UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in

Economia e Commercio

INVESTIMENTI IN CRIPTOVALUTE

CRYPTOCURRENCY INVESTMENTS

Relatore: Chiar.mo
Prof. Attilio Mucelli

Rapporto Finale di
Luigi Imperatori

Anno Accademico 2020/2021

Indice

Introduzione

L'invenzione del Bitcoin nel 2008, e la successiva introduzione di numerose altre criptovalute alternative ad esso, sono state una delle più grandi innovazioni nel mondo della finanza alternativa, avvenute in un periodo, quello della crisi economica del 2008/2009, in cui numerosi investitori cercavano soluzioni più proficue.

Per la prima volta si creava un'intera economia totalmente online; chi emette le valute son gli stessi utenti che partecipano al software, autorizzandole e verificando le transazioni, che loro stessi e altri soggetti effettuano; il bitcoin e le altre criptovalute non esistono in forma fisica, sono detenute e spese soltanto nel mondo virtuale: basta una connessione ad internet.

Queste caratteristiche permettono minori controlli e minori restrizioni, grazie all'assenza di autorità centrali, offrendo la possibilità di ottenere grandi profitti, ma anche grandi rischi.

La tecnologia blockchain che sta alla base di tutto rappresenta un meccanismo versatile, che può essere applicato non solo al mondo cripto, dando la possibilità ai nodi della rete di veriricare e autorizzare operazioni.

L'obiettivo di questa tesi è spiegare, in modo semplice, ad un principiante, le caratteristiche di queste valute e metodi di pagamento innovativi, per iniziarlo al mondo della valute digitali.

Nel primo capitolo verranno affrontate le criptovalute in generale, partendo dal significato e etimilogia del termine, per passare poi alla storia e alla definizione.

Nel secondo capitolo si parlerà più specificatamente del Bitcoin, la prima criptovaluta introdotta nel mercato nel 2008, per poi passare in rassegna tutta una

serie di altre criptovalute, diverse dal bitcoin, definendo cosa sono e come vengono paragonate tra loro e commercializzate.

Nell'ultimo capitolo infine si tratterà dell'architettura del Bitcoin, ovvero di tutte le tecnologie che stanno alla base di un sistema sempre più in espansione, per poi passare ad osservare quelli che possono essere i vantaggi e gli svantaggi di una tale tecnologia.

Capitolo 1

Cosa sono le criptovalute?

1.1 Il concetto di criptovaluta: il termine

Il termine "criptovaluta" è composto di due parole, "cripto" e "valuta". La valuta si può spiegare come l'unità di misura dei pagamenti, una forma di denaro solitamente emessa dalla zecca di un paese, che ha tra le funzioni principali: quella di riserva di valore, di unità di conto e di mezzo di scambio. Il termine "cripto" si riferisce invece al fatto di essere una valuta "nascosta", in quanto è visibile e utilizzabile solo conoscendo le chiavi di accesso, composte da un codice informatico.

Il primo ad utilizzare il termine "criptovaluta", in inglese "cryptocurrency", fu David Lee Chaum, uno tra i più grandi crittografi al mondo, nato nel 1955 negli Stati Uniti.

Egli fu uno tra i promotori della prima conferenza mondiale di crittografia, chiamata CRYPTO, tenutasi a Santa Barbara nel 1982.

In questa sede Chaum tenne un intervento, intitolato "Blind signature for untraciable payments" in cui introduceva l'idea di una valuta virtuale, un primo protocollo di moneta che poteva essere nascosto e anonimo, ma che riscosse poco successo tra gli esperti all'epoca, che lo associarono al movimento "Cypherpunk"[1]

Chaum non si arrese e nel 1990 fondò a Amsterdam, in Olanda, paese scelto per il suo vantaggioso sistema fiscale, la società "Digicash", che cercava di

[1] Chyperpunk: movimento nato verso la fine degli anni '80, che aveva come obiettivo quello di tutelare la privacy degli utenti, oltre che un desiderio di porsi in modo sovversivo cercando di apportare un cambiamento nell'ambito sociale e politico

implementare la moneta con la crittografia, sempre seguendo l'obiettivo di rendere anonime le transazioni.

La società di Chaum però fallí nel 1999 a causa di problemi economici, ed egli si occupò in seguito di moneta elettronica, abbandonando il sentiero delle criptovalute e della crittografia.

1.2 La storia delle criptovalute

L'evoluzione delle tecnologie legate al mondo virtuale e dell'informatica ha coinvolto tutti i settori della realtà e della vita quotidiana, e quindi anche il sistema dei pagamenti e della moneta.

Tra gli anni settanta e ottanta si è sviluppata una corrente di pensiero, detta "libertarismo", che considerava la libertà, espressa come individuale, politica e di associazione, come il fine più alto ed importante da raggiungere. Un movimento questo che era fortemente "antiautoritario e sostenitore di politiche volte a limitare il potere" [2]

Da questo filone di pensiero, e con la preoccupazione per la costante minaccia alla privacy, sorse la corrente "Cypherpunk".

A questa, come già detto, fu accostata l'idea di David Lee Chaum, perché aspirava ad una rappresentazione digitale del valore, basato sulla crittografia, con cui proteggere e rafforzare la privacy degli utenti. Nel loro manifesto, firmato, anni dopo, da Eric Hughes il 3 Marzo 1993, si legge, infatti, "*Noi Cypherpunks siamo attivi nella costruzione di sistemi informatici anonimi grazie all'impiego della crittografia, affinché lo scambio di informazioni e di denaro resti riservato. Noi scriviamo i codici software e li divulghiamo gratuitamente affinché siano disponibili ed adottati dal maggior numero di persone"*[3].

[2] Christian Ferri, Blockchain&Made in Italy, Mondadori, Milano, 2020, pag.31
[3] Eric Hughes, "A Cypherpunk's Manifesto", Marzo 1993

In seguito alla teoria di Chaum, si ebbero altre pubblicazioni e tentativi di sviluppare soluzioni per proteggere la privacy online.

Nel 1991, Stuart Haber e Scott Stornetta descrissero l'idea che sta alla base della tecnologia "blockchain", di cui si tratterà in seguito, applicandola al mondo dei documenti digitali, in modo da segnarli per non essere retrodatati o manomessi.

Altro passo decisivo si ha nel 1997, quando Adam Back, crittografo e altro esponente del cypherpunk, teorizzò un protocollo denominato "Hashcash", primo algoritmo "proof of work"[4], ancora oggi alla base delle monete digitali, con cui si rendono "scarse e sicure anche nel mondo digitale" [5]le risorse.

Grazie alle idee di Back, un anno dopo, nel 1998, l'ingegnere informatico Wei Dai propose "un sistema di cassa elettronico distribuito ed anonimo"[6] chiamato B-money, basato su due protocolli: uno che è una sorta di riproposta del "proof of work" di Back, e un altro invece che promuove un'infrastruttura per gestire transazioni, in cui una parte di utenti, chiamata "nodi valiatori", detiene la propria versione delle liste delle transazioni aggiornata e controllata, funzione che può essere svolta pagando una cauzione; l'altra parte , che non partecipano alla validazione, hanno comunque la possibilità di richiedere informazioni; i validatori che non rispettano le regole appaiono disonesti e perdono la propria funziona e la cauzione versata.

Nel 2004 poi Nick Szabo tentò, unendo e applicando i concetti di Dai, di lanciare Bit-Gold, una prima valuta digitale decentralizzata, ma non ebbe successo.

---

[4] Proof of work: La Proof of Work (comunemente abbreviata in PoW) è un meccanismo per prevenire le doppie spese. La maggior parte delle principali criptovalute la utilizzano come *algoritmo di consenso*, un metodo per proteggere il registro di una criptovaluta. Il sistema HashCash di Adam Back è un esempio precoce dell'algoritmo Proof of Work che precede l'avvento delle criptovalute. Richiedendo ai mittenti di eseguire una piccola quantità di computazione prima di inviare una e-mail, i riceventi possono mitigare lo spam. Questa computazione costa virtualmente zero a un mittente legittimo, ma si accumula rapidamente per qualcuno che invia e-mail in massa; Che cos'è la Proof of Work, https://cryptorobin.it/che-cose-la-proof-of-work/, Ottobre 2021

[5] Christian Ferri, Blockchain&Made in Italy, Mondadori, Milano, 2020, pag.33

[6] "Chi é Wei Dai?, https://academy.bit2me.com/it/chi-è-wei-dai/, Gennaio 2022

Per trovare la prima vera criptovaluta funzionante occorre attendere il 2008, quando uno sconosciuto, sotto lo pseudonimo di Satoshi Nakamoto pubblicò un saggio chiamato "Bitcoin: a peer-to-peer Electronic Cash System", che consente di creare "un sistema di transazioni sicure ed elettroniche, senza che vi sia un rapporto di fiducia tra i partecipanti" [7], e di cui si tratterà più avanti in un paragrafo dedicato.

Dopo il Bitcoin, negli anni, si è registrata una fitta attività creativa, e sono venute alla luce numerose altre criptovalute, denominate "Altcoin", basate su alcune similitudini con i Bitcoin, ma differenziate per alcuni aspetti, che hanno trovato un terreno florido per creare un vero e proprio mercato cripto.

