criptovalute hanno delle caratteristiche particolari che le contraddistinguono. Come prima caratteristica si ha un “protocollo”, ovvero le modalità attraverso le quali i partecipanti possono effettuare transazioni sono stabilite da un insieme di regole.

La seconda caratteristica che contraddistingue le criptovalute è il cosiddetto “libro mastro” anche definito *distributed ledger*, che è il registro contabile che tiene il conto di tutti i bitcoin esistenti e di tutte le transazioni che sono state eseguite; a differenza dei tradizionali *database*, può essere letto e modificato da tutti gli utenti di una stessa rete. È inoltre strutturato come una catena di blocchi (da qui il termine *blockchain*) contenenti le transazioni effettuate, e tutti i *nodi* della rete possono partecipare al processo di validazione delle transazioni da includere nel registro stesso.

La terza caratteristica riguarda una rete di *miners* decentralizzata, che hanno lo scopo di conservare, aggiornare e consultare la blockchain delle transazioni, secondo le regole del protocollo che sono già state stabilite in precedenza.

1.2. La Blockchain

La *Blockchain* (“catena di blocchi”) è la tecnologia alla base di tutte le criptovalute e di tutte le applicazioni decentralizzate. È costituita da un “libro mastro”, ovvero un registro aperto che permette di immagazzinare le transazioni tra gli utenti in

modo sicuro tramite l'utilizzo della crittografia, raggruppandole in blocchi concatenati.

Si definiscono *nodi* coloro che partecipano al sistema e sono connessi tra di loro; ognuno possiede una copia identica del registro così da garantire la presenza di un sistema decentralizzato. In questo modo il controllo dei dati viene distribuito tra i *nodi*, che sono entità indipendenti, e non viene quindi affidato ad una singola autorità come nel caso del sistema centralizzato.² (figura 1.1.)

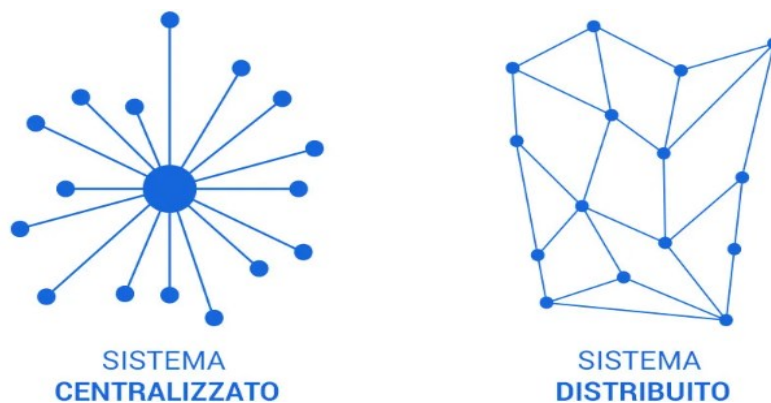


Figura 1.1.

Questo sistema non richiede la fiducia verso l'intermediario o verso il gestore, poiché l'esattezza delle scritture è verificabile costantemente dagli utenti del sistema; la fiducia è affidata così alle regole di funzionamento del software.

² <https://fontidireddito.it/blockchain-come-funziona-tecnologia-base-criptovalute>

La catena dei blocchi è replicata in migliaia di copie, che vengono aggiornate e sincronizzate attraverso aggiunte successive, questo è svolto grazie al lavoro dei *miners* che risolvono calcoli algoritmici molto complessi.

Diversi sono gli elementi distintivi che caratterizzano la *blockchain*.

Innanzitutto, vi è *l'unicità* data dal fatto che la blockchain è l'unico registro fedele per tutti gli operatori e per tutte le transazioni.

Un altro elemento distintivo è *l'indipendenza*, poiché il funzionamento è governato da software e da leggi matematiche, non modificabile e quindi completamente indipendente da gestioni centrali.

Vi è poi *l'irreversibilità* data dalla non modificabilità della sequenza temporale delle transazioni.

Rientra tra gli elementi distintivi della blockchain la *programmabilità*: i software programmano le condizioni di sblocco e il successivo vincolo della moneta.

Un'altra caratteristica della *blockchain* è la *rintracciabilità*, ovvero ogni singolo bitcoin o altra criptovaluta presa in considerazione sono rintracciabili e tracciabili.

In conclusione, si hanno due elementi distintivi fondamentali della *blockchain*: *l'immutabilità e la sicurezza*; ogni qualvolta si aggiunge un blocco di dati nella *blockchain* si innesca un algoritmo matematico che produce un "*hash*" ovvero una chiave crittografata. Il nuovo blocco conterrà così *l'hash* del blocco precedente e

ne genererà uno nuovo, che si andrà ad agganciare al successivo e così via di continuo.³ (figura 1.2.)



Figura 1.2.

1.3. Modelli di moneta virtuale

Nel 2012 la BCE (Banca Centrale Europea) ha classificato le valute virtuali, titolando tale classificazione in “Modelli di moneta virtuale”.

