LUISS

Dipartimento Di
Economia e Management

Tesi di laurea triennale
Cattedra di Economia dei Mercati e degli Intermediari Finanziari

# Lo Stato Attuale e il Processo Evolutivo delle Criptovalute

Prof.Claudio Boido
RELATORE

Alessandro Bolognesi
CANDIDATO

219881
MATRICOLA

Anno Accademico 2019/2020

*A mia mamma,*
*da sempre l'unica,*
*per crederci sempre.*

*A Caterina,*
*ai nervi saldi nelle notti bianche,*
*per farmi perdonare.*

# INDICE

# INTRODUZIONE

Il commercio per gran parte della storia dell'uomo è stato fondato su un principio di valore tangibile e comprensibile a tutti. Il baratto, che per secoli ha rappresentato il metodo di scambio per eccellenza, era fondato su rapporti di valore ben definiti tra le unità dei prodotti oggetto dello scambio, basati su tempi di produzione e quantità di lavoro necessaria e che fissavano i rapporti quantitativi corretti per rendere lo scambio equo. L'intensificazione degli scambi, delle necessità e degli spostamenti ha fatto si che il baratto lasciasse il posto all'uso di monete d'oro, comode, universalmente accettate ed estremamente liquide che consentissero di semplificare gli scambi e mantenessero sempre lo stesso valore. La nascita delle banche ha infine dato ai possessori di oro l'opportunità di depositarlo in un luogo sicuro ricevendo in cambio un foglio di carta che garantisse al portatore la restituzione dell'oro in qualunque momento, la banconota.

Nel corso del XX secolo tuttavia, una serie di eventi come la crisi del 29, la rivoluzione industriale e l'espansione incontrollata del consumo di massa, hanno messo in discussione i pilastri su cui da sempre si fondava il commercio. Una crescita così elevata degli scambi e del denaro in circolazione non permetteva più ai governi di garantire ai possessori la restituzione dell'oro. Il denaro perde ogni tipo di valore reale, assumendone uno fittizio attribuitogli dalle istituzioni che iniziano a detenerne il controllo. Il denaro è ufficialmente e irrimediabilmente legato al concetto di fiducia, nelle istituzioni, nei governi e nelle banche centrali, che si impegnano a preservarlo nel tempo e a garantirne la funzione di conservazione della ricchezza.

Questo nuovo sistema sorto nel 1970 con la fine degli accordi di Bretton Woods subisce un duro colpo nel 2008 quando la crisi globale crea un malcontento diffuso nei confronti delle grandi banche e porta alla creazione di un mercato parallelo che si sottrae al controllo e al dominio delle istituzioni e la cui linfa vitale è ancora la fiducia, questa volta però non nei confronti di un potere superiore, ma di tutti gli altri utenti (peer to peer). Nasce ufficialmente la blockchain su cui si basa il sistema di scambio delle criptovalute. Nei dodici anni trascorsi dalla sua introduzione questa realtà si è evoluta, approcciandosi dapprima a una nicchia ristretta di investitori, e successivamente a un numero sempre crescente di persone senza ancora raggiungere la diffusione dei contanti. È giusto dare a questo strumento la fiducia di cui necessita per sopravvivere? Quali limiti, regole, e garanzie sono necessari, e di quali abbiamo bisogno, per fare ciò? Come possiamo

sfruttare al meglio questa nuova realtà e come dobbiamo comportarci per evitare i grandi effetti collaterali che potrebbe comportare? Per rispondere a queste domande è necessaria un'analisi che mostri il funzionamento di questa innovazione, le opportunità e i rischi a cui ci espone.

Questo elaborato si propone di intraprendere questo percorso di analisi in quattro momenti distinti.

Nel primo capitolo si definisce la blockchain, come processo tecnologico pur rappresentando l'elemento portante dello scambio delle criptovalute. Saranno analizzati i processi, le caratteristiche e il funzionamento, percorrendo infine un'analisi dei possibili usi e vantaggi in ogni campo e ambito della vita quotidiana alternativi al mercato della moneta digitale.

Nel secondo capitolo si esamina come la criptovaluta si sia evoluta nel corso del tempo e soffermandosi sulle caratteristiche generali, i problemi irrisolti, gli orizzonti futuri, conducendo uno studio di casi specifici per sottolineare le diverse tipologie esistenti e le relative differenze.

Nel terzo capitolo vengono esaminati gli approcci regolamentari nel mondo (Asia, Stati Uniti, Regno Unito ed Unione Europea), analizzando il ruolo del cambiamento che dovrebbe essere attuato dalle banche centrali.