1.3 Criptovalute in breve: definizione e caratteristiche

Le criptovalute, conosciute anche come monete virtuali, sono dei beni crittografici, che, come è già stato anticipato, sono nascosti, e visualizzabili solo per chi è in possesso di un determinato codice informatico; naturalmente esistono solo online e quindi in forma virtuale. Queste utilizzano la crittografia per garantire la sicurezza delle proprie transazioni, tra soggetti che sono attivi nella stessa rete.

Uno degli elementi costitutivi di queste valute è un insieme di regole, detto "protocollo", ovvero un codice informatico che specifica il modo in cui i partecipanti possono effettuare le transazioni.[8]

La definizione di criptovalute non è ancora definita specificatamente, questa può essere sia assimilata ad una moneta, quindi usata come mezzo di scambio per transazioni, o ad un mezzo di finanziamento di azienda o di investimento.

Una delle caratteristiche principali delle valute digitali è il fatto di essere decentralizzate. Con questo si intende che sono prive di un ente centrale che

[7] Christian Ferri, Blockchain&Made in Italy, Mondadori, Milano, 2020, pag.49
[8] Le criptovalute; https://www.consob.it/web/investor-education/criptovalute, Gennaio 2022

controlli e curi la loro emissione, e di conseguenza prive di intermediari che ne controllino le transazioni.

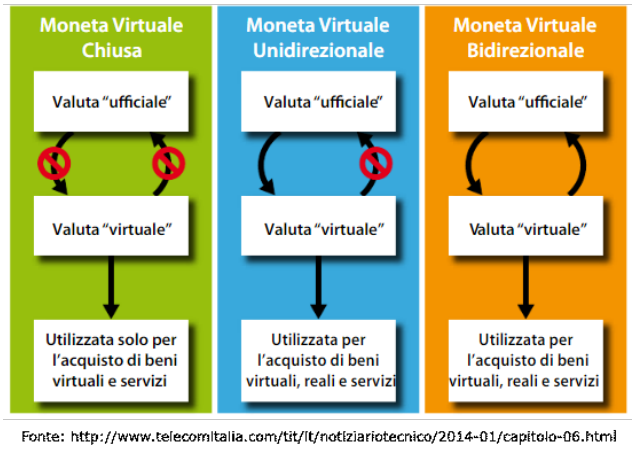
Si parla quindi di valute non sottoposte al controllo di autoritá pubbliche, ma emesse da emittenti privati che si servono di software altamente specializzati[9].

Il processo di creazione e convalida delle valute è detto allora mining, e verrà spiegato nei dettagli in un paragrafo a parte. Intanto si può anticipare che i *miners*, singoli utenti, eseguono operazioni, tramite complicati algoritmi, che hanno il compito di convalidare e garantire il funzionamento sicuro della piattaforma, ricevendo in cambio le criptovalute stesse come pagamento.

Le operazioni di volta in volta convalidate vengono aggiunte, come dei nuovi blocchi, al libro mastro "Blockchain" [10], altro elemento fondamentale che caratterizza il Bitcoin e altre criptovalute, che appunto permette agli utenti, in modo decentralizzato, di gestire la rete di transazioni e di parteciparvi. Anche la Blockchain verrà trattata in modo specifico in un paragrafo a parte.

Un'altra classificazione in uso prevede la suddivisione tra moneta virtuale 'chiusa', 'unidirezionale' e 'bidirezionale'.

Figura 1.1 Tipologie di monete virtuali



Fonte: http://www.telecomitalia.com/tit/it/notiziariotecnico/2014-01/capitolo-06.html

[9] Glossario, Criptovaluta https://www.borsaitaliana.it/borsa/glossario/criptovaluta.html, Gennaio 2022

[10] Blockchain può essere tradotto come "catenda di blocchi"

La differenza tra le tre fattispecie risiede nella possibilità o meno di poter scambiare la criptovaluta con moneta a corso legale (o valuta 'ufficiale' o 'moneta fiat', secondo altre comuni denominazioni) e nella tipologia di beni/servizi acquistabili. Il bitcoin, ad esempio, è una moneta virtuale bidirezionale in quanto può essere facilmente convertita con le principali valute ufficiali e viceversa.[11]

Ora, per concludere, bisogna concentrarsi sulla differenza tra moneta elettronica e moneta digitale.

Per moneta elettronica si intende un pagamento con valuta reale in corso legale che avviene sul web[12]. È un pagamento effettivo senza passaggio reale di denaro fisico. Questo viene depositato in un conto deposito di un intermediario ed ogni volta che avviene una spesa sulla rete questa viene prelevata da questo conto. Si utilizza quindi una moneta reale dematerializzata. Le criptovalute invece consentono pagamenti a distanza come "contante digitale" e non richiedono intermediari, sono immediate ed anonime proprio come moneta corrente. Si possono effettuare spese di ogni entità ed in ogni parte del mondo garantendo la più assoluta sicurezza ed efficacia.

[11] Le criptovalute; https://www.consob.it/web/investor-education/criptovalute, Gennaio 2022
[12] È possibile parlare infatti di E-cash

Capitolo 2

Il Bitcoin e le altre criptovalute

2.1 Bitcoin: storia definizione e principali caratteristiche

Nel 2008 il "fantomatico" Satoshi Nakamoto[13] depositò il nome a dominio bitcoin.org[14], e nello stesso anno pubblicò anche un articolo intitolato "Bitcoin: a peer-to-peer Electronic cash system".

Importante è innanzitutto la differenza tra Bitcoin e bitcoin[15], infatti il software che permette la creazione e la transazione di bitcoin, mentre la stessa parola con la lettera minuscola indica propriamente la moneta digitale scambiata nel sistema.

Il bitcoin è la prima valuta digitale decentralizzata, ovvero non sottoposta al controllo e alla direzione di autorità centrali e di intermediari, che ne curino emissione e transazioni. Proprio questa particolarità viene percepita dall'attuale Presidente del Consiglio, Mario Draghi[16], come una delle problematicità del bitcoin: egli afferma infatti che "mentre le valute hanno dietro le banche centrali dei loro paesi e dei loro governi, questo non accade per le criptovalute"[17].

---

[13] Satoshi Nakamoto è lo pseudonimo dell'inventore del Bitcoin; ci sono numerose teorie riguardo la sua identità, ma tutt'ora non si sa se sia un "lui" o una "lei". Ci si può basare solo sulla composizione del nome: "Naka" può significare "medium", "dentro" o "relazione". "Moto" può significare "origine" o "fondamentohttps://it.wikipedia.org/wiki/Satoshi_Nakamoto, Gennaio 2022

[14] https://bitcoin.org/it/, è il sito ufficiale della piattaforma Bitcoin

[15] bitcoin: simbolo: ₿, codice: BTC o XBT

[16] Mario Draghi, nato a Roma nel 1947, è un economista e manager italiano, ha ricoperto numerosi ruoli di rilievo tra cui Presidente della Banca Centrale Europea; dal 13 Gennaio 2021 è Presidente del Consiglio dei Ministri della Repubblica Italiana, https://www.treccani.it/enciclopedia/mario-draghi, Gennaio 2022

[17] https://www.ilsole24ore.com/art/draghi-studia-blockchain-e-bitcoin-dice-non-e-bce-dover-scrivere-regole--AEPESUzD, Febbraio 2018

L'obiettivo del bitcoin è quello di velocizzare le transazioni online[18], rendendole comunque sicure ed affidabili, utilizzando la crittografia.

Il ruolo che nelle monete legali viene svolto dalle autorità centrali, qui viene preso dai singoli utenti o "nodi" della rete, che possono scaricare sui loro dispositivi l'omonimo software "Bitcoin", e partecipare alla convalida e alla registrazione delle transazioni di due soggetti, che si vogliono scambiare questo tipo di valute, mantenendo comunque l'anonimato.

Questo tipo di attività è denominata "mining", e sfrutta la potenza dei singoli dispositivi dei vari utenti per convalidare le transazioni, dando in cambio bitcoin di nuova emissione.

Tanti più utenti e dispositivi sono collegati alla rete, tanto più si può definire centralizzato il sistema Bitcoin, che è infatti open-source[19], nel senso che permette a chiunque sia interessato di parteciparvi.

La sicurezza e il controllo di questo network è garantito dall'adesione ad un insieme di regole, "protocollo comune", che definiscono il funzionamento del sistema e del software Bitcoin.