La moneta virtuale può essere suddivisa in: moneta virtuale chiusa, moneta virtuale unidirezionale, moneta virtuale bidirezionale.

Con la moneta virtuale chiusa il collegamento tra la valuta digitale o virtuale e la valuta ufficiale reale è inesistente; ad esempio, le valute dei giochi online appartengono a questo tipo di schema, i giocatori acquistano moneta virtuale con la moneta reale che può essere utilizzata esclusivamente all’interno del gioco per acquistare oggetti virtuali.

Con la moneta virtuale unidirezionale, la moneta virtuale può essere acquistata con denaro reale ad un determinato tasso di cambio, ma una volta comprata non può

³ <https://fontidireddito.it/blockchain-come-funziona-tecnologia-base-criptovalute>

essere riconvertita in valuta reale, da qui l'aggettivo "unidirezionale"; la moneta digitale è usata per comprare beni e servizi che vengono offerti da determinate comunità che accettano quest'ultima. Può anche essere possibile l'acquisto di beni reali con la suddetta moneta virtuale, ne è un esempio Facebook, con i *Facebook Credits*.

Infine, c'è la moneta virtuale bidirezionale: questa può essere scambiata con quella reale e viceversa in modo semplice e viene utilizzata nel mondo come fosse una valuta reale a tutti gli effetti, consentendo l'acquisto di beni e servizi reali e digitali. L'esempio più significativo è quello del bitcoin.

Qui di seguito viene riportato uno schema per semplificare la spiegazione sui "modelli di moneta virtuale"⁴ (Figura 1.3.)

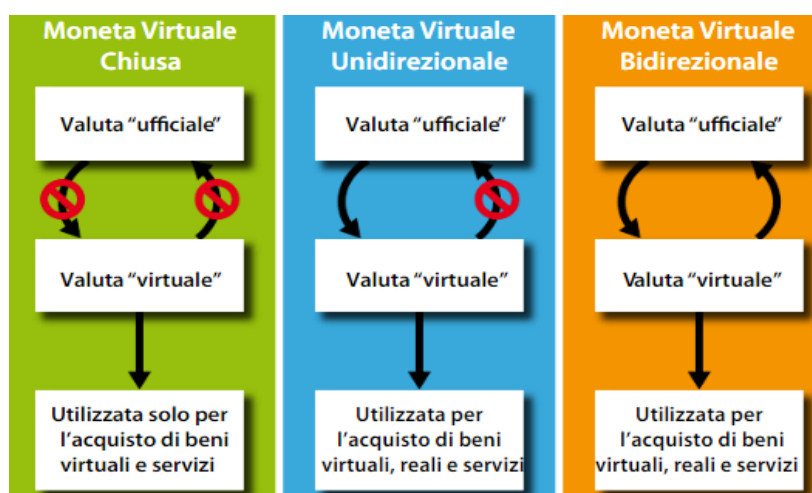


Figura 1.3. Modelli di moneta virtuale

⁴ <https://www.consob.it>

1.4. Tipi di criptovaluta

Diverse sono le criptovalute che si sono maggiormente affermate nel corso degli anni. La moneta virtuale per eccellenza, la prima distribuita a livello internazionale sul mercato finanziario, è il *Bitcoin*. Di questa moneta si parlerà in maniera approfondita nel capitolo II.

Un'altra criptovaluta è *Ether*, introdotta per la prima volta nel 2013 dal programmatore informatico e ricercatore di valute virtuali Vitalik Buteri. È un tipo particolare di criptovaluta poiché è orientata su un sistema speciale della piattaforma Ethereum, basato sulla tecnologia di blockchain. Questa piattaforma permette lo sviluppo di applicazioni decentralizzate, cercando di restituire il controllo delle app agli sviluppatori. Sono gli *smart contract* (in italiano: contratto intelligente) a permettere lo sviluppo di queste applicazioni: questi sono protocolli informatici che rendono possibile l'esecuzione di un contratto, escludendo totalmente o in parte la clausola contrattuale. È la seconda criptovaluta maggiormente capitalizzata seconda solo al Bitcoin.

Litecoin, ideato da Charles Lee nell'ottobre 2011, prende ispirazione e risulta molto simile al Bitcoin; infatti, è nato con il principale scopo di migliorare il Bitcoin, rendendo la transazione più rapida e sicura. Nel tempo ha raggiunto una

capitalizzazione sempre maggiore, arrivando ad essere una tra le criptovalute a più alto valore al mondo.

Fa parte delle criptovalute anche *Ripple (o XRP)*, una valuta digitale che non si basa su un sistema decentralizzato ma su un sistema open source, così da permettere a ciascun sviluppatore di dare il proprio contributo con interventi e modifiche, sempre sulla base di una regolamentazione. È stata progettata nel 2012 dall'industriale Chris Larsen. Facilita i trasferimenti in qualsiasi valuta a qualsiasi richiedente in modo veloce ed economico.

