UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia e Commercio

IL NUOVO MERCATO DEI BITCOIN

BITCOIN'S NEW MARKET

Relatore:
Prof. Alberto Manelli

Rapporto Finale di:
Luca Olivanti

Anno Accademico 2020/2021

INDICE

Bibliografia e Sitografia…….

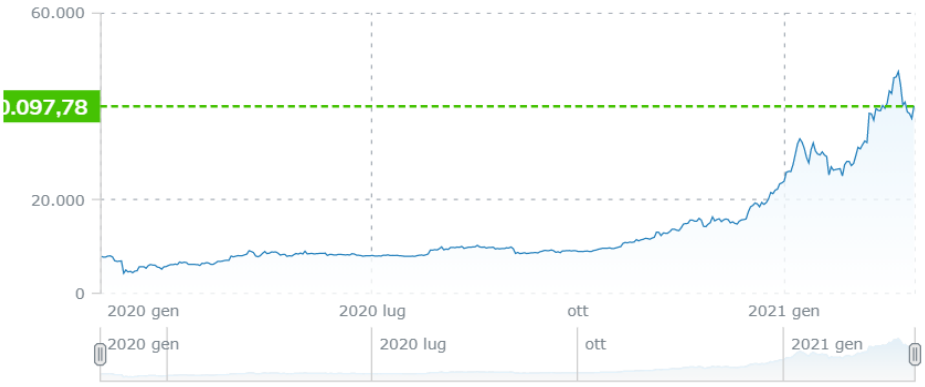
INTRODUZIONE

Come possono essere definiti i Bitcoin? Con il termine Bitcoin stiamo parlando della prima valuta decentralizzata. Questa moneta virtuale è stata creata da un hacker riconosciuto con il nome di Satoshi Nakamoto nel 2009.

Diversamente dalle altre valute il Bitcoin non ha dietro una Banca Centrale che distribuisce nuova moneta ma si basa fondamentalmente su due principi: un network di nodi, cioè di pc, che la gestiscono in modalità distribuita, peer-to-peer; l'uso di una forte crittografia per validare e rendere sicure le transazioni. Si può stimare anche secondo un articolo della Borsa Italiana, che fino a circa un anno fa i Bitcoin disponibili in rete erano 21 milioni[1], mentre quelli effettivamente in circolazione circa 9 milioni. In questo momento il Bitcoin, dopo vari periodi di alti e bassi, assume un valore di 58790.70$ circa, un valore che è comunque sempre in costante mutamento nel tempo.

[1] 21 milioni di Bitcoin disponibili è la quantità stimata sul sito di Borsa Italiana

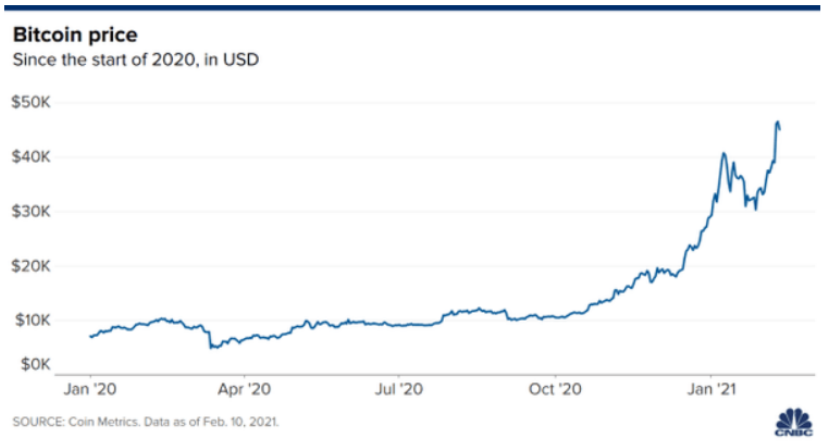
Figura 1 - Esempio della variazione del Bitcoin in un dato periodo di tempo.



*I dati intraday e in tempo reale sono tratti dalle quotazioni di prodotti OTC.

Mentre in questo secondo grafico viene rappresentato l'andamento del Bitcoin nel corso del 2020, possiamo notare una netta risalita a partire dalla fine dell'anno.

Figura 2 – Andamento del Bitcoin nel corso del 2020.



L'andamento del Bitcoin nel corso del 2020. (Grafico targato CNBC-Coin Metrics).