La struttura che garantisce questo tipo di partecipazione e organizzazione degli utenti partecipanti alla rete è detta "peer-to-peer"[20], ovvero un tipo di architettura che vede i nodi sistemati non solo in ordine gerarchico, sotto forma di client e di

[18] Da non confondere con dei semplici pagamenti digitali

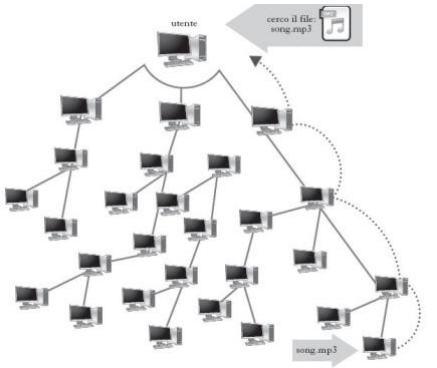
[19] Open-soource: Software di cui l'utente finale, che può liberamente accedere al file sorgente, è in grado di modificare a suo piacimento il funzionamento, correggere eventuali errori, ridistribuire a sua volta la versione da lui elaborata; https://www.treccani.it/enciclopedia/open-source/, Gennaio 2022

[20] Rete informatica nella quale i computer degli utenti connessi fungono nello stesso tempo da client e da server. In tal modo, gli utenti sono in grado di accedere direttamente l'uno al computer dell'altro, visionando e prelevando i file presenti nelle memorie di massa e mettendo a loro volta a disposizione i file che desiderano condividere. Le reti peer-to-peer sono usate in partic. per scambiare file audio o video;https://www.treccani.it/enciclopedia/peer-to-peer, Gennaio 2022

server, ma anche paritetico, come appunto intende la parola inglese “peer”, tra nodi equivalenti, fungendo da client e da server verso altri nodi della rete.

In questo modo ogni nodo può avviare da solo una completa transazione.

Figura 2.1: Struttura della rete peer-to-peer



Fonte: https://www.treccani.it/enciclopedia/peer-to-peer_%28Lessico-del-XXI-Secolo%29/

Lo stesso sito ufficiale di Bitcoin, infatti, afferma: “*Bitcoin usa la tecnologia peer-to-peer per non operare con alcuna autorità centrale o con le banche; la gestione delle transazioni e l'emissione di bitcoin viene effettuata collettivamente dalla rete. Bitcoin è open-source; la sua progettazione è pubblica, nessuno possiede o controlla Bitcoin e ognuno può prendere parte al progetto. Attraverso alcune delle sue uniche proprietà, Bitcoin permette utilizzi entusiasmanti che non potrebbero essere coperti”*[21].

Tra le caratteristiche principali di Bitcoin emergono:

- DECENTRALIZZAZIONE: come già affermato, Bitcoin non è soggetto al controllo di nessuna autorità governativa e nessun intermediario, ma bensì alla totalità dei nodi facenti parte del sistema
- ANONIMATO: l’indirizzo del portafoglio non può essere ricollegato a nessuna informazione personale, mentre le banche detengono ogni singolo dettaglio

[21] www.bitcoin.org

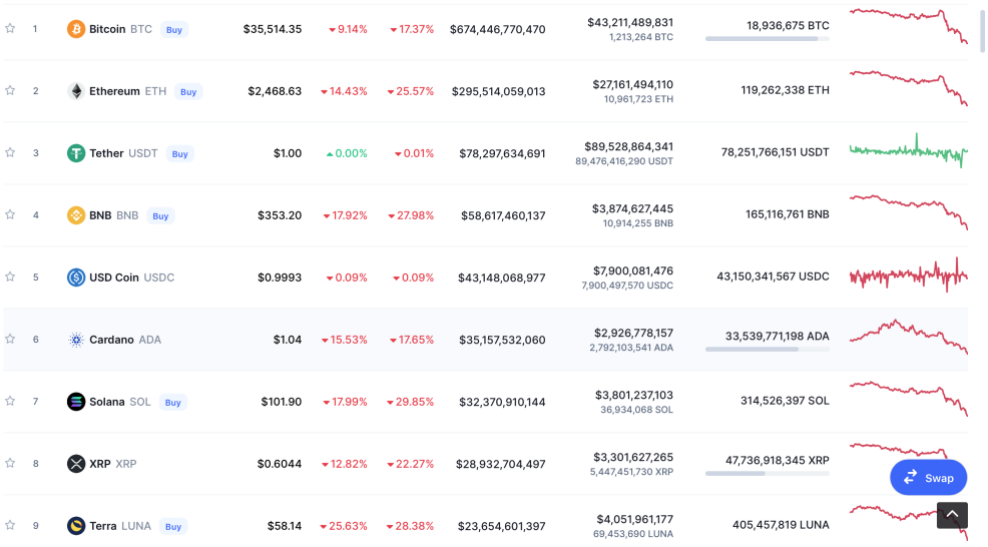
dei loro clienti. Le transazioni avvengono, infatti, tra "indirizzi pubblici", che sono punti di ricezione e invio di Bitcoin

- TRASPARENZA: tutte le transazioni effettuate nel sistema Bitcoin vengono registrate in una sorta di libro mastro, aperto al pubblico, da cui è possibile capire quanti Bitcoin possiede ogni indirizzo pubblico e chi glieli ha trasferiti. Di conseguenza rimane traccia di ogni singola transazione avvenuta, da cui però non è possibile arrivare alla persona fisica dell'utente che l'ha effettuata
- VELOCITÀ: le transazioni di Bitcoin avvengono istantaneamente, indipendentemente dalla localizzazione geografica degli utenti, a differenza delle banche tradizionali, le operazioni delle quali possono anche impiegare alcuni giorni
- NON RIFIUTABILITÀ: una volta che i bitcoin sono stati spediti non possono essere ripresi, a meno che il ricevente non li rimandi indietro
- BASSI COSTI DI TRANSAZIONE: il costo della transazione è libero, nel senso che ogni utente è libero di scegliere l'importo al momento della transazione, ma per evitare difficoltà si aggirano attorno allo 0,00001 BTC
- INDIPENDENZA RISPETTO A POLITICHE MONETARIE: l'assenza di un'autorità centrale di controllo fa si che il circolante non possa essere modificato in aumento o in diminuzione come avviene con le politiche monetarie delle banche. L'offerta di moneta è stabilita dal protocollo che gli utenti accettano entrando nella piattaforma Bitcoin, e aumenta tramite la convalida delle operazioni. La caratteristica principale è però che c'è un limite massimo stabilito, che si raggiungerà quando i bitcoin emessi saranno 21 milioni

2.2 Le criptovalute alternative, le criptovalute innovative e le critpovalute “piattaforma”

Si è detto che tra le caratteristiche principali della rete Bitcoin si trova quella di essere aperta a tutti, e proprio questo dettaglio, oltre a essere stato uno dei punti di forza, ha permesso la nascita di numerose altre criptovalute, per alcuni tratti simili al Bitcoin, per altre diversi.

Figura 2.2: Le più performanti criptovalute attualmente in circolazione



Fonte: https://coinmarketcap.com

La figura 2.2 indica quelle che ad oggi, Gennaio 2022, hanno maggior importanza tra gli investitori.

Le principali altre criptovalute oltre al Bitcoin possono essere raggruppate in tre diversi gruppi: le criptovalute “alternative”[22], le criptovalute “innovative” e le “criptovalute piattaforme”.

[22] Conosciute anche come “altcoins”, abbreviazione di Alternative Coin, ha più definizioni: Stephanie Yang ha definito le *altcoins* come "valute digitali alternative", mentre Paul Vigna ha descritto l'*altcoin* come una "versione alternativa del bitcoin". Aaron

Le criptovalute alternative vengono sviluppate come una biforcazione, in inglese "fork"[23], del Bitcoin. Queste prevedono o un "espansione", da un codice sorgente già esistente di un software nuovo, in questo caso quello di Bitcoin, oppure una creazione di un nuovo sistema, con regole e caratteristiche simili al Bitcoin, o addirittura copiate.

Non introducono dunque grandi novità nel panorama delle criptovalute rispetto a quelle già evidenziate, ma, anzi, posso essere definite quasi definire "copie".

Le cripto alternative cercano di migliorare, seppure imitando il sistema già esistente, alcuni elementi della tecnologia Bitcoin, come i tempi di attesa per le transazioni, giusto per citarne uno.

Secondo il sito coinmarketcap.com[24], oggi esistono circa diecimila altcoins diverse, e tra cui troviamo le prime nate Litecoin[25]e Namecoin[26], Dogecoin[27], Tether[28], Mana[29], Sand[30], le ultime due legate al recente mondo del metaverso[31].

Litecoin è una criptovaluta nata nel 2011, che si poneva l'obiettivo di creare l'argento in un sistema in cui il Bitcoin era l'oro[32].

Hankins definisce *altcoin* qualsiasi criptovaluta che differisca dal bitcoin https://it.wikipedia.org/wiki/Criptovaluta, Gennaio 2022

[23] Fork: Un fork, nell'ambito dell'ingegneria del software e dell'informatica, indica lo sviluppo di un nuovo progetto software che parte dal codice sorgente di un altro già esistente, a opera di un programmatore, https://it.wikipedia.org/wiki/Fork_(sviluppo_software), Gennaio 2022

[24] www.coinmarketcap.com è uno dei più autorevoli siti che si occupano di criptovalute

[25] https://litecoin.org/it/

[26] https://www.namecoin.org

[27] https://dogecoin.com; interessante il coinvolgimento del miliardario Elon Musk, che ha annunciato di vendere accessori di Tesla acquistabili tramite dogecoin

[28] https://tether.to/en/

[29] https://www.coinbase.com/it/price/decentraland

[30] https://coinmarketcap.com/it/currencies/the-sandbox/

[31]. Spazi virtuali, in cui sottoforma di avatar, che rappresentano gli utenti, si può interagire, possedere oggetti, creare e molto altro. Importante il ruolo delle valute digitali che possono essere utilizzate all'interno di questi universi; https://www.treccani.it/enciclopedia/metaverso, Gennaio 2022 https://tech.everyeye.it/notizie/cos-e-metaverso-chiarezza-definizione-fedez-551703.html, Novembre 2021

[32] Il continuo riferimento ai metalli preziosi si vede anche nel nome stesso della creazione delle cripto, e degli utenti che le creano: mining e miners

Utilizza algoritmi computazionali molto più semplici di Bitcoin e ha anch'esso un numero massimo di unità che è il quadruplo del Btc, ovvero ottantaquattro milioni.