Infine, una delle criptovalute che si sta diffondendo sempre di più è *Binance Coin*, nonostante abbia una storia ben più recente rispetto alle altre criptovalute esaminate. È stata creata nel luglio 2017 ed è la criptovaluta ufficiale di Binance. Binance è il più importante exchange al mondo per la compravendita di criptovalute. *Binance Coin* permette di far ottenere ai propri possessori tutti i servizi di *Binance* con commissioni ridotte e un *cashback* più elevato.⁵

⁵ Hossain, M., S., 2021, *What do we know about cryptocurrency? Past, present, future*, China Finance Review International.

1.5. Regolamentazione

Quello sulle criptovalute è un dibattito ancora aperto nell'ambito finanziario; molte persone sono favorevoli al trading di esse, mentre altre sono in dubbio.

Dal punto degli investitori, Bitcoin, Ethereum e molte altre sono considerate attività rischiose, poiché scambiate con una volatilità molto elevata. Sono presenti limiti che impediscono l'utilizzo delle criptovalute come strumenti di investimento.

Uno di questi riguarda il collegamento sempre più diffuso tra il dark web e le criptovalute, reso possibile dalle caratteristiche di anonimato e digitalizzazione, oltre che dalla loro semplicità nell'utilizzo. Ciò ha aumentato l'utilizzo della moneta digitale per il finanziamento del terrorismo e delle attività criminali, inducendo molti investitori e commercianti a non trattare più con le criptovalute.

La sfiducia degli investitori deriva da una mancanza di trasparenza, ma soprattutto da una scarsa regolamentazione, in alcuni casi completamente inesistente. Per questo è ancora in corso a livello globale una discussione sulla loro regolamentazione e attuabilità.⁶

Altri limiti di queste valute sono la volatilità molto elevata, la frequente perdita di valore e la mancanza di un'accettazione diffusa da parte del pubblico.

⁶ Butler, S. (2019), "Criminal use of cryptocurrencies: a great new threat or is cash still king?", *Journal of Cyber Policy*, Vol. 4 No. 3, pp. 326-345.

Foley, S., Karlsen, J.R. and Putnins, T.J. (2019), "Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?", *The Review of Financial Studies*, Vol. 32 No. 5, pp. 1798-1853.

Il tasso di accettazione delle criptovalute da parte del governo mondiale e delle banche centrali è basso per ragioni simili, ovvero i legami delle criptovalute con le attività legali, la speculazione e la capacità di aggirare i controlli imposti dai governi.

Riguardo alla regolamentazione delle criptovalute tre sono gli approcci esistenti: conservativo, liberale e neutrale.

La regolamentazione conservativa prevede restrizioni e divieti per le criptovalute; è questo il caso di alcuni paesi quali Cina, Sudafrica, Brasile e Kazakistan. Questo approccio proibitivo può avere come effetti negativi la riduzione dei progetti innovativi che coinvolgono le criptovalute e il loro trasferimento in Paesi con giurisdizioni normative più trasparenti. In Cina il governo di Xi Jinping ha vietato le valute virtuali, con il fine di “fermare speculazione, attività criminali, raccolte di fondi illegali e riciclaggio”. Va considerato che la banca centrale di Beijing sta sviluppando una moneta ufficiale digitale, per cui nasce il dubbio che la mossa del governo cinese sia un tentativo mirato per liberare il campo della eventuale concorrenza⁷.

La regolamentazione liberale autorizza le operazioni con le criptovalute; ciò rende possibile l’esenzione fiscale e la riduzione dei requisiti di licenza e di controllo finanziario da parte del governo. Ne è un esempio la repubblica della Bielorussia.

⁷ *Cina, in cosa consiste il bitcoin di Stato: al bando le altre criptovalute*, 2021. Disponibile in: <https://quifinanza.it/>

La regolamentazione neutrale prevede quattro attività: decidere sulla tassazione dei ricavi e delle transazioni, determinare la natura giuridica delle criptovalute, trovare il miglior compromesso nella loro regolamentazione legislativa e individuare l'approccio alla concessione di licenze per le attività dei partecipanti al mercato. La Russia ha adottato questo approccio.

Delle criptovalute si è anche dibattuto in Europa, che sta pensando a un Euro Digitale, che rispetto a criptovalute quali il dogecoin o il bitcoin sarebbe più sicuro, legale e diminuirebbe l'impatto ambientale (dovuto al mining).

Gli strumenti in Europa per poter progettare una valuta virtuale ci sono, tuttavia quello che manca è una volontà della politica; interessante è il dato che è stato desunto dai dati analizzati post-pandemia: nonostante il lockdown e la pandemia abbiano accelerato strumenti di pagamento diversi dal contante, durante la pandemia c'è comunque stato un ritorno al contante. I motivi di questa tendenza non sono facili da comprendere, ma senza dubbio i tassi d'interesse bassi e a volte negativi hanno dato maggiormente al contante la funzione di riserva di valore, considerato quindi come un "bene rifugio". Questo è dipeso anche da una crescente sfiducia economica. Un'altra ipotesi è poi che chi preferisce il contante dia un'importanza maggiore all'anonimato.⁸

⁸ *Che cos'è l'Euro Digitale, quando arriva e quali problemi ci sono*, 2021. Disponibile in: <https://quifinanza.it/>

Le criptovalute hanno avuto un importante impatto sull'economia e sulla società, ne sono un esempio le persone e aziende che stanno prosperando e che sono diventate ricche da un giorno all'altro trovando così opportunità di crescita.