Nel quarto ed ultimo capitolo infine si approfondiscono le opportunità di investimento che le monete digitali offrono, la loro classificazione in relazione agli strumenti di investimento tradizionali e il coefficiente di correlazione con essi. Inoltre si esamina la probabilità della loro persistenza sul mercato e l'applicazione del Capital Asset Pricing Model proprio delle criptovalute. Infine si valuta l'entità dell'effetto distorsivo che il sentimento degli investitori provoca sui prezzi delle valute digitali.

# CAPITOLO 1 - BLOCKCHAIN

Blockchain è un termine che consente una traduzione in italiano solo letterale che corrisponde a "catena di blocchi". Questa tipologia di struttura dati appare per la prima volta nel 2008, quando un autore anonimo noto sotto lo pseudonimo di Satoshi Nakamoto le ha attribuito la funzione di libro mastro per tutte le transazioni svolte sul mercato dei Bitcoin, la prima forma di criptovaluta.

## 1.1 DEFINZIONI E CLASSIFICAZIONI

Dare una definizione chiara, sintetica e completa della blockchain è un compito arduo a causa del vasto impiego che si è fatto di questa tecnologia nei suoi 12 anni di vita e dei diversi punti di vista da cui può essere studiata e analizzata. Una prima definizione che merita di essere considerata descrive la blockchain come "un registro aperto e distribuito che può memorizzare le transazioni tra due parti in modo sicuro, verificabile e permanente[1]". In questo sistema, in cui ogni soggetto partecipante prende il nome di "nodo", ogni operazione (o transazione) che si verifica si collega alle precedenti attraverso un sistema che ne garantisce chiarezza e immutabilità grazie all'uso della crittografia.

Analizzata da un altro punto di vista più vasto e astratto possiamo definire la blockchain come "nuova internet" o "internet delle transazioni" in quanto la sicurezza di questo nuovo sistema apre la via a moltissime attività in ambito economico e finanziario impensabili con il "vecchio" internet a causa dei limiti imposti dalla struttura e dal funzionamento dello stesso. Questa visione fa quindi della fiducia il fulcro della blockchain, affiancando all'ormai ben noto "internet of people" il nuovo concetto di "internet of things" il cui sviluppo verte su 7 colonne portanti fondamentali rappresentate da:

1. Decentralizzazione
2. Trasparenza
3. Sicurezza
4. Immutabilità
5. Consenso

[1] Definizione proposta dalla CONSOB sulla propria pagina web nel report di presentazione di blockchain e criptovalute.

6. Responsabilità
7. Programmabilità.

Un'altra definizione, separata ma facilmente assimilabile alle precedenti, pone l'attenzione su un'altra grande novità apportata dalla blockchain ed è quella che la assimila al concetto di Distributed Ledger, un sistema privo di centri dove ogni "nodo" gode di grande autonomia grazie alle garanzie che la struttura della rete offre agli altri partecipanti. Ciò consente il superamento non solo dell'ormai datato concetto di Centralized Ledger, fondato sul rapporto uno-a-tanti e totalmente affidato al controllo dell'autorità, ma anche del Decentralized Ledger dove il controllo del vertice era soltanto ridotto e decentralizzato in vari satelliti di potere. Il fulcro del concetto di Distributed Ledger è dunque ancora una volta la fiducia tra le parti in un sistema dove nessuno può prevalere sugli altri e l'unico controllo esistente è del tipo peer-to-peer.

Alla luce dei tratti analizzati possiamo cercare di tracciare una definizione univoca di blockchain, tentando di racchiudere in poche righe i vari aspetti su cui abbiamo posto l'attenzione.

Il blockchain è costituito da un archivio dati immutabile contenente un libro mastro di transazioni, distribuito presso il pubblico, che si serve di un sistema crittografico per determinare la validità delle attività e basato sulla fiducia e il controllo reciproco.

Delineate le caratteristiche generali della blockchain è necessario focalizzarsi sulle diverse tipologie che è possibile incontrare. La classificazione si muove su due direttrici parallele basate su aspetti differenti.

La prima classificazione distingue sulla base dei permessi necessari per partecipare al processo di verifica e distingue tra: a) Permissionless blockchain, dove ognuno può prendere parte al processo di verifica senza necessità di autorizzazione anche in cambio di un ritorno economico; b) Permissioned blockchain, dove i nodi che si occupano dell'attività di verifica sono predeterminati da un'autorità.