Le criptovalute innovative invece rappresentano monete virtuali che, partendo dalla tecnologia Bitcoin, sono progettate in maniera differente.

Le differenze principali che si possono riscontrare nelle due critpovalute innovative più famose, Iota[33] e Ripple[34], sono, una tecnologia Blockchain, di cui più avanti si parlerà, diversa da quella Bitcoin, e una centralizzazione per Ripple. Ripple, infatti, anche in questo caso è sia il nome del software, che della valuta digitale (XRP), prevede un'autorità centrale, la società stessa, terza però rispetto ai governi e agli intermediari, che attraverso un protocollo denominato "*Ripple Transaction Protocol"* gestisce i trasferimenti e le transazioni.

Altra differenza col Bitcoin è che all'interno del sistema Ripple possono circolare non solo le valute stesse del sistema ma ogni altro tipo di valuta, senza commissioni e senza oscillazioni.

Viene definita, infatti, da molti "non criptovaluta", ed è spesso stata accostata ad alcune banche, per la fiducia di cui gode tra queste, che stanno sperimentando questa tecnologia nei bonifici bancari.

Iota si distacca dal Bitcoin per il non utilizzo di una blockchain, ma il "Tangle"[35], un diverso protocollo software, in cui le transazioni sono gestite in parallelo e in modo asincrono, quindi tutto molto più veloce.

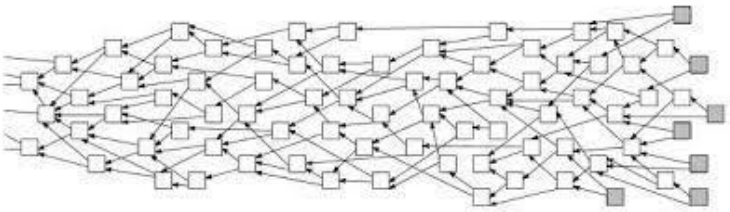
---

[33] https://www.iota.org

[34] https://ripple.com/xrp/

[35] Tangle: protocollo software basato su un grafo aciclico diretto, è una struttura dunque che non ha cicli diretti, ovvero scegliendo qualsiasi vertice del grafo non è possibile tornare ad esso percorrendo gli archi del grafo, una sequenza può passare soltanto dal prima al dopo e non viceversa, https://www.italianotizie24.it/iota-alcune-differenze-fondamentali-con-i-bitcoin/, Giugno 2018

Figura 2.3 Il Tangle



Fonte: https://www.criptoguide.it/iota-guida/struttura-tangle-iota/

Infine, le criptovalute "piattaforma", definite anche "criptovalute 2.0", tra cui la più importante Ethereum[36], seconda per capitalizzazione di mercato dopo Bitcoin.

Ethereum, creata nel 2013, non è sono un sistema al'interno del quale circola la criptomoneta Ether, ma una struttura decentralizzata in cui possono essere gestiti dei "contratti intelligenti"[37], sviluppati software e applicazioni.

Alla base di tutto c'è l'idea di sfruttare al massimo tutte le possibilità della blockchain e della decentralizzazione.

Questi contratti si sostanziano nella creazione di applicazioni che eseguono autonomamente e automaticamente ciò che è stato programmato nella contrattazione tra le parti.

La criptovaluta Ether, è usata per tutte le transazioni effettuate all'interno di Ethereum.

Bisogna introdurre un'ulteriore differenziazione tra le criptovalute in base alla piattaforma su cui lavorano: i coin e i token.

[36] https://ethereum.org/en/

[37] Gli smart contract (in italiano: *contratto intelligente*) sono protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale. Gli smart contract, di solito, hanno anche un'interfaccia utente e spesso simulano la logica delle clausole contrattuali, https://it.wikipedia.org/wiki/Smart_contract, Giugno 2018

I coin sono cripto indipendenti, quelle di cui si è trattato fino ad ora, che hanno una loro blockchain e una loro rete, sono decentralizzate e gestite in maniera condivisa dai partecipanti al sistema, mentre i token non hanno niente di tutto ciò, si appoggiano ad un sistema già esistente, operano su una piattaforma di un altro software e non hanno protocolli o blockchain proprie e possono essere sviluppate all'interno delle critpovalute definite 2.0.

L'Osservatorio Digital Innovation del Politecnico di Milano definisce un token come "un'informazione digitale, registrata su un registro distribuito, univocamente associata a uno e un solo specifico utente del sistema e rappresentativa di una qualche forma di diritto: la proprietà di un asset, l'accesso a un servizio, la ricezione di un pagamento, e così via[38].

Un esempio di token è il già citato Tether, che viene ospitato sulla piattaforma di Ethereum, ed è particolare perché definito "stablecoin"[39], ovvero il loro valore è collegato ad un asset o ad un bene reale, che possono essere il dollaro, l'euro oppure l'oro.

2.3 Fattori di comparazione e analisi delle principali criptovalute

Quando vengono analizzate e comparate tra loro le differenti criptovalute, si è soliti usare tre elementi, ovvero la capitalizzazione di mercato, il volume degli scambi e la circulating supply.

La capitalizzazione di mercato possiamo riassumerla come il valore totale espresso in dollari di tutte le valute già sottoposte a mining, quindi già estratte dai vari utenti della rete e viene determinato moltiplicando il numero totale di valute

[38] https://focus.namirial.it/differenze-vantaggi-token-criptovalute/, Giugno 2021

[39] Stablecoin definiti così perché il loro prezzo è ancorato a un'attività di riserva come il dollaro statunitense o l'oro. Gli stablecoin, pertanto, sono molto meno volatili dei bitcoin e rappresentano una forma di valuta digitale molto più adatta al commercio di ogni giorno e alle operazioni trasferimento tra valute diverse, https://www.coinbase.com/it/learn/crypto-basics/what-is-a-stablecoin, Gennaio 2022

"minate"[40], per il valore di una singola valuta, che è il prezzo medio di mercato, ottenendo così molto semplicemente il totale. Gli investitori tramite questo strumento riescono a confrontare tra di loro le varie criptovalute in circolazione. Infatti, cripto con capitalizzazioni di mercato più elevate rappresentano investimenti più sicuri, essendo meno esposte alle oscillazioni e ai "capricci" del mercato, mentre cripto con capitalizzazioni medie o basse rimangono più scoperte.

Il volume degli scambi indica il numero di transazioni effettuate dagli investitori in un determinato lasso di tempo. Da tale informazione è possibile dedurre l'interesse per una valuta da parte del mercato; è quindi un'importante indicazione sulla relazione tra domanda e offerta e sul dinamismo dello scambio.

Per circulating supply intendiamo invece il numero di criptovalute attualmente in circolazione. Se ben si ricorda infatti è già stato detto che numerose valute digitali hanno un numero massimo raggiungibile, per il bitcoin per esempio parliamo di ventuno milioni di unità. Più la circulating supply sarà vicina al massimo, tanto più il valore potrà aumentare, essendo un bene limitato.

Di conseguenza, valute che hanno limiti più bassi potranno raggiungere valori più alti e viceversa valute che hanno limiti maggiori avranno valori inferiori: il prezzo della prima tenderà ad essere alto e il prezzo della seconda tenderà ad essere basso.

[40] Cdm = NCE x PMM
Cdm: capitalizzazione di mercato
NCE: unità di criptovalute minate
PMM: prezzo medio di mercato

Figura 2.4 Fattori di analisi

Fonte: https://coinmarketcap.com

2.4 Come offrire una criptovaluta sul mercato: le ICO

Per lanciare sul mercato criptovalute si può ricorrere ad una cosiddetta ICO[41], inizialmente utilizzate per raccogliere fondi per nuove criptovalute e ora maggiormente per finanziare nuove iniziative imprenditoriali.

Il sistema è molto simile alla IPO[42], ma in questo caso per raccogliere fondi non vengono offerte azioni, bensì dei "coin" o dei "token", attraverso una piattaforma blockchain, in cambio di denaro o di criptovalute già esistenti.

Si possono evidenziare dunque due attori, chi intende sottoscrivere l'ICO, e chi invece intende immettere nel mercato il "coin" o il "token".

Il soggetto che finanzia l'ICO, attraverso denaro o altre criptovalute già esistenti riceverà la cripto immessa nel mercato una volta che il contratto sarà scaduto, mentre il soggetto che riceve i finanziamenti li userà per finanziare e lanciare la sua impresa.

Ora mentre le IPO sono sottoposte a controlli, le ICO non sono regolate in maniera chiara dai legislatori.