CAPITOLO I

"IL BITCOIN"

I.1 – NASCITA ED EVOLUZIONE DEL BITCOIN

Di date significative per la storia e l'evoluzione del Bitcoin ce ne starebbero veramente tante da ricordare. Da quando venne registrato per la prima volta il dominio bitcoin.org (18 agosto 2008), appena un anno prima della data che risale alla nascita ufficiale della criptovaluta, alla quotazione record di oltre 17mila euro (più di 19mila dollari), raggiunta il 17 dicembre 2017. Una delle date più significative è il 3 gennaio 2009 dove vede la luce il primo blocco di bitcoin. Da allora sono passati oltre 10 anni, segnati da record e speranze per chi ha deciso di investirci. E grande è stato anche il contributo che il bitcoin ha dato all'innovazione e alla finanza, spingendola verso il denaro virtuale e pratiche di sicurezza e trasparenza, grazie alla blockchain, che più avanti analizzeremo, un tempo impensabili. Ma facendo un passo indietro, nel 2009, anno in cui nasce la nuova valuta, il suo valore è di 0,00079 dollari, molto meno di quanto serviva a produrre un solo bitcoin, considerando le spese per computers ed energia elettrica. L'anno successivo avviene il primo acquisto di un bene vero e proprio pagato con moneta digitale crittografata: due pizze al prezzo di 10.000 bitcoin; vede inoltre la luce MT.Gox, il primo sito per scambiare criptovalute. Il 2011, un anno storico per Bitcoin, che raggiunge la parità con il dollaro USA. Nel 2012, Bitcoin

continua a rivalutarsi sui mercati finanziari e per la prima volta fu erogato un finanziamento ad un'azienda basata su blockchain. Alla fine dell'anno un bitcoin valeva 10 dollari, e nel 2013, la crescita sui mercati finanziari è esponenziale, in quest'anno la criptovaluta tocca prima quota 100 dollari e poi raggiunge i 1.000 dollari. L'attenzione sul Bitcoin comincia ad aumentare ed il concetto di moneta criptata inizia a diventare di dominio pubblico; molti store sono disposti ad accettarlo come metodo di pagamento. E' forse l'inizio di una nuova era.

Per la prima volta dalla sua nascita la storia del Bitcoin avrà un risvolto negativo, nel 2014, l'annata peggiore per la nuova valuta, la Cina vieta lo scambio in Bitcoin a tutte le istituzioni finanziarie, per cui diventava illegale ogni transazione in Bitcoin. Un colpo durissimo visto che l'80% degli scambi avveniva in Cina. Non basta, infatti in questo stesso anno chiude il sito MT.Gox, che dichiarò bancarotta a seguito del più grande attacco hacker di criptovalute, in cui furono rubati 750.000 bitcoin di clienti e 100.000 di aziende. Il 2015 però sembra dare il via ad una risalita, si riconsolida la fiducia verso le divise virtuali e Bitcoin, grazie soprattutto alla tecnologia blockchain che comincia a farsi strada e ad interessare aziende e investitori. La moneta digitale principale chiude l'anno con un valore di 400$. L'anno successivo inizia come si conclude il precedente, l'effetto degli investimenti si sente, il mercato si espande e l'ecosistema Bitcoin fondato su blockchain diventa più sicuro. Le quotazioni sui mercati speculativi superano di nuovo la soglia dei 1.000 dollari ed inoltre aumenta l'attenzione dei traders

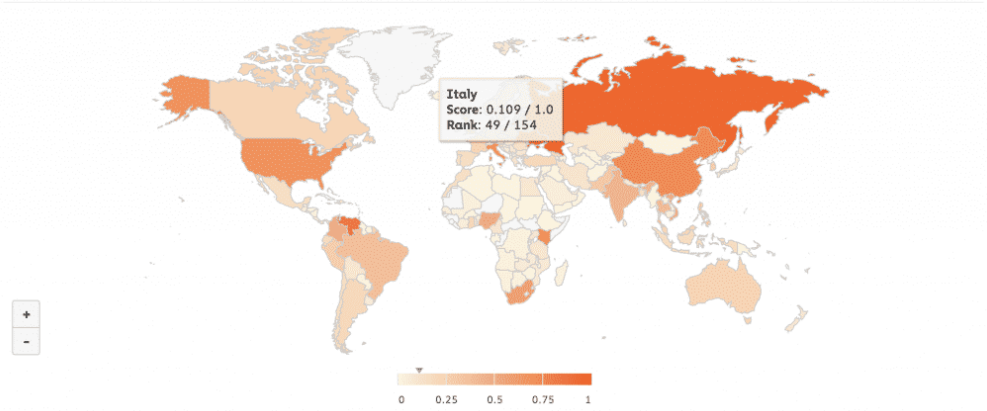
privati. Nell'anno 2017, Bitcoin vive un'incredibile impennata dei prezzi che porterà il suo valore a oltre 4.000$ prima e a sfiorare i 20.000 dollari a fine anno. Si intensifica, di conseguenza, l'interesse mediatico che oramai è concentrato su questo fenomeno economico. Le dinamiche del mercato di Bitcoin investono piccoli, medi e grandi operatori. Già da inizio 2018, il valore di Bitcoin attraversa un'ondata ribassista, importante sebbene le quotazioni si siano prima assestate sopra i 4.000$, superando ripetutamente poi i 9.000$. La tecnologia che sostiene la principale divisa digitale si inserisce in ambiti alternativi al solo comparto economico e raggiunge aspetti sociali e produttivi della vita delle persone. Infine dal 2019 fino ai giorni nostri, possiamo dire che, Bitcoin risulta una delle innovazioni finanziarie più chiacchierate, e anche più rilevanti dell'ultimo decennio. La criptovaluta ha una specifica valutazione, che varia nel tempo, e che può aumentare o diminuire a seconda dell'andamento del mercato. La moneta digitale non é semplicemente uno strumento finanziario da sfruttare nel trading per il suo valore volatile, ma viene anche convertita in altre valute virtuali per fare acquisti. Quindi tra alti e bassi, il Bitcoin con una storia poco più che decennale, è riuscito a ritagliarsi una posizione importante, soprattutto in questi ultimi anni in cui possiamo notare un'ascesa dirompente ai vertici dell'economia mondiale, con valori che nel lontano 2009 potevano sembrare pura utopia.