Un altro esempio riguarda quello di Paesi con scarse risorse bancarie che tipicamente ricorrono a prestiti dubbi e pericolosi, ma le cripto essendo talmente volatili e facili da usare colmano questo vuoto rendendo grazie all'uso della tecnologia tutti più connessi e “finanziariamente più forti”.

L'economia si sta pian piano adattando a queste esigenze e a questi cambiamenti, di pari passo le tecnologie sono lo strumento cardine di questa trasformazione.⁹

⁹ Ojih, J., E., 2022, *Crypto-hesitancy: is regulation the answer?* Journal of Indian Business Research.

CAPITOLO 2

IL BITCOIN

Il bitcoin è una delle tante valute virtuali appartenente all'insieme delle criptovalute, è la più grande per capitalizzazione di mercato, nonché il primo asset nella storia a raggiungere una capitalizzazione complessiva di 1 Trilione di dollari in maniera così veloce.

Si tratta di una moneta criptata, moneta la cui esistenza poggia su un algoritmo matematico. È nato nel 2008 durante la crisi finanziaria, ideato da *Satoshi Nakamoto* che attraverso un *white paper* ha stabilito i principi alla base della rete *peer-to-peer* del bitcoin. All'epoca il bitcoin veniva scambiato per pochi centesimi, aumentando nel tempo il suo valore e di conseguenza la sua domanda ha iniziato ad aumentare gradualmente. Nel 2015 il bitcoin è stato scambiato per 290 dollari per poi arrivare nel 2021 al suo valore massimo di oltre 50000 dollari, questo fa capire la grande crescita di valore che ha avuto nel tempo.

2.1. Caratteristiche e funzioni

Come si è già descritto nel capitolo precedente il bitcoin è una moneta virtuale che poggia su una *blockchain*, e su un *protocollo*, in modo tale da fornire determinate regole che danno vita ad un sistema più flessibile, più privato e meno soggetto a controlli normativi rispetto alle altre forme di pagamento tradizionali. In alcune parti del mondo più povere o in via di sviluppo, l'accesso ai servizi bancari

è limitato, favorendo così il bitcoin e altri sistemi simili come strumenti di pagamento a basso costo.

Il bitcoin può essere quindi inteso come il primo meccanismo capace di fornire una “scarsità” di moneta, non avendo un’ autorità centralizzata che lo crei. Di conseguenza il processo di emissione e di creazione di moneta è molto più difficile rispetto ai classici metodi di creazione di moneta e questo porta alla sua scarsità. Questa scarsità protegge dalla contraffazione e permette di poter garantire la correttezza delle registrazioni.

La maggior parte degli utenti trattano i propri investimenti in bitcoin non come mezzi di pagamento ma come attività speculative.

Il bitcoin si basa su tecnologie crittografate come ad esempio: la chiave pubblica e la chiave privata.

Il sistema bitcoin assegna bitcoin in modo periodico a coloro che risolvano la crittografia dietro ai blocchi della blockchain, tramite degli algoritmi matematici. Questo processo è appunto chiamato *mining* e assicura che l’ordine totale su tutti i blocchi (“catena”) sia concordato dalla rete. I minatori così facendo stanno valutando la corretta registrazione delle transazioni e le verificano, per questo loro lavoro (effettuato tramite computer e una procedura molto complicata) venivano ricompensati con 50 bitcoin all’inizio poi 25 fino al 2015 ed infine dopo che sono stati conati 21 milioni di bitcoin, questo ricompensa è scesa a zero.

Il protocollo di bitcoin stabilisce un ritmo controllato per l'espansione della valuta e un limite massimo al numero di bitcoin emessi.

In primo luogo, i bitcoin non dispongono di una struttura di *governance* diversa da quella del software; quindi, non impone a un istituto finanziario o a un altro intermediario di verificare l'identità dell'utente o di controllarlo attraverso liste di controllo o controlli incrociati. In secondo luogo, i bitcoin non impongono divieti sulle vendite di particolari articoli (da qui nasce anche la problematica relativa alle attività illecite); al contrario gli strumenti tradizionali quali carte di credito vietano nel luogo di vendita ogni transazione che sia illegale.

Infine, i bitcoin sono irreversibili ovvero il pagatore non può in alcun modo annullare l'acquisto che sia indesiderato o accidentale; mentre altri metodi di pagamento, come le carte, prevedono questo tipo di procedure, con la possibilità di bloccare il pagamento qualora esso sia avvenuto in modo accidentale o in modo imprevisto. Questo tipo di decisioni sono intenzionali: ovvero nascono dall'intenzione di semplificare la piattaforma bitcoin e riducono la necessità di garanzie centrali, pur però alzando le preoccupazioni per alcuni utenti che si sentono così più vulnerabili.