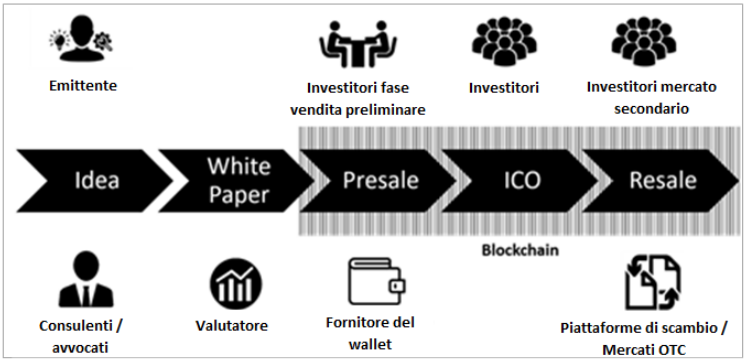
[41] Initial coin offering
[42] Particolare tipologia di offerta pubblica di vendita o di sottoscrizione finalizzata all'ammissione alla quotazione su un mercato regolamenta, https://www.borsaitaliana.it/borsa/glossario/ipo-offerta-pubblica-iniziale.html, Gennaio 2022

Inoltre, mentre chi acquista azioni in una IPO diventa a tutti gli effetti azionista, chi acquista “coin” e “token” non partecipa alla società che li ha immessi nel mercato, seppure il fine di entrambe le metodologie sia lo stesso, ovvero raccogliere fondi.

I coin e i token lanciati possono essere utilizzati sono nella blockchain del sistema che li ha introdotti, quindi parliamo di criptovalute 2.0.

Coloro che immettono nel mercato una ICO sono detti “sponsor”, e in generale seguono questo paradigma: creazione di un progetto ‘innovativo' da sviluppare e finanziare; redazione e pubblicazione (sul web) di un documento informativo non standardizzato relativo a emittente, progetto, coin/token e membri chiave del team ("white paper")[43]; utilizzo della blockchain per le fasi di coinvolgimento degli investitori (su mercato primario e, ove previsto, secondario)[44].

Figura 2.5 Come avviene una ICO



Fonte: https://www.consob.it/web/investor-education/criptovalute

[43] In italiano “libro bianco” sono strumenti utilizzati per la promozione di tecnologie o di prodotti, in cui si evidenziano le caratteristiche principali, i possibili utilizzi e i punti di forza, https://www.studiosamo.it/glossario/white-paper/, Aprile 2020
[44] https://www.consob.it/web/investor-education/criptovalute, Gennaio 2022

Capitolo 3
Architettura del Bitcoin

3.1 La Blockchain

La Bitcoin è la blockchain[45] legata alla moneta bitcoin e puó essere immaginata come una sorta di libro mastro pubblico, in cui sono riportate tutte le transazioni avvenute fino ad un dato istante.

Visivamente si può descrivere come una catena di blocchi, a loro volta visti come un agglomerato di transazioni. La particolarità della blockchain è quella di garantire la sicurezza, i controlli e l'efficacia delle transazioni, non passando per il controllo di un terzo soggetto o di un'autorità. I dati sono protetti grazie alla crittografia dalle manomissioni e dalle modifiche.

La catena di blocchi è in continua crescita, tramite la registrazione di nuove operazioni e di conseguenza con l'aggiunta man mano di nuovi blocchi alla sequenza.

Le transazioni avvengono con frequenza continua all'interno del sistema mentre la connessione dei blocchi avviene circa ogni dieci minuti, in modo cronologico partendo dal blocco originario, detto "genesis block"[46].

Prima di essere collegato alla catena, un blocco è un insieme di transazioni, per l'esattezza ogni singolo blocco può contenerne quattromiladuecento[47], ancora da autenticare.

---

[45] La blockchain appartiene alla più ampia famiglia delle "distribute ledger", ovvero sistemi basati su un registro distribuito, che ogni utente può leggere e modificare, La blockchain spiegata semplice, https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni, Febbraio 2019

[46] Il Genesis Block è il primo blocco della catena Bitcoin, è stato creato il 3 gennaio 2009 da Satoshi Nakamoto, https://www.investopedia.com/terms/g/genesis-block.asp, Luglio 2021

[47] Per l'esattezza una ogni 7 secondi

Una volta autenticato come già detto viene legato alla serie e l'operazione è definitiva, nel senso che ogni transazione non può essere annullata.

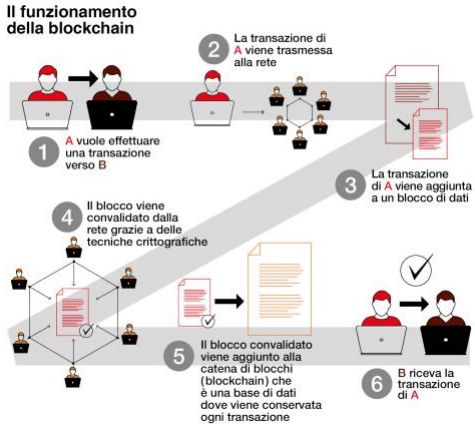
La convalida avviene applicando una "marca temporale", ovvero associando una data e un'ora all'operazione, quindi una validazione che è opponibile ai terzi.

Ad ogni concatenamento la rete effettua un controllo su tutti i blocchi della catena, in questo modo avviene una verifica che tutte le transazioni siano state effettuate nel corretto modo e una volta sola, evitando così la double spending, cioè che un utente invii lo stesso bitcoin a due soggetti diversi.

Ogni singolo nodo della rete che scarica il software Bitcoin sul proprio terminale detiene una copia della blockchain.

Mentre i blocchi sono concatenati in modo cronologico, le transazioni all'interno sono ordinate in modo da unire ricevente e mandante di bitcoin, cosicché chi effettua un'operazione è legato a chi gli ha dato disponibilità di bitcoin e a chi li riceverà.

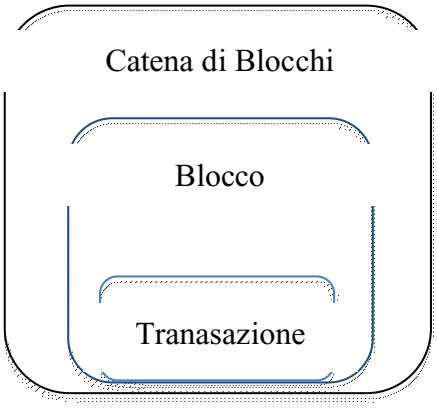
Figura 3.1 Il funzionamento della blockchain



Fonte: https://www.kmu.admin.ch

La transazione, dunque, è la particella più piccola di un sistema che poi a ingrandire vede i blocchi e la catena.

Figura 3.2 Schematizzazione di un blocco



Su alcuni limiti e difetti della blockchain si sono concentrati i creatori di numerose altre criptovalute, dando vita così, come è già stato accennato al paragrafo 2.2, a moltissime altre monete virtuali.

Si può fare una distinzione tra "blockchain permissionless" e "blockchain permissioned"[48]. Nelle prime chiunque può partecipare alla rete e al processo di validazione, Bitcoin ne è un esempio; nelle seconde invece il processo di validazione e l'accesso alla rete sono riservati ad un ristretto numero di attori.

Gli utilizzi e le implicazioni della blockchain, ora limitata quasi esclusivamente al mondo delle criptovalute, possono essere numerosi[49], dalla finanza alle istituzioni e alle università, e magari in un futuro non tanto lontano si vedrà applicato questo sistema in molti campi differenti.

[48] La blockchain spiegata semplice, https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni, Febbraio 2019

[49] Questa innovazione consente, potenzialmente, di fare a meno di banche, notai, istituzioni finanziarie e così via, La blockchain spiegata semplice, https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni, Febbraio 2019

3.2 Il mining e i minators

Si hanno quattro possibili modi diversi per ottenere bitcoin:

- cambiare una valuta in bitcoin, ovvero scambiare una valuta in corso legale, o un'altra criptopovaluta con dei bicoin;
- acquistare bitcoin presso i "Bitcoin ATM's[50], ovvero dispositivi fisici che diminuiscono di molto i tempi richiesti per l'autenticazione nelle altre transazioni;
- vendere beni o servizi in cambio di bitcoin, e ultimamente sempre maggiori sono i negozi fisici e virtuali che accettano pagamenti tramite tale valuta;
- fare "mining", ed è proprio su questo aspetto che ci si concentrerà in questo paragrafo;

Con mining si intende un processo basato sulla risoluzione di un algoritmo.

Ogni *miner* mette a disposizione del sistema la potenza computazionale dei suoi dispositivi, in modo che questi lavorino per decriptare, risolvere e verificare le informazioni provenienti dalle transazioni.

Una volta compiuta tale operazione, come è già stato spiegato nel precedente paragrafo, tutte le informazioni validate in quel certo intervallo di tempo rientrano all'interno di un blocco, che viene aggiunto alla catena.

Il risultato di tali soluzioni è quello di mantenere protetta e integra l'intera blockchain.

Ora ci si deve concentrare su come avviene effettivamente la verifica delle informazioni e la risoluzione degli algoritmi.