I.2 – DIFFERENZE RISPETTO ALLA MONETA TRADIZIONALE

Qualunque sistema monetario in uso è caratterizzato da molteplici differenze rispetto al Bitcoin, quest'ultimo infatti presenta notevoli diversità rispetto alle valute a corso legale che usiamo normalmente tutti i giorni. Le banche centrali possono stampare e mettere in circolazione a volontà le loro valute a corso legale, facendo questo provocano la svalutazione del loro valore. Il numero di Bitcoin che si possono invece produrre, non può essere deciso da nessuno, dato che la quantità totale di Bitcoin che si potranno creare è definito da regole matematiche che sono state programmate durante la sua creazione; questa quantità equivale a 21 milioni di Bitcoin, cifra che si raggiungerà nell'anno 2140 e non si potrà superare. Un altro motivo di notevole rilevanza che rende questa nuova moneta digitale così differente è la sua decentralizzazione, cioè non dipende da un ente centrale che la controlla, ciò significa, in poche parole, che mentre una Banca registra tutti i movimenti e i trasferimenti di denaro in un database che si trova in un server specifico, i movimenti del Bitcoin vengono invece registrati in un database gigante denominato Blockchain o catena di blocchi, che non si trova in un solo luogo come nel caso delle banche, ma in migliaia di computer che appartengono a persone differenti, che offrono la loro potenza per mantenere questa rete attiva e sicura. Fra le possibilità che offre il Bitcoin c'è quella di permettere alle persone nei paesi in via di sviluppo, che non hanno la possibilità di accedere ad un servizio bancario, di poter partecipare all'economia mondiale

senza la necessità di ricorrere ad un'entità bancaria; è sufficiente avere a disposizione un dispositivo intelligente come un cellulare per poter effettuare pagamenti utilizzando Bitcoin e poter comprare prodotti e servizi che fino a quel momento risultano inaccessibili per loro. Secondo le statistiche[2], ci sono più di 2000 milioni di persone che non hanno accesso al sistema bancario nei paesi in via di sviluppo, l'uso del Bitcoin risolverebbe questo grande problema umanitario permettendo alle aziende di poter offrire i loro prodotti a queste persone e nei mercati finora vergini.

Figura I.2: Mass Adoption Bitcoin.



Nella figura I.2 possiamo osservare come dei Mass Adoption Bitcoin, ovvero i paesi leader, fanno parte parecchi paesi in via di sviluppo, ad eccezione dei colossi

[2] Statistiche offerte dalla Banca

Russia, Cina, Usa, come Ucraina (che si è piazzata al primo posto), Venezuela, Kenya, Sud Africa, Nigeria, Colombia e Vietnam. Come precedentemente analizzato è evidente che il settore del Bitcoin è particolarmente attivo nei paesi in via di sviluppo, ad esempio i venezuelani utilizzano le criptovalute come uno strumento di risparmio, vista l'incertezza economica che regna nel paese latino-americano.

CAPITOLO II

"CARATTERISTICHE E FUNZIONAMENTO"

II.1 – COME OTTENERE BITCOIN?

Ci sono diversi modi per ottenere dei bitcoin, alcuni semplici ed immediati, altri che richiedono un po' più di tempo ed organizzazione. Sono in continua crescita gli esercizi commerciali, sia fisici che online dove si possono spendere. Tuttavia, prima di pensare a come ottenere e spendere dei bitcoin è necessario mettersi nelle condizioni di poterli ricevere, e una volta ricevuti di poterli tenere al sicuro, senza rischiare di perderli o di farseli "rubare". A questo scopo è necessario possedere un Wallet Bitcoin, un portafoglio elettronico che, molto metaforicamente, svolge le stesse funzioni di un portafoglio materiale, cioè di custodia del nostro denaro che in questo caso è digitale.

I portafogli Bitcoin custodiscono le chiavi private dell'utente, che gli permettono di spendere i bitcoin associati al preciso indirizzo che deriva dalla chiave pubblica che a sua volta deriva dalla chiave privata in oggetto; questo è ciò. Infatti il Wallet offre all'utente un'interfaccia intuitiva, che gli permette di visualizzare il bilancio di bitcoin a sua disposizione di tutti gli indirizzi diversi che egli possiede, dandogli la possibilità di effettuare delle transazioni in uscita verso determinati beneficiari, o di ricevere dei pagamenti ad un determinato indirizzo.