Quindi l'innovazione principale riconosciuta al bitcoin è senz'altro la sua decentralizzazione, che offre alcuni vantaggi: il primo vantaggio è poter fare a meno di concentrazioni di potere che potrebbero permettere ad un'organizzazione o ad una singola persona di prendere il controllo, un altro vantaggio su cui però c'è ancora

molto da discutere riguarda la questione *privacy* per gli utenti, in quanto non si può prendere di mira un singolo blocco.

La decentralizzazione non si è totalmente realizzata.

Le prime aziende che hanno adottato il bitcoin cercavano un maggiore anonimato e il fatto che ci fosse un'assenza di regole su ciò che poteva essere comprato e venduto; infatti, all'inizio venivano molto usati per la compravendita di stupefacenti e di farmaci soprattutto sul negozio online chiamato *Silk Road*, a cui veniva dato il soprannome di *Ebay illegale* che è stato poi chiuso nel 2013 dal FBI.

I bitcoin sono molto usati anche all'interno dei siti di gioco d'azzardo grazie alla formula dell'anonimo.

Il bitcoin veniva anche utilizzato come strumento per eludere i controlli internazionali sui capitali, spostando all'estero capitali di moneta tramite il cambio in bitcoin.

2.2. Exchange e commissioni

Quando si vuole comprare bitcoin o altre criptovalute il metodo più comune per poterlo fare è passare tramite gli *exchange*, ovvero siti web che permettono agli utenti di scambiare i bitcoin con le valute tradizionali o con le altre valute virtuali.

Ciascun exchange ha la propria offerta di criptovaluta, applica delle commissioni e funziona in maniera differente. Queste società di exchange si pongono a tutti gli effetti come intermediari che permettono di comprare e vendere denaro contro

criptovaluta (o viceversa), al tasso di cambio corrente più le commissioni che variano da sito a sito. Sono a tutti gli effetti i cambi valute dedicati alle criptovalute. Tuttavia, a causa della disparità di prezzo e delle commissioni può verificarsi che il prezzo della criptovaluta vari da sito a sito, o che addirittura si possa acquistare a un prezzo più basso su un exchange “A” per poi rivendere subito ad un prezzo più alto su un exchange “B”.

Questo fenomeno è chiamato arbitraggio e consiste nello sfruttare uno squilibrio di prezzi.

La maggior parte di questi scambi vengono effettuati tramite delle aste molto simili a quelle effettuate per i mercati finanziari tradizionali, con un’applicazione delle commissioni che varia dallo 0,2% fino ad arrivare al 2%. Tuttavia, per poter svolgere questi cambi di valuta è necessario avere un’”infrastruttura” online in grado di far fronte agli attacchi informatici e attacchi da hacker, per questo motivo il numero di exchange di bitcoin è rimasto molto limitato e sono sempre meno quelli che hanno un volume significativo.

Si è molto dibattuto sull’impatto del bitcoin sulle commissioni, il bitcoin potrebbe essere un’alternativa che potrebbe indurre una riduzione delle commissioni applicate dalle reti di carte di credito e di debito. Alcuni rivenditori online hanno già sperimentato questa soluzione, accettando così il ricevimento di pagamenti in bitcoin, riportando degli esiti positivi, tra cui un importante aumento delle entrate ed un aumento degli ordini di medie e grandi dimensioni.

Con il tempo sempre più commercianti hanno optato per adattare i loro siti web in modo da poter accettare il pagamento in bitcoin, ne sono un esempio: siti di viaggi, elettronica, consegna e asporto di ristoranti; rimanendo soddisfatti in quanto l'elaborazione di questi pagamenti in bitcoin erano a basso costo per loro. Tuttavia, lo stesso non si può dire per i consumatori, che rinunciando alle carte di credito perdono così sconti e bonus. Molto spesso i consumatori possessori di bitcoin convertono la moneta virtuale in valuta tradizionale pagando una commissione in media dell'1% per poi poter usare quei soldi per i pagamenti e per poter usufruire così degli sconti e bonus di *cashback* della carta di credito. Un'ulteriore barriera d'intralcio all'utilizzo di bitcoin è la catena dei blocchi che deve registrare ogni singola transazione effettuata in bitcoin e devono venire copiate in tutte le future transazioni, questo deve avvenire anche per pagamenti generici e quindi piccole transazioni.

Quindi se i bitcoin si espanderanno così tanto da includere un'ingente quantità di transazioni quotidiane e di piccola entità si dovrà fare i conti con la memorizzazione di tutte questi pagamenti. L'aggiornamento della catena di blocchi comporta così un ritardo indesiderato rendendo così il bitcoin troppo lento per i pagamenti.