---

[50] Gli ATM delle banche erogano banconote e nei casi più evoluti funzionano da sportelli automatici per versamenti e molte altre operazioni bancarie; gli ATM di bitcoin erogano la criptovaluta inventata da Satoshi Nakamoto e anche altre criptovalute. Non dobbiamo aspettarci che emetta monetine con il logo di bitcoin stampato sulle due facce. Le criptovalute sono immateriali, https://www.fxempire.it/education/article/cosa-sono-gli-atm-di-bitcoin-e-come-funzionano-140337, Gennaio 2022

Tutto il sistema si basa sulla decifrazione di una funzione "hash"[51] per ottenere una "hash value". Ad ogni operazione iniziale di un blocco è associata infatti una determinata funzione "hash value" che i miners devono trovare, ed è l'unico modo questo per convalidare le informazioni. Tutto ciò rende sicuro e immutabile il sistema, infatti anche la più piccola variazione determina un cambiamento della "hash value".

Inoltre, ogni "hash value" contiene informazioni anche sui blocchi precedenti, in questo modo verificando di volta in volta la correttezza dell'intera catena.

Ogni miner, facendo "per forza" un innumerevole numero di tentativi, gareggia per essere il primo a trovare la funzione "hash value", in modo da trovare la stringa alfanumerica che riesca a chiudere il blocco.

Nel momento in cui un nodo della rete riesce a trovare l'"hash value", lo annuncia al resto del sistema, ottenendo così come pagamento una frazione di bitcoin.

Il blocco così viene aggiunto alla catena e i miners iniziano il lavoro su un nuovo blocco di transazioni.

"Semplificando possiamo dire che ogni nuova transazione viene accorpata dentro un nuovo blocco della catena. Il contenuto di ogni nuovo blocco viene passato attraverso l'hash function e ogni blocco contiene l'hash function del precedente"[52].

[51] Nel linguaggio matematico e informatico, l'hash è una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita, https://it.wikipedia.org/wiki/Funzione_di_hash, Settembre 2021

[52] Christian Ferri, Blockchain&Made in Italy, Mondadori, Milano, 2020, pag.52

Figura 3.3 Blocchi concatenati grazie alla funzione di hash

Figura 7 All'interno di blockchain, i blocchi di dati sono concatenati grazie all'hash function

Fonte: Christian Ferri, Blockchain&Made in Italy, 2020, Mondadori, pag.52

Ogni volta che un minatore risolve una funzione, viene ricompensato come già detto con una frazione di bitcoin, che dipende da molte variabili, tra cui la difficoltà dell'operazione, i costi di transazione e la capacità computazionale messa a disposizione.

Le regole però per il mining sono ben definite dal protocollo; infatti, ogni due settimane si devono produrre duemilasedici[53] nuovi blocchi, indipendentemente dalle transazioni presenti nel sistema.

Proprio questa definizione del numero di nuovi blocchi permette di stabilire e regolare di volta in volta la difficoltà degli algoritmi da risolvere.

Se infatti ci si discosta da duemilasedici, la difficoltà cambia, a seconda che si sia superato quel numero o non lo si sia raggiunto.

Oltre a ciò, se il numero di soggetti "minatori" aumenta, lo fa di conseguenza la difficoltà di risoluzione, perché sono maggiori i mezzi computazionali che si occupano di tale operazione.

È inoltre stabilita anche la quantità di bitcoin di nuova emissione che viene liberata ad ogni nuova risoluzione della funzione hash. Si è partiti da 50 bitcoin per

[53] Circa uno ogni dieci minuti

blocco e questo numero viene dimezzato ogni duecentodiecimila blocchi[54]. Questo è l'unico modo in cui i bitcoin possono essere messi in circolazione.

Il mining è un processo molto costoso per tutti i soggetti coinvolti, in quanto gli strumenti utilizzati sono calcolatori che hanno prezzi rilevanti, consumano molta energia elettrica e che lavorando ininterrottamente al massimo della loro CPU[55], si usurano velocemente. Di conseguenza al giorno d'oggi per poter fare mining è necessario iscriversi ad un gruppo, che sfruttando l'insieme di individui registrati riesce a risolvere l'algoritmo in meno tempo e ha più probabilità di trovare la soluzione. L'iscrizione ad un pool però prevede il pagamento di una tassa pari ad una percentuale variabile per ogni ricompensa in bitcoin ricevuta.

3.3 I portafogli e le transazioni

I portafogli di bitcoin possono essere associati a dei conti correnti. Fanno una specie di estratto conto in tempo reale delle operazioni di entrata e uscita avvenute sul portafoglio e del contenuto di questo.

La similitudine con il conto corrente si ferma però qui; infatti, i bitcoin sono contenuti nella blockchain, che, come è già stato ampiamente detto, funge da registro pubblico, mediante specifici indirizzi, appartenenti ai diversi utenti.

Dagli indirizzi, composti da una combinazione di numeri e lettere, non è possibile risalire ai soggetti proprietari dei bitcoin e questo garantisce anonimato e sicurezza.

Una transazione è un trasferimento di valori tra portafogli Bitcoin che viene incluso nella blockchain[56].

---

[54] Circa ogni quattro anni

[55] CPU Sigla di central processing unit, la componente di un calcolatore (detta anche processore) che carica le istruzioni dei programmi in memoria, le interpreta e manipola i dati di conseguenza, https://www.treccani.it/enciclopedia/cpu/, Gennaio 2022

[56] https://bitcoin.org/it/come-funziona, Gennaio 2022

Il fondamento di tutto è quello delle "transazioni asimmetriche", in cui sono presenti una chiave pubblica e una chiave privata: codici alfanumerici mediante i quali possono essere effettuate operazioni.

Ogni fruitore ha una coppia di chiavi, pubblica e privata.

La chiave privata identifica un wallet e serve per apporre le firme digitali ai bitcoin in uscita, e dunque solo chi possiede tale chiave può effettuare operazioni sui bitcoin presenti nel wallet.

La chiave pubblica invece deriva quella privata, e serve per verificare che le firme digitali sulla transazione siano corrette.

Dalla chiave privata dunque si può arrivare alla pubblica, ma non viceversa, da quella pubblica non si può giungere alla privata, ed è proprio per questo motivo che le transazioni vengono definite asimmetriche.

Per ogni chiave privata possono essere associate, al momento della creazione del wallet, cento chiavi pubbliche. In questo modo, ad ogni utente, usufruendo di queste chiavi, è garantita la privacy, perché seppure venga collegata una chiave pubblica ad un soggetto, sarebbe impossibile risalire alle altre operazioni effettuate con le altre novantanove chiavi.

In ogni scambio, per far si che sia unico, per ogni chiave privata esiste una sola chiave pubblica, che è una di quelle cento associate al portafoglio.

Per semplicità possiamo associare la chiave pubblica all'IBAN[57] di un nostro normale conto corrente bancario, sarà proprio verso questo che un utente effettuerà un pagamento in bitcoin.

[57] L'IBAN, acronimo di International Bank Account Number, è il codice numerico che identifica univocamente un conto corrente bancario a livello mondiale**.** L'IBAN viene definito secondo standard internazionali ed è composto da una combinazione di lettere e numeri che indicano il paese dove il conto è stato sottoscritto, un codice di controllo, la banca e in particolare la filiale di riferimento e il numero progressivo di conto. In Italia l'IBAN conta 27 caratteri, https://www.bancobpm.it/magazine/glossario/iban/, Gennaio 2022

Una volta effettuata la transazione dalla chiave privata di chi gestisce il portafoglio pagante a quella pubblica di chi riceve il pagamento, entrano in gioco gli altri utenti.

La transazione, come già detto, viene inserita in un blocco e convalidata dai nodi della rete tramite la funzione hash.

Solo una volta che tale verifica viene effettuata la transazione può dirsi conclusa.

Unicamente chi ha la chiave privata è "proprietario" dei bitcoin presenti su quel wallet, diventandone importantissima la custodia.

Si possono trovare quattro tipologie di wallet: i "desktop wallet", i "mobile wallet", gli wallet "online" e gli wallet "hardware".

Il portafoglio più comune è il "desktop wallet". Esso è costituito da un software da installare sul proprio computer, e può presentare dei rischi, in quanto se non viene regolarmente cambiata la password e non viene aggiornato l'antivirus, rischia di essere "hackerato"[58], ovvero rischia che qualcuno entri nel computer e di conseguenza nel portafoglio e rubi i bitcoin lì detenuti.

I "mobile wallet" invece consistono in un'applicazione da installare sui propri telefoni e tablet[59], per il resto le caratteristiche son le stesse dei "desktop wallet", presentando, con le dovute differenze, gli stessi rischi.

Gli wallet più rischiosi in assoluto sono gli "online wallet", ma sono anche i più veloci e pratici.

Questo servizio è messo a disposizione online dagli exchange, che hanno il ruolo di scambiare le criptovalute con la moneta legale.

Sono spesso soggette anch'esse ad attacchi "hacker", e quindi molto rischiose.

---

[58] Introdursi senza autorizzazioni in reti protette di computer o realizzare virus informatici, https://dizionari.corriere.it/dizionario_italiano/H/hacker.shtml, Gennaio 2022

[59] Tablet**:** un computer portatile con cui si interagisce principalmente tramite un display "touchscreen" utilizzando le dita o uno stilo, https://www.treccani.it/enciclopedia/tablet, Gennaio 2022

Infine, il portafoglio più sicuro è l'"hardware wallet".