Esistono diversi tipi di portafogli tra cui scegliere, a seconda dei livelli di praticità, sicurezza e complessità desiderata:

Paper wallet: in parole semplici, un portafoglio di carta è un documento che memorizza l'indirizzo Bitcoin e la chiave privata, che vengono utilizzati per inviare e ricevere Bitcoin. È abbastanza semplice usare un portafoglio di carta in quanto è sotto forma di un codice QR che può essere facilmente scansionato. Il paper wallet genera la chiave privata in formato cartaceo, ciò significa che nessuno può attaccarlo o hackerarlo.

Questi sono i portafogli più utilizzati, in quanto queste chiavi sono offline. Ciò rende quasi impossibile per i truffatori attaccare le chiavi stampate. È ancora fondamentale adottare misure preventive per evitare qualsiasi tipo di attacco dannoso o hack.

Desktop wallet: sono i portafogli che devono essere installati sul computer, cioè i portafogli desktop. Questi portafogli memorizzano le chiavi private su un disco rigido. Rispetto ai portafogli mobili e online, i portafogli desktop sono considerati più sicuri. Questi sono necessari per essere connessi a Internet ma non includono terze parti per controllare le chiavi private. I vari tipi di portafogli desktop includono Exodus, Atomic Wallet, Electrum e altri.

Web wallet: sono i portafogli gestiti con una connessione Internet. Questi portafogli memorizzano le chiavi private sul server e terze parti controllano le

chiavi private. Esistono diversi tipi di portafogli web che forniscono diverse funzionalità che possono essere collegate a portafogli desktop e mobili.

Il principale svantaggio dei portafogli web è che questi sono sempre online e sono controllati da terze parti. È imperativo proteggere correttamente le chiavi come se non fosse stato fatto; può consentire l'accesso a chiavi private a terzi. In questi casi, si potrebbero perdere tutti i Bitcoin.

Mobile wallet: i trader che commerciano o investono regolarmente in Bitcoin, richiedono uno strumento facile. Lo strumento più essenziale e facile per fare trading di Bitcoin è un portafoglio mobile. I portafogli mobili possono essere eseguiti su tablet o smartphone ed è utile per memorizzare la chiave privata sul telefono e pagare direttamente a chiunque. Questi portafogli sono compatibili con gli utenti Android e iOS.

Indubbiamente, i portafogli mobili sono la soluzione migliore per gli utenti regolari, ma anche questi portafogli sono soggetti ad attacchi e virus. Una volta perso il controllo sul proprio dispositivo mobile, andranno persi tutti i Bitcoin e non ci sarà più modo di recuperarli.

Figura II.1: esempio di Paper Wallet

Possono esserci diversi modi per ottenere Bitcoin: possiamo acquistarli da persone disposte a venderli, ad esempio attraverso un sito chiamato “localbitcoins.com” che ha la funzione di mettere in contatto chi vuole vendere bitcoin con chi li vuole comprare e viceversa, quindi rappresenta la piattaforma leader del servizio di scambio face-to-face. Chi vuole comprare dei bitcoin può decidere se effettuare lo scambio online, scegliendo il metodo di pagamento prescelto (bonifico bancario, paypal, postepay, ...), oppure è possibile accordare un incontro fisico con il

venditore e scambiare bitcoin in cambio di contanti, in quanto si possono trovare offerte anche relativamente vicine in termini geografici.

Acquistarli presso gli Exchange online: sul web esistono molti siti che consentono la compravendita di bitcoin in cambio di moneta legale o di altre criptovalute. Tali piattaforme svolgono il ruolo di market makers fissando i tassi di cambio a cui l'Exchange compra o vende bitcoin in cambio delle principali valute tradizionali o di altre valute virtuali.

Bitcoin ATMs: un servizio di acquisto o vendita molto più rapido rispetto agli exchange online è offerto dai Bitcoin ATMs (o Bancomat Bitcoin). Il primo bancomat bitcoin, prodotto dall'americana Robocoin, è stato installato nell'ottobre 2013 presso la Waves Coffee House di Vancouver, Canada, e già nel suo primo giorno di funzionamento ha registrato ben 81 transazioni per un valore totale di oltre 10.000 $.

Oppure infine è possibile vendere beni e servizi in cambio di Bitcoin, attualmente in Italia, questa opzione è più facilmente percorribile da chi conduce un esercizio commerciale. Sono sempre più numerosi i negozi, sia fisici che online, che accettano pagamenti in bitcoin in cambio di beni e servizi.

II.2 – TECNOLOGIE RELATIVE AL BITCOIN

Le tecnologie relative al funzionamento del sistema dei Bitcoin non sono in realtà un'innovazione bensì una "fusione" o combinazione di altre tecnologie già esistenti.

In questi brevi paragrafi che seguono saranno esposte e spiegate le tecnologie più importanti e fondamentali alla base del funzionamento del Bitcoin.

II.2.1 – Crittografia

La crittografia è una tecnica utilizzata per salvaguardare i dati ed impedire a terzi non autorizzati di accedere o alterare informazioni preziose a proprio vantaggio o a danno di altri.

Oggi, la crittografia è uno dei pilastri fondamentali su cui si basa la tecnologia blockchain; quest'ultima permette il funzionamento della rete e garantisce i meccanismi di consenso tra gli utenti e l'integrità della blockchain.