Mentre molte altre persone acquistano bitcoin per tenerli in conto e non per usarli. Oggi la maggior parte dei pagamenti comporta la necessità di convertire almeno una parte in o da bitcoin, aumentando così i costi di transazione; tuttavia, se il pagatore fosse in possesso di Bitcoin e il ricevente decidesse di conservarli piuttosto

che convertirli le commissioni sarebbero relativamente basse: gli unici costi di transizione sarebbero per i *miners* che hanno risolto l'algoritmo dietro il pagamento.

2.3. I rischi del Bitcoin

Ci sono diverse incertezze tuttavia sull'utilizzo del bitcoin, si può avere ad esempio: un *rischio di mercato* che si verifica quando avvengono le fluttuazioni del tasso di cambio tra le altre valute e il bitcoin presso gli exchange.

Un altro rischio riguarda la presenza di *mercati poco profondi*, all'interno del quale un singolo agente che cerca di scambiare grandi quantità di bitcoin non può farlo in modo rapido e senza influenzare il prezzo di mercato.

Un'ulteriore problematica che si viene a creare riguarda la *controparte*, ovvero molto spesso gli *exchange* agiscono come vere e proprie banche, negli ultimi anni sono parecchi i casi di *exchange* a basso volume che una volta aver convertito la valuta in Bitcoin sono fuggiti senza aver dato spiegazioni, un dato mostra che il 46% degli *exchange* che hanno chiuso non hanno rimborsato i propri clienti.

Se gli utenti cercano di spostare i loro bitcoin dal *exchange* e li utilizzano tramite un servizio di portafoglio digitale; sorgono altri rischi, non è un mistero, infatti, che alle volte queste imprese di *exchange* sono create con una finalità criminale informatica, al fine di rubare i bitcoin degli utenti.

Un altro è il *rischio di transazione* legato all'irreversibilità dei pagamenti, ovvero il sistema bitcoin non offre nessuna garanzia per poter bloccare l'invio di essi, anche

se quest'invio avviene per errore o per frode; tuttavia, il venditore e l'acquirente posso comunque accordarsi volontariamente per correggere l'errore, ma il protocollo bitcoin non prevede nessun'azione per recuperare i fondi coattivamente. Al momento della transazione, finché essa non viene aggiunta alla catena dei blocchi non viene dunque cancellata, le transazioni vengono aggiunte alla catena dei blocchi in media ogni dieci minuti, e questo può portare ad: annullare tutte le transazioni registrate in quella versione dei blocchi, quindi la *blockchain* considerata autorevole viene così messa da parte, come deciso dalla maggioranza dei partecipanti; e può portare i partecipanti a spendere due volte i Bitcoin se effettuassero transazioni rapide prima dell'aggiornamento della catena dei blocchi. Dietro a questo problema i ricercatori hanno provato a adottare misure a contrasto, ma tuttavia si è dimostrato la possibilità di attacchi se i bitcoin venissero utilizzati per pagamenti più rapidi di quanto previsto dal progetto.

Si è pensato ad una soluzione per limitare il rischio di transazione, ovvero l'inserimento dei *bitcoin contaminati* all'interno di una lista nera scritta da un insieme di *arbitri* e annunciata pubblicamente così da consentire alla comunità di poter rifiutare i pagamenti in entrata effettuati con bitcoin che appaiono registrati su questa lista.

Queste *liste nere* porterebbero con loro non poche problematiche, prima di tutto si verrebbe a creare la possibilità di rifiutare transazioni già avvenute, trasferendo le perdite ai soggetti che hanno inconsapevolmente accettato bitcoin che poi si sono

scoperti illeciti; un'altra problematica di queste liste nere riguarda la possibilità che si vengano a creare abusi da parte di coloro che le gestiscono; infine, in quanto ogni bitcoin può essere storicamente rintracciato, gli operatori di mercato potrebbero attribuirgli diversi valori di mercato in base al loro rischio di appartenere o meno ad una lista nera, compromettendo così la fungibilità dei bitcoin stessi.

Infine abbiamo il *rischio operativo* che riguarda tutte le azioni svolte da soggetti malintenzionati con *malware* (programmi) per poter entrare in possesso delle credenziali dei portafogli e delle chiavi private. Se la potenza di calcolo della piattaforma bitcoin venisse controllata almeno al 51% si può perdere il controllo del sistema con una seguente crisi di fiducia verso il bitcoin (prende il nome di attacco del 51%).

Rientrano sempre nel rischio operativo gli attacchi di *denial-of-service* ovvero di negazione del servizio; consistono nel tempestare di messaggi e richieste un'azienda con l'obiettivo di renderla più lenta o addirittura inutilizzabile. Gli obiettivi di questi attacchi sono differenti: possono colpire i minatori al fine di impedirgli di verificare e risolvere il blocco e quindi dare un vantaggio agli altri minatori; possono colpire gli *exchange* rendendo difficile l'operatività del servizio e compromettendo la fiducia degli utenti, così da poter chiedere riscatto ai fornitori di questi servizi. Infine la notizia di un attacco può minacciare la fiducia in uno scambio o addirittura nel bitcoin stesso, consentendo così l'acquisto di essi a prezzi più bassi.