Si parla di "hardware" per indicare dispositivi fisici, solitamente chiavette USB[60], che si collegano al computer e interagiscono col software del wallet installato nel computer. Questi custodiscono le chiavi private degli indirizzi bitcoin.

Finite le operazioni da effettuare sul portafoglio, il dispositivo si scollega e non può essere raggiunto da attacchi "hacker" online.

Figura 3.4 Varie tipologie di portafogli hardware

Fonte: http://platformcoop.net/it/recensione-del-miglior-portafoglio-hardware/

[60] USB ⟨*u-èsse-bi*⟩ – Nel linguaggio informatico, sigla della locuz. ingl. *Universal Serial Bus* «bus seriale universale», tipo di interfaccia del computer usata per collegare unità e dispositivi periferici. Anche come aggettivo.: *cavo USB*; *i computer di ultima generazione hanno quattro porte USB*; *memoria USB*, memoria rimovibile, portatile e di piccole dimensioni https://www.treccani.it/vocabolario/usb/, Gennaio 2022

3.4 Gli exchange

Per ogni tipo di operazione attraverso le criptovalute si deve passare dal Bitcoin, data la sua natura di criptovaluta più importante e conosciuta.

Si hanno principalmente due modi: uno scambio immediato tra chi ha nel proprio wallet dei bitcoin e chi invece vuole acquistarli oppure una transazione gestita da intermediari, che prendono il nome di "exchange".

Lo scambio diretto può essere condotto anche da siti specializzati, ad esempio localbitcoin[61], assimilabili quindi anch'essi a degli exchange.

Questi si occupano di mettere in contatto chi intende vendere e chi intende acquistare, e lo scambio può essere effettuato online, mediante pagamenti con bonifici bancari o postepay[62], oppure fisicamente, con l'incontro, in luoghi dotati di connessione internet, scelti dallo stesso sito.

I servizi di localbitcoin sono attivi in circa 1600 città e più di 200 nazioni, tra cui anche l'Italia, soprattutto al nord.

Un'altra tipologia di incontro diretto è l'organizzazione tramite dei social network[63], in cui si mettono in contatto soggetti interessati allo scambio face-to-face.

Oltre agli scambi diretti esistono scambi gestiti e intermediati da degli "exchange" online, che offrono servizi per la compravendita di criptovalute con valute di corso legale.

Gli "exchange" si svilupparono subito dopo la nascita del bitcoin, nel 2008, infatti il primo venne aperto nel 2010 e da quel momento ne sono stati creati a centinaia.

---

[61] Localbitcoin è una piattaforma di scambio di bitcoin con sede e Helsinki in Finlandia, https://localbitcoins.com/it/, Gennaio 2022

[62] La carta Postepay Standard è la prepagata ricaricabile di Poste Italiane

[63] Termine usato in varie discipline tecniche, specialmente in elettrotecnica, elettronica e informatica, come sinonimo di rete, https://www.treccani.it/vocabolario/network/, Gennaio 2022

Il loro ruolo è importantissimo per il mercato delle cripto, in quanto consentono di creare trading e liquidità per il mercato stesso, e di definire di conseguenza un prezzo per le cripto, decidendo quale deve essere quello di acquisto o di vendita di ogni singola valuta[64].

Gli "exchange" si possono raggruppare in due tipologie: quelli che effettuano operazioni prevalentemente in bitcoin e quelli invece attraverso cui si può passare dalle varie criptovalute alle monete in corso legale e viceversa.

Con i primi chi intende acquistare altre criptovalute che non siano bitcoin, deve depositare questi ultimi nel conto dell'"exchange"[65], e una volta fatto questo potrà acquistare tutte le valute digitali presenti nella piattaforma. Importante sottolineare che, se una volta acquistate altre criptovalute, si volesse comprare, con quella valuta acquistata, altro, si deve ripassare dal bitcoin: quindi ricambiare quella valuta in bitcoin e poi procedere nuovamente come già è stato spiegato.

In tutte queste operazioni sono presenti delle commissioni.

Negli altri "exchange" si può passare direttamente invece dalle criptovalute alle valute in corso, e viceversa, acquistando o vendendo semplicemente la valuta che si possiede.

Si hanno in generale tre tipi di funzioni adibite agli "exchange": quella di *order*, quella di *broker* e quella di *trading*.

Con *order* intendiamo che l'intermediario si limita a far incontrare chi vuole vendere e chi vuole comprare, guadagnano solamente dalle commissioni.

Tramite la funzione di *broker* invece l'intermediario, ricevuto un ordine di acquisto o di vendita, va sul mercato per eseguirlo; quindi, qui non viene unita la domanda e l'offerta, ma è l'intermediario che opera direttamente sul mercato.

---

[64] Hanno un ruolo di "Market maker"

[65] L'utilizzo del bitcoin in questo ruolo di passaggio è dovuto al fatto che è la criptovaluta più conosciuta e con capitalizzazione di mercato più alta

Infine, nella funzione di *trading*, le piattaforme acquistano e detengono delle criptovalute, ed effettuano l'acquisto/vendita come diretti venditori/acquirenti dei clienti. Queste presentano i maggiori rischi dato che sono esposte alle oscillazioni del valore delle valute che detengono.

3.5 Vantaggi

Si possono evidenziare numerosi vantaggi legati all'utilizzo del bitcoin e delle altre criptovalute.

- riduzione dei costi e dei tempi di transazione: le transazioni in bitcoin, a differenza dei normali pagamenti, prevedono una commissione non a carico del venditore, ma bensì del compratore. Le commissioni vengono stabilite dagli utenti della rete e c'è anche la possibilità che non vengano stabilite affatto. Si è già detto che questi pagamenti sono un incentivo all'attività dei *miner* ad inserire una transazione appena effettuata nel blocco. Dunque, c'è una proporzionalità tra costo della transazione e tempo d'attesa, che è a libera scelta dell'utente: meno tempo d'attesa significa un costo, quindi un incentivo per i *miner* maggiore. I tempi d'attesa in ogni caso rimangono comunque inferiori rispetto a quelli del mondo bancario;
- libertà e decentralizzazione: come è già stato detto, bitcoin, così come quasi tutte le altre criptovalute, non sono soggette al controllo di un'autorità centrale, ma sono gli stessi utenti e nodi della rete a verificare e regolare tutte le transazioni che avvengono nel sistema, semplicemente accordandosi ad un protocollo di regole che accettano scaricando il software. Questa libertà fa si che la struttura non possa essere soggetta a politiche fiscali e a tariffe;

- alta portabilità: tutto il sistema è online, se non per i citati "hardware wallet", serve solo una connessione ad internet, e la transazione sarà istantanea, senza bisogno di intermediari;
- accessibilità e sicurezza: chiunque può possedere un portafoglio e può accedere al sistema, e accettare o ricevere pagamenti. Fondamentale la protezione della chiave privata di accesso al wallet, perché chi ne è in possesso è virtualmente il proprietario delle valute contenute all'interno del portafoglio;
- trasparenza: tutte le transazioni vengono verificate e registrate sulla blockchain. Il protocollo del sistema è criptato, rendendo impossibile a chiunque di modificarlo. Nella catena però non sono presenti i nomi degli utenti, ma solo gli username, e conoscendo le chiavi pubbliche dei due utenti coinvolti nella transazione, i nodi della rete riescono a verificarne la correttezza;
- ruolo degli esperti: in bitcoin non c'è nessuno che ha il controllo e il potere di apportare modifiche al sistema. Ma cosa succederebbe se si riscontrassero dei problemi? Il ruolo in questo caso lo ha la comunità di esperti e programmatori, che migliorano il sistema ed emettono una nuova versione del software più aggiornata. Fondamentale ricordare che tale versione diventa effettiva solo se la grande maggioranza di *miner* e di utilizzatori inizia a usarla, sostituendola con quella vecchia, mentre se non viene accettata non accade nulla. Nel caso sia utilizzata dalla maggioranza dei *miner*, quei pochi che non la usano vedranno i blocchi da loro risolti rifiutati dal sistema;
- irreversibilità: una volta effettuata la transazione e registrata nella blockchain non può essere annullata ed è considerata irreversibile. Quindi chi ha mandato i bitcoin non può riottenerli, senza il consenso di chi li ha ricevuti. Questo rende vani i numerosi tentativi di frode che invece si vedono nei pagamenti con carte di credito, in cui chi ha ottenuto la merce cerca di annullare la transazione senza rimandare indietro quanto ha ricevuto;

- non genera inflazione: a differenza del denaro a corso legale, in cui le banche e le autorità possono decidere, in situazioni di particolare difficoltà, di stampare altre monete con un meccanismo chiamato facilitazione quantitativa[66], facendo in questo modo perdere di valore alla moneta e generando inflazione, in bitcoin ciò non può accadere. Questo perché è stabilito un numero massimo che può essere emesso, che è ventuno milioni;
- durevolezza e anticontraffazione: a differenza delle monete cartacee, i bitcoin non esistono in forma fisica, ma solo in forma digitale, hanno quindi una durata che può essere eterna. Inoltre, la regolarità di ogni bitcoin è garantita dalla blockchain, impedendo quindi ogni minimo tentativo di frode;
- fungibilità: sebbene alcune monete possano essere utilizzate in più paesi, come il dollaro o l'euro, spesso molte valute vengono accettate solo all'interno dei confini geografici della nazione che le emette. Il bitcoin invece non conosce limiti, e può essere utilizzato liberamente ovunque;