Per garantire che nessuno di esterno possa accedere ai dati, si utilizzano la crittografia a chiave pubblica (crittografia asimmetrica) e la crittografia a chiave segreta (crittografia simmetrica). La crittografia a chiave pubblica genera un hash che semplifica la distribuzione delle informazioni mentre la chiave privata, crittografa e decrittografa le informazioni tra mittente e destinatario.

In Bitcoin, la chiave pubblica viene ottenuta dalla chiave privata, ma è impossibile eseguire il processo inverso. Vale a dire, non è possibile ottenere la chiave privata

dalla chiave pubblica. La chiave pubblica, dopo successive modifiche, è l'indirizzo che possiamo condividere con tutti i membri della community in modo che possano inviarci denaro, o quella di altri utenti della comunità che useremo all'occorrenza per effettuare un pagamento a loro favore. Non c'è rischio di furto, poiché i fondi sono accessibili solo tramite la chiave privata.

La chiave privata è simile a un PIN o una password che utilizziamo per accedere a diverse pagine Web, ma in questo caso è crittografata, quindi dà molta più sicurezza. Questo significa che inserendo una serie di termini o parole e questi verranno crittografati e proteggeranno il wallet o portafoglio . Solo chi li inserisce possiede queste parole, quindi vanno conservate al sicuro e non vanno condivise con nessuno; in questo modo è possibile accedere ai propri fondi in qualsiasi momento.

Come precedentemente detto la crittografia può essere simmetrica o asimmetrica a seconda del tipo di chiave utilizzata. La crittografia simmetrica, che è stata utilizzata sin dall'inizio della storia e per molto tempo, è anche chiamata crittografia a chiave privata o crittografia a una chiave. Per portarla a termine e per farle crittografare e decrittare un messaggio, viene utilizzata un'unica chiave, che sia il mittente che il destinatario devono preventivamente conoscere. Questo è il punto debole di questo metodo, poiché è più probabile che la chiave venga intercettata da una terza parte quando il mittente la trasmette al destinatario. Nella crittografia simmetrica deve essere utilizzata una chiave molto difficile da

indovinare, perché i computer di oggi possono indovinare le password molto rapidamente. Dobbiamo quindi considerare che, poiché gli algoritmi crittografici sono pubblici, è necessario garantire che la loro forza dipenda dalla loro complessità interna e dalla lunghezza della chiave utilizzata, per evitare attacchi forzati.

La crittografia asimmetrica fa uso di due chiavi, una pubblica e una privata, non è quindi necessario conoscere già una password. La chiave pubblica può essere inviata e resa nota a chiunque, mentre la chiave privata è quella che non deve essere condivisa con nessuno. Quando un mittente desidera inviare un messaggio, utilizza la chiave pubblica per crittografare il messaggio e lo invia e solo il destinatario con la sua chiave privata può decrittografare il messaggio. La crittografia asimmetrica fornisce un livello di sicurezza straordinario, al punto che nemmeno la persona che ha criptato il messaggio può decriptarlo senza la chiave privata. Questo è il metodo utilizzato nelle criptovalute, ed è un tassello fondamentale nella blockchain per poter svolgere operazioni e scambiare informazioni tra pari in totale sicurezza e senza la necessità di fidarsi l'uno dell'altro.

Figura II.2.1: Crittografia, la sicurezza alla base delle blockchain.

II.2.2 – Rete peer to peer

Una rete peer-to-peer (spesso abbreviata P2P), dal punto di vista informatico è una rete caratterizzata dall'assenza della struttura gerarchica tipica dei sistemi client/server e nella quale ciascun nodo (detto servent) può operare come client o come server a seconda delle circostanze.
Un nodo può essere rappresentato da un computer, da uno smartphone o da un qualsiasi altro elaboratore elettronico in grado di far girare il software necessario per la connessione alla rete.

Nei sistemi client/server i computer client comunicano tra loro sempre passando attraverso il server centrale. I computer coinvolti in una rete peer-to-peer, invece, vengono considerati nodi paritari (in inglese peer significa, appunto, paritario). Le reti peer-to-peer serverless differiscono da quelle cosiddette ibride, nelle quali è comunque necessaria la presenza di server per svolgere un limitato numero di compiti.

Storicamente le reti peer-to-peer sono legate al fenomeno del file sharing, ovvero la condivisione di file all'interno di una rete (come Internet, ad esempio).

Una delle componenti critiche delle applicazioni P2P è rappresentato dall'indice delle informazioni, che tiene nota della posizione di tali informazioni nei vari host (terminali collegati alla rete).

Da questo punto di vista le directory centralizzate sono probabilmente molto pratiche, ma possono costituire un collo di bottiglia per le prestazioni della rete e anche un punto debole facilmente attaccabile.

In alternativa esiste l'approccio distribuito, chiamato query flooding, dove l'indice è completamente distribuito ciascun nodo della rete indicizza unicamente i file che rende disponibili alla condivisione. Quindi i vari nodi effettuano una certa richiesta inoltrandola ai nodi vicini, i quali a loro volta faranno lo stesso, finché la ricerca non è soddisfatta.