Anche la *privacy* tanto elogiata potrebbe essere compromessa, quindi si può mettere nella categoria dei rischi del bitcoin anche il *rischio di privacy*. Le transazioni effettuate in bitcoin molto spesso rivelano nomi reali, per esempio quando i fondi vengono convertiti in valute dalle banche tradizionali o quando i fondi vengono convertiti da valute, oppure quando si effettuano acquisti e vendite che rilevano il proprio nome e indirizzo postale, si può risalire così all'identità dell'utente risalendo a queste fonti.

Infine, il sistema bitcoin è esposto a molti *rischi legali* in quanto si tratta di un sistema ancora oggi poco normato, si tratterà della sua regolamentazione nel seguente sotto capitolo.

2.4. Regolamentazione

Le autorità di regolamentazione hanno messo sotto la lente di ingrandimento il bitcoin e i relativi reati a loro connessi, ovvero: i *crimini specifici del bitcoin*, ad esempio come sopra citati gli attacchi *denial-of-service*, gli attacchi ai *minatori* e agli *exchange*. Tuttavia, far fronte a questi reati non è un compito facile da attuare, perché sono novità e per mancanza di chiarezza su quale giurisdizione o agenzia debba trattare il problema.

Altri reati connessi all'uso del bitcoin sono il *riciclaggio di denaro* e i *crimini facilitati da bitcoin* come l'acquisto o la vendita di beni e servizi illegali.

L'obiettivo di eliminare i reati non è di certo fine a sé stesso, ma è giustificato dall'obiettivo delle autorità di proteggere e tutelare i consumatori. Quest'argomento è diventato sempre più discusso dopo il fallimento nel 2014 della borsa di bitcoin Mt.Gox che ha perso un ammontare di Bitcoin pari a oltre 300 milioni.

L'irreversibilità dei bitcoin non gioca di certo a favore per la tutela dei consumatori, che devono essere informati attraverso le divulgazioni di informazioni per comprendere i prodotti che stanno acquistando.

Ad oggi il bitcoin opera in una zona grigia dal punto di vista legale. Poiché è una nuova tecnologia e quindi le legislature di tutto il mondo si trovano in difficoltà a regolamentarle. I legislatori non avendo a disposizione leggi chiare e specifiche che li regolamenti, sono costretti a considerare le legge già esistenti per valutare se possono essere applicate a questa nuova situazione. Un tribunale statunitense ha stabilito che il bitcoin è una valuta e di conseguenza, è su questo che deve concentrarsi l'analisi legale. Man mano che i Bitcoin acquistano valore e che diventano sempre più conosciuti, i governi hanno iniziato a prenderne atto.

Lo scorso 30 marzo 2022 in Italia è stato presentato un disegno di legge che racchiudeva una serie di disposizioni fiscali riguardanti le valute virtuali con il fine di monitorarle dal punto di vista sia fiscale che in materia di imposte sui redditi.

Il disegno di legge si apre con la definizione di moneta virtuale come rappresentazione di valore digitale, che pur non essendo emessa o garantita da una banca centrale o da un'istituzione pubblica gli viene comunque riconosciuto lo

status di mezzo di scambio e quindi può essere trasferita, memorizzata e scambiata elettronicamente.

2.5. Pareri e prospettive della BCE

La BCE si è espressa su questo argomento pubblicando un documento che valuta i sistemi di valuta virtuale, tra cui il bitcoin; il governo cinese invece ne ha vietato l'uso da parte delle istituzioni finanziarie. Nel rapporto la BCE ha definito la moneta virtuale come: *“un tipo di moneta digitale non regolamentata, emessa e di solito controllata dagli sviluppatori e utilizzata e accettata dai membri di una specifica comunità virtuale”*¹⁰.

Come già visto sopra la BCE ha definito tre modelli di monete virtuali: il modello chiuso, unidirezionale e il modello o sistema bidirezionale.

L'obiettivo della BCE con questo documento è quello di analizzare i problemi che minacciano i compiti della banca centrale, con l'obiettivo di proteggere la stabilità dei prezzi, la stabilità finanziaria e la stabilità del sistema dei pagamenti.

Tuttavia, data la ridotta entità delle transazioni, le valute virtuali e i bitcoin attualmente non rappresentano un rischio né per la stabilità dei prezzi né per sistemi finanziari e di pagamento.

¹⁰ <https://www.ecb.europa.eu/>

Il rapporto della BCE ha posto poi l'attenzione su un ulteriore punto, ovvero le banche centrali devono fare attenzione ai bitcoin e alle valute virtuali in generale, in particolare al loro potenziale rischio di ripercussioni negative sulla reputazione delle banche centrali di controllare l'andamento della moneta e del credito; in caso di incidenti riguardanti le valute virtuali le banche centrali potrebbero essere viste non di buon occhio come le responsabili e incapaci di svolgere adeguatamente il proprio lavoro

Il rapporto stabiliva che, poiché le valute virtuali sono create al di fuori della regolamentazione delle banche centrali, esse hanno il potenziale (non ancora realizzato) di ridurre l'efficacia dei tentativi delle banche centrali di controllare l'andamento della moneta e del credito.