3.6 Svantaggi

A fronte dei numerosi vantaggi, si hanno però anche alcuni svantaggi, tra cui:

- necessaria conoscenza tecnologica: a differenza dei contanti e delle monete, di cui tutti hanno conoscenza ed esperienza, per i bitcoin è necessaria una familiarità con la tecnologia, che può essere anche minima per chi vuole semplicemente detenere bictoin in un portafoglio e spenderli;

[66] In politica monetaria, con allentamento quantitativo (o alleggerimento quantitativo o facilitazione quantitativa; sovente anche con la locuzione inglese quantitative easing, in sigla QE) si designa una delle modalità non convenzionali eterodosse e ultra-espansive con cui una banca centrale interviene sul sistema finanziario ed economico di uno Stato, per aumentare la moneta a debito in circolazione, https://it.wikipedia.org/wiki/Allentamento_quantitativo, Ottobre 2021

- volatilità: il prezzo delle criptovalute scende e sale di continuo[67] tanto che da alcuni viene definito addirittura "bolla finanziaria", questo può essere vantaggioso per chi le detiene a scopo speculativo, ma non per chi invece lo utilizza a scopo di investimento e mezzo di scambio. Proprio questo dettaglio tiene lontani molti individui, i cosiddetti "avversi al rischio", che preferiscono ancorarsi ai sistemi di investimento tradizionali;
- irreversibilità: oltre a essere un vantaggio, questa caratteristica può rappresentare anche uno svantaggio, in quanto se per errore si inserisse nella transazione un errato indirizzo del destinatario, i bitcoin inviati non possono essere richiesti indietro, in quanto difficile sarebbe determinare l'identità del destinatario, che in ogni caso sarebbe libero di tenersi ciò che ha ricevuto. Nei sistemi di pagamento tradizionali esiste invece la possibilità di annullare lo scambio e ottenere il rimborso di quanto trasferito;
- questioni legali e livello di riconoscimento: l'opinione giuridica riguardo i bitcoin varia da paese a paese, in alcuni è incoraggiato, in altri è vietato e reso illegale. Infatti, in alcuni paesi è riconosciuto come moneta ed è prevista una legislazione a riguardo, mentre nella maggior parte non è ammesso o non è presente un corpo di leggi che ne regoli l'utilizzo;
- mancanza di diffusione: al giorno d'oggi bitcoin non è molto diffuso, sono poche le aziende e i negozi che accettano questo tipo di pagamento;
- rischio di smarrimento: se i dispositivi sia fisici che digitali all'interno dei quali sono contenuti i bitcoin dovessero danneggiarsi o fossero smarriti, le criptovalute contenute all'interno sarebbero perse per sempre. Stessi rischi corre la chiave privata di accesso;
- possibilità di un futuro controllo delle autorità: è già stato spiegato cosa significhi decentralizzazione e i vantaggi che questa porta con se, ma non è escluso

[67] Ciò è legato anche al fatto che non ci sia un'autorità centrale o una banca centrale a sostenerne il valore, come avviene invece per le monete a corso legale

che in un futuro i governi decidano di regolamentarlo e prenderle sotto il proprio controllo;

Conclusioni

Per concludere è possibile effettuare un'analisi SWOT, che sintetizzi in un'unica rappresentazione quanto detto fin'ora, per avere un'idea generale del mondo del Bitcoin e delle criptovalute in generale

- **strenght:** i punti di forza del bitcoin e delle valute digitali in generale sono la blockchain e il processo di mining, con cui si riesce a ottenere un sistema di transazioni economiche, veloci e sicure, non facendo mancare l'assenza di un'autorità centrale;

- **weakness:** punti di debolezza del sistema sono la volatilità del valore delle criptovalute e la mancanza di diffusione. La volatilità fa si che ancora oggi molti investitori preferiscano i sistemi tradizionali, molto più sicuri e stabili, al rischio maggiore offerto dalle criptovalute. Proprio questo ne limita la diffusione. Sono poche infatti le attività commerciali che accettano questo tipo di pagamento nel mercato;

- **opportunities:** le opportunità principali sono offerte dalla tecnologia blockchain, che può essere implementata in molti settori della vita quotidiana, velocizzandoli e rendendoli più sicuri. Le applicazioni della blockchain sarebbero infinite, dal mondo delle banche, a quello della scuola e della legittmazione del voto elettorale, fino alla pubblica amministrazione, alla sanità e alle assicurazioni;

- **threats:** le principali minacce delle criptovalute e del bitcoin sono rappresentate dal possibile utilizzo in attività illecite, come il riciclaggio, offerto dalla mancanza di controllo da parte di un governo o di un'autorità

centrale, e quindi dall'assenza di un corpo di leggi specifico. Altro rischio è la possibilità di smarrimento o di furto della chiave privata, e quindi la perdita di ogni pretesa sul portafoglio di bitcoin;

La tecnologia, dunque, sostituisce completamente ogni altro elemento presente nei sistemi tradizionali, ma da sola non può però apportare grandi cambiamenti; sono gli utenti, aderendo al protocollo e scaricando i software nei loro dispositivi a renderla così diffusa e potente.

Si capisce che l'importanza e l'innovazione portate dal sistema della blockchain e delle criptovalute in generale non possono essere ignorate, ma non possono neanche essere lasciate totalmente a sé stesse.

Senza far perdere la caratteristica importante dell'autonomia e della decentralizzazione, le autorità dovrebbero iniziare a considerare e comprendere questo tipo di meccanismi, per evitare le spiacevoli situazioni offerte dalle minacce più critiche del bitcoin, come il riciclaggio o l'esportazione di capitali, e per cercare di "disciplinarle", dal punto di vista legale e anche fiscale.

I pagamenti tradizionali e quelli in criptovalute non vanno considerati come due alternative, ma vanno implementati insieme, magari in settori diversi.

Bibliografia

Bellini M, “Enciclopedia Treccani Decima Appendice”, Istituto della Enciclopedia Italiana, Roma, 2020

Capaccioli S, “Criptovalute e bitcoin: un’analisi giuridica”, Giuffrè, Milano, 2015

Chaum D L, “Blind signature for untraceable payments”, 1983

Dai W, “b-money an anonymous, distributed electronic cash system”, 1998

Ferri C, Blockchain&Made in Italy, Mondadori, Milano, 2020

Hughes E, “A cypherpunk’s Manifesto”, 9 Marzo 1993

Nakamoto S, “Bitcoin: a peer-to-peer electronic cash system”, 2008

Schiaroli I, Dark web & bitcoin. La nuova era della rete, Lantana Editore, Roma, 2013

Tonelli S, “Dall’oro al Bitcoin”, Youcanprint, 2017

Sitografia

https://academy.bit2me.com/it/chi-è-wei-dai/

https://bitcoin.org/it/

https://bitcoinveneto.it/perche-bitcoin/

https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni

https://coinmarketcap.com

https://coinmarketcap.com/it/currencies/the-sandbox/

https://www.treccani.it/enciclopedia/metaverso

https://cryptorobin.it/che-cose-la-proof-of-work/

https://dizionari.corriere.it/dizionario_italiano/H/hacker.shtml

https://dogecoin.com

https://ethereum.org/en/

https://focus.namirial.it/differenze-vantaggi-token-criptovalute/

https://it.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin

https://it.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin

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

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

https://it.wikipedia.org/wiki/Fork_(sviluppo_software)

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

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

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

https://litecoin.org/it/
https://localbitcoins.com/it/
https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt
https://ripple.com/xrp/
https://tech.everyeye.it/notizie/cos-e-metaverso-chiarezza-definizione-fedez-551703.html
https://tether.to/en/
https://www.bancobpm.it/magazine/glossario/iban/
https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/
https://www.borsaitaliana.it/borsa/glossario/criptovaluta.html
https://www.borsaitaliana.it/borsa/glossario/ipo-offerta-pubblica-iniziale.html
https://www.coinbase.com/it/learn/crypto-basics/what-is-a-stablecoin
https://www.consob.it/web/investor-education/criptovalute
https://www.fxempire.it/education/article/cosa-sono-gli-atm-di-bitcoin-e-come-funzionano-140337
https://www.ilsole24ore.com/art/draghi-studia-blockchain-e-bitcoin-dice-non-e-bce-dover-scrivere-regole--AEPESUzD
https://www.investopedia.com/terms/g/genesis-block.asp
https://www.iota.org
https://www.italianotizie24.it/iota-alcune-differenze-fondamentali-con-i-bitcoin/
https://www.namecoin.org

https://www.studiosamo.it/glossario/white-paper/
https://www.treccani.it/enciclopedia/cpu/
https://www.treccani.it/enciclopedia/mario-draghi
https://www.treccani.it/enciclopedia/open-source/
https://www.treccani.it/enciclopedia/peer-to-peer
https://www.treccani.it/enciclopedia/tablet
https://www.treccani.it/vocabolario/network/
https://www.treccani.it/vocabolario/usb/