Questo procedimento presenta comunque dei problemi di scalabilità e di utilizzo delle risorse.

Nel corso degli anni sono diversi i protocolli di trasmissione dati che sono stati studiati per condividere file anche di grandi dimensioni attraverso Internet. Attualmente il protocollo P2P più utilizzato è probabilmente BitTorrent.

II.3 – BLOCKCHAIN

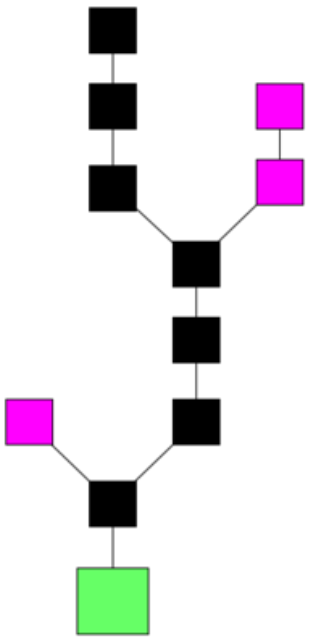
La blockchain (letteralmente "catena di blocchi") è una struttura dati condivisa e "immutabile". È definita come un registro digitale le cui voci sono raggruppate in "blocchi", concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia. Sebbene la sua dimensione sia destinata a crescere nel tempo, è immutabile in quanto, di norma, il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura.

Tali tecnologie sono incluse nella più ampia famiglia delle Distributed Ledger, ossia sistemi che si basano su un registro distribuito, che può essere letto e modificato da più nodi di una rete. Non è richiesto che i nodi coinvolti conoscano l'identità reciproca o si fidino l'uno dell'altro. Difatti, per garantire la coerenza tra le varie copie, l'aggiunta di un nuovo blocco è globalmente regolata da un protocollo condiviso. Una volta autorizzata l'aggiunta del nuovo blocco, ogni nodo aggiorna la propria copia privata: la natura stessa della struttura dati garantisce l'assenza di una sua manipolazione futura. Le caratteristiche che accomunano i sistemi sviluppati con le tecnologie Blockchain e Distributed Ledger sono digitalizzazione dei dati, decentralizzazione, disintermediazione, tracciabilità dei trasferimenti, trasparenza/verificabilità, immutabilità del registro e programmabilità dei trasferimenti.

Grazie a tali caratteristiche, la blockchain è considerata pertanto un'alternativa in termini di sicurezza, affidabilità, trasparenza e costi alle banche dati e ai registri

gestiti in maniera centralizzata da autorità riconosciute e regolamentate (pubbliche amministrazioni, banche, assicurazioni, intermediari di pagamento, ecc.).

Figura II.3 – Rappresentazione della blockchain con i blocchi della catena principale (blocchi neri), con il blocco di genesi (blocco verde) e i blocchi orfani (blocchi viola).



II.4 – MINING

Il termine mining significa scavare, estrarre e viene dalla parola inglese “mine”, che significa anche miniera. Questa felice espressione spiega alla perfezione il funzionamento del mining, che consiste nella creazione di monete virtuali tramite

un duro lavoro informatico che sfrutta la capacità di calcolo dei computer invece della forza fisica di un minatore.

Tutto inizia nella blockchain, il libro mastro della contabilità delle criptovalute. Qui vengono annotate tutte le transazioni di Bitcoin, Ethereum, Ripple e tutte le altre criptomonete. Per aggiungere una transazione alla blockchain è necessario crittografarla e convalidarla con una funzione di hash, che richiede una serie di calcoli lunghi e complessi.

Questi calcoli vengono eseguiti dai sistemi informatici dedicati al mining di bitcoin, su cui sono installati programmi specifici come BitMinter[3]. Normalmente, questi sistemi sono composti da diverse CPU e GPU collegate in serie. Ogni volta che il sistema completa un'operazione o una parte di essa, la rete crea una certa frazione di Bitcoin nuovi che viene accreditata al miner, ovvero il possessore del computer o della farm dedicata al mining.

In parole povere, i miner di bitcoin lo fanno per lavoro, per guadagnarci, e non appartengono a una rete no profit o una banca centrale delle criptovalute. Di fatto, questo sistema è stato pensato proprio per fare a meno di un organismo di controllo centralizzato, sfruttando i vantaggi delle reti peer to peer.

Il bitcoin mining è stato progettato dai creatori delle criptovalute in modo da diventare sempre più complesso con il passare del tempo, affinché l'aumento

[3] Bitminer è la soluzione migliore di software di mining Bitcoin, è compatibile con Windows, Mac Os X e Linux, inoltre non richiede nemmeno installazione

della valuta disponibile nel mercato sia proporzionale al suo valore e alla difficoltà di reperibilità (in questo caso anche di produzione).

Calcoli più complessi richiedono computer più potenti e più energia elettrica consumata. Basti pensare che nel 2019 si è stimato che il consumo di elettricità del Bitcoin mining mondiale equivaleva a quello della Svizzera, e da allora non ha smesso di aumentare!