Poiché le valute virtuali come il bitcoin presentano caratteristiche simili ai sistemi di pagamento tradizionali e a causa dei loro potenziali impatti, la conclusione della BCE è stata che queste valute rientrano nelle responsabilità di valutazione delle banche centrali mondiali, rendendo così indispensabile un riesame periodico sulla questione.

Le banche centrali e i governi si troverebbero di fronte a grandi difficoltà se volessero vietare o controllare qualsiasi sistema di valuta virtuale, qualsiasi tentativo di questo tipo verrebbe gravemente ostacolato dalla mancanza di confini geografici.

Nello specifico caso dei bitcoin, non c'è un server o un punto di accesso centrale che possa essere chiuso se le autorità lo ritengano necessario. Sebbene un governo decidesse di vietare bitcoin, attualmente, nessuna istituzione avrebbe la capacità di bloccarli favorendo così la loro continua e costante espansione.

Considerati i potenziali benefici di una rete bitcoin regolamentata, un approccio ostile a questo sistema da parte dei governi sarebbe un errore, l'approccio più probabile e saggio che si potrebbe adottare è quello di cercare di regolamentare le transazioni che avvengono in Bitcoin, piuttosto che il sistema stesso.

Sarebbero tre i motivi per cui i governi non dovrebbero tentare di fermare o mettere fuori legge i bitcoin, ovvero: il primo motivo consiste nel fatto che attualmente i bitcoin non sono illegali secondo i quadri giuridici esistenti in quasi tutti i Paesi; il secondo motivo è che il bitcoin offre significativi vantaggi economici rispetto alle valute e ai metodi di pagamento tradizionali; infine, i governi non hanno attualmente la capacità di colpire direttamente la rete bitcoin.

CONCLUSIONE

In questo elaborato si è vista quindi la nascita, lo sviluppo e soprattutto l'impatto delle criptovalute e specialmente dei bitcoin sul sistema economico-finanziario e sociale. È un fenomeno quello delle criptovalute sempre più sotto gli occhi di tutti e per questo c'è bisogno di una regolamentazione, o almeno di un approccio che non vieti o limiti il loro utilizzo, con lo scopo di tutelare i consumatori e i venditori da possibili crimini economico-informatici.

Per via del loro scopo speculativo e della loro natura di moneta instabile e volatile il bitcoin e le altre criptovalute non hanno molte probabilità di sostituire il sistema di pagamenti esistente, ma si presume che in futuro le transazioni elettroniche aumenteranno significativamente, e se la tecnologia blockchain ridurrà in modo significativo i costi di elaborazione delle transazioni, sarà quasi sicuramente adottata.

Al momento ci sono troppe variabili ancora sconosciute

Qualunque cosa accada in futuro, una cosa rimane certa: il mondo è in continua evoluzione e i governi, le banche e le aziende devono stare al passo con questi cambiamenti se vogliono mantenere le loro posizioni di potere in futuro.

BIBLIOGRAFIA

- Böhme, R., Christin, N., Edelman, B., Moore, T., 2015, Bitcoin: Economics, Technology, and Governancet, Journal of Economic Perspectives, vol. 29, pp. 213-238.
- Butler, S. (2019), “Criminal use of cryptocurrencies: a great new threat or is cash still king?”, Journal of Cyber Policy, Vol. 4 No. 3, pp. 326-345.
- De Bonis, R., Vangelisti, M., I., 2019, Moneta. Dai buoni di Omero ai Bitcoin, Società editrice il Mulino.
- Foley, S., Karlsen, J.R. and Putnins, T.J. (2019), “Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies?”, The Review of Financial Studies, Vol. 32 No. 5, pp. 1798-1853.
- Hossain, M., S., 2021, What do we know about cryptocurrency? Past, present, future, China Finance Review International.
- Oyelude, A., 2022, Cryptocurrency: the future money here now..., Library Hi Tech News.
- Ojih, J., E., 2022, Crypto hesitancy: is regulation the answer? Journal of Indian Business Research.
- Turpin, J., B., 2014, Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework, Indiana Journal of Global Legal Studies, Vol. 21, pp. 335- 368.

SITOGRAFIA

Che cos'è l'Euro Digitale, quando arriva e quali problemi ci sono, 2021.

Disponibile in: <https://quifinanza.it/>

Cina, in cosa consiste il bitcoin di Stato: al bando le altre criptovalute, 2021.

Disponibile in: <https://quifinanza.it/>

<https://fontidireddito.it/blockchain-come-funziona-tecnologia-base-criptovalute>

<https://www.consob.it>

<https://www.informazionefiscale.it/valute-virtuali-criptovalute-disegno-legge-tassazione-monitoraggio-fiscale>

<https://www.senato.it>

<https://www.ilsole24ore.com/>

<https://www.ecb.europa.eu/>

<https://ec.europa.eu/eurostat>