Attualmente, per produrre 1 BTC sono necessarie moltissime ore di lavoro di decine di computer potenti collegati in rete.

Figura II.4 – Bitminer Factory rappresenta la prima esperienza nel nostro paese di produzione di criptovalute su scala industriale

CAPITOLO III

"DATI A CONFRONTO"

III.1 – VANTAGGI

Utilizzare Bitcoin come moneta alternativa alle valute tradizionali presenta, come è facile intuire, vantaggi ma anche svantaggi. Importanti vantaggi che ne derivano possono essere: costi e tempi di transazione molto bassi, i pagamenti in bitcoin sono costantemente processati senza costi oppure con addebiti estremamente bassi. Gli utenti possono accettare di pagare delle commissioni che sono generalmente intorno ai 0,02€, quando eseguono una transazione, per aumentare la velocità di elaborazione, che si traduce in una conferma più rapida della stessa, esistono anche dei programmi commerciali, ideati per agevolare i commercianti nell'elaborazione delle transazioni, convertendo bitcoin in moneta e depositando fondi direttamente nei conti bancari dei commercianti. Si tratta di servizi che vengono offerti a costi molto più bassi di quelli offerti con PayPal o dalle carte di credito. Inoltre, le transazioni sono molto veloci, infatti una transazione impiega in media 10 minuti per essere registrata nella blockchain, ottenendo una conferma iniziale, tuttavia è consigliato attendere circa 6 conferme, per un totale di un'ora di tempo.

Un fattore che ha sicuramente influito nell'ascesa del Bitcoin è la facilità e l'accessibilità, infatti utilizzarlo è semplice e alla portata di tutti, chiunque in

qualsiasi momento può creare un indirizzo e ricevere dei pagamenti da qualunque parte del mondo senza dover possedere alcun conto corrente bancario, inoltre non essendoci nessuna autorità di controllo che possa congelare i fondi o imporre qualunque tipo di limitazione, ognuno ha il più totale controllo del proprio denaro. Un altro importante vantaggio è sicuramente la trasparenza e neutralità: tutte le informazioni riguardanti i movimenti di bitcoin sono prontamente disponibili sulla blockchain a chiunque, per verifica e utilizzo in tempo reale. Nessun privato e nessuna organizzazione possono controllare o manipolare il protocollo Bitcoin, perché la sua sicurezza è garantita dall'uso della crittografia.

III.2 – SVANTAGGI

Uno degli svantaggi più importanti che caratterizza il Bitcoin è certamente la sua volatilità, infatti la forte volatilità che caratterizza il prezzo del Bitcoin è la principale attrattiva per coloro che li detengono a scopo speculativo ma un problema per tutti gli altri utilizzatori. Le continue fluttuazioni del prezzo rendono troppo rischioso detenere unità di Bitcoin e di conseguenza c'è uno scoraggiamento generale nell'abbandono delle vecchie monete tradizionali in favore del Bitcoin. Anche i commercianti, che li accettano in cambio di beni e servizi, avranno difficoltà a fissare i prezzi di tali beni in Bitcoin e inoltre dovranno stare sempre attenti alle fluttuazioni, cioè potrebbe capitare ad un venditore di vendere un prodotto ad inizio giornata per un certo ammontare di

Bitcoin, e ritrovarsi a fine giornata un valore completamente diverso, sia in aumento che in diminuzione naturalmente.

In aggiunta a quanto precedentemente detto, è chiaro che vige un mancato riconoscimento sociale a livello globale, molte persone sono ancora inconsapevoli dell'esistenza del Bitcoin. Ogni giorno, sempre più aziende accettano i bitcoin, volendone trarre dei vantaggi, ma la lista resta piccola e ha ancora bisogno di crescere, per poter beneficiare degli effetti della rete.

Purtroppo, oltre a questi importanti fattori già elencati, si vanno ad aggiungere componenti negative come l'irreversibilità delle transazioni, ovvero quando un utente invia dei Bitcoin ad un determinato indirizzo e la transazione viene processata e già registrata nella blockchain non è possibile annullarla; oppure la regolamentazione legale e fiscale del Bitcoin che non si presenta omogenea ma varia da nazione a nazione. Addirittura, ci sono stati in cui effettuare transazione di valuta Bitcoin è illegale e penalmente perseguibile come Ecuador, Bolivia e altri paesi del Nord Africa e Asia, che sono attualmente i paesi più avversi.

Figura III.2 – Nella seguente mappa possiamo individuare, come già espletato nel paragrafo precedente, come uno svantaggio lampante sia il mancato riconoscimento sociale a livello globale, infatti sono pochi i paesi raffigurati come "green" cioè dove il bitcoin viene riconosciuto legalmente, mentre invece sono molti i paesi che hanno delle limitazioni a riguardo o che non sono regolamentati.

CONCLUSIONI

Dalle analisi svolte e dalle argomentazioni trattate risulta che dal 2009, anno di nascita del Bitcoin, si è fatto un notevole passo in avanti nel mondo dei mercati internazionali.

Possiamo tranquillamente considerare il Bitcoin una valida alternativa alla moneta tradizionale, ma oltre ad avere notevoli benefici, anche innovativi, ha purtroppo anche dei lati negativi che difficilmente la vede, anche in ottica futura, come unica moneta del mercato. In parole povere è difficile attuare una previsione in cui la moneta unica in utilizzo sarà il Bitcoin che avrà sostituito la moneta tradizionale al 100%.

Tantissimi economisti, giornalisti, scrittori e tante altre personalità di spicco si sono pronunciate in materia, ad esempio Bill Gates[4], fondatore di Microsoft, si pronunciava così a riguardo: "Bitcoin è meglio della moneta in quanto non dovete essere fisicamente nello stesso posto e, prevedibilmente, per le transazioni di grandi dimensioni, la moneta può diventare piuttosto sconveniente… C'è molto che il Bitcoin o le sue varianti possono fare per rendere più facile il movimento di soldi tra i paesi e per far abbassare molto le tariffe. Ma il Bitcoin non sarà il sistema dominante. Quando si parla di economia personale, è rassicurante sapere che se invii denaro alla persona sbagliata, puoi effettivamente recuperare la

[4] Bill Gates si esprime in tal modo durante un'intervista rilasciata a fine 2014; dopo tante altre varie argomentazioni rilasciate a Forbes.

transazione. E un sistema tradizionale non ha queste enormi oscillazioni in cui il valore del tuo portafogli va su e giù. Abbiamo bisogno di cose che si basino sulla rivoluzione del Bitcoin, ma il Bitcoin da solo non è abbastanza buono". Così definiva il nuovo colosso dell'economia Bitcoin, il leader di Microsoft, un'analisi chiara e attenta, ma che per quanto coincisa, non lascia spazio ad un'interpretazione soggettiva, Bitcoin, al momento ha ancora dei limiti importanti. E' possibile osservare anche un'ulteriore importante intervista rilasciata da Richard Branson[5], fondatore del gruppo Virgin che vede il Bitcoin in modo leggermente diverso rispetto a Bill Gates, nel 2017 così si esprimeva "Beh, penso che funzioni. Ci possono essere altre valute simili che potrebbero essere ancora migliori. Ma nel frattempo, c'è una grande industria attorno a Bitcoin. Alcune persone hanno fatto fortuna col Bitcoin, alcuni hanno perso i soldi. È volatile, ma la gente fa soldi anche con la volatilità ". Insomma parole importanti di grande stima verso un progetto che sembrava funzionare 4 anni fa, ma che alla luce dei fatti, nel 2021 sta scalando numeri su numeri, infatti nell'ultimo anno Bitcoin ha raggiunto un valore elevatissimo dopo qualche sali-scendi.

Infine, possiamo notare un diretto collegamento del Bitcoin anche ad uno dei settori dove circola più denaro cioè il mondo del calcio, infatti negli ultimi anni si sta legando sempre di più, al mondo del Bitcoin. Guardando una partita del

[5] Richard Branson ha rilasciato le seguenti dichiarazioni a Forbes nel luglio del 2017, occasione in cui Branson e il gruppo Bitfury hanno ospitato un "esclusivo" ritiro Bitcoin e blockchain su Necker, l'isola privata di Branson Necker.

Watford in Premier League quest'anno si può senz'altro notare una B con due stanghette, simili a quelle del simbolo del dollaro sulla manica dei giocatori, quella B è il simbolo dei Bitcoin.

Come dichiarato dalla società inglese, la sponsorizzazione ha l'obiettivo di rendere sempre più popolare la conoscenza del Bitcoin al grande pubblico permettendo di presentare i vantaggi legati all'utilizzo delle criptovalute.

E sempre in Premier League nella scorsa stagione sette squadre, tra cui il Tottenham Hotspur e il Leicester City hanno firmato un accordo pubblicitario con la piattaforma di trading eToro in Bitcoin. Un legame quello con la Premier League che sta spingendo anche altre squadre e campionati a esplorare le opportunità delle criptovalute e della tecnologia blockchain.

BIBLIOGRAFIA E SITOGRAFIA

https://www.borsaitaliana.it/notizie/sotto-la-lente/bitcoin-172.htm

https://www.eurobit.space/

https://www.wired.it/economia/finanza/2021/01/05/bitcoin-criptovalute-trend-2021/

https://cryptorivista.com/

https://cryptorivista.com/news/chainalysis-ecco-la-classifica-della-mass-adoption-di-bitcoin/

https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html

https://medium.com/@AndreaFerraresso/la-crittografia-dietro-a-bitcoin-72cc6ad3fa41

https://www.criptovaluta.it/bitcoin-mining

https://academy.bit2me.com/it/cos%27%C3%A8-una-rete-p2p

https://notizie.tiscali.it/economia/articoli/Dentro-la-prima-fabbrica-italiana-di-Bitcoin-Bitminer-Factory/

https://www.wired.it/economia/business

https://www.torinoggi.it/2020/03/06/sommario/sport/leggi-notizia/argomenti/altri-sport-4/articolo/calcio-e-bitcoin-un-legame-sempre-piu-forte.html