La seconda ragione di classificazione distingue tra blockchain pubblica, dove ognuno può accedere o inscrivere transazioni nel sistema, e blockchain privata, dove questo accesso o l'iscrizione di dati sono limitati a un gruppo ristretto di soggetti.

## 1.2 FUNZIONAMENTO

Per apprezzare e comprendere al meglio i benefici della blockchain è necessario analizzarne i componenti, la struttura e il funzionamento concreto. Come abbiamo visto

questa tecnologia si fonda su un protocollo di comunicazione basato sulla logica del database distribuito (Distributed Ledger), ovvero in cui i dati non sono immagazzinati in un solo computer ma su più dispositivi connessi. Il procedimento che siamo interessati a studiare è quello attraverso cui queste parti riescono ad ampliare la catena con nuovi blocchi. Le componenti fondamentali del processo, che elenchiamo di seguito brevemente per approfondirne successivamente funzioni e legami sono:

- Nodo: ogni soggetto partecipante alla blockchain, è rappresentato fisicamente da ognuno dei dispositivi connessi che formano la rete.
- Transazione: consiste in un'interazione tra due nodi e dai dati tra essi scambiati
- Blocco: è costituito da una serie di transazioni verificate e rese immutabili
- Ledger: è composto dai vari blocchi connessi tra loro e rappresenta un libro mastro ad accesso solitamente pubblico che ordina tutte le operazioni verificate e immutabili.
- Hash: rappresenta un'operazione che traccia una chiave identificativa di ogni blocco trasformando una stringa di dati a lunghezza variabile in una identificativa a lunghezza determinata. Registra tutte le informazioni di un blocco e del precedente creando la catena che collega i due blocchi.

*Dalle transazioni alla "chain"*

Come emerge da questa prima analisi, il processo centrale di accrescimento della catena è rappresentato dal passaggio da transazioni a blocchi e da blocchi a blockchain e dal momento dell'autenticazione approvato da tutti gli altri partecipanti al sistema. Partendo dalla componente di base, ovvero la singola transazione, vediamo come questa sia costituita da tre elementi individuati dall'acronimo S.T.R.:

- Sender (mittente)
- Transaction (transazione)
- Receiver (Ricevente).

Quando tra due nodi ha luogo una transazione è necessario riportare sul server i dati inerenti all'oggetto della stessa (caratteristiche del bene o del servizio considerato) oltre che di Sender e Receiver. Il tutto viene approvato e confermato con la firma digitale privata e pubblica del mittente. La transazione entra successivamente a far parte di un blocco, ovvero un agglomerato contente anche altre transazioni, che deve essere

autorizzato dagli altri nodi della blockchain che ne verificano veridicità e regolarità. Infine, dopo l'approvazione, il blocco si dice "risolto" ed entra a far parte della blockchain legandosi al blocco precedente. Questo passaggio comporta finalmente la pubblicazione del blocco sulla blockchain e la visibilità a tutti i nodi partecipanti al sistema. Giunta a questa fase ogni transazione è definitivamente immutabile nel tempo. L'immutabilità è infatti garantita dal fatto che per modificare un blocco ormai inserito non esiste un server centrale che se violato e modificato riporta la modifica su tutti gli altri. Sarebbe dunque necessario violare contemporaneamente tutti i nodi partecipanti per modificare ogni copia del ledger salvata su di essi: è questa la grande rottura col passato rappresentata dal Distributed Ledger.

*Integrità dei Dati*

Una delle principali peculiarità della blockchain è rappresentata dalla sicurezza e integrità offerta sui dati. Prima di entrare nel merito degli strumenti che offrono questo genere di protezione è necessario comprendere cosa si intende per integrità. Questo concetto può essere infatti articolato in tre diversi rami:

- Vincoli semantici; ovvero regole sul corretto stato del sistema durante le operazioni. La funzione principale di questi vincoli e schemi obbligatori è garantire un certo grado di protezione contro modifiche dei dati.
- Identificazione, autorizzazione e audit; cioè obblighi di riconoscimento e verifica dell'identità nonché controllo della validità delle operazioni svolte
- Autorizzazione; una serie di regole mirata a definire chi ha diritto ad accedere a un determinato tipo di informazione. Distingue tra chi può inserire dati, chi può svolgere attività di sorveglianza sulle transazioni, ecc.

Negli anni molti approcci e studi hanno proposto diversi punti di vista e diversi strumenti per il mantenimento dell'integrità dei dati. I due modelli che analizzeremo come esempi degni di nota sono il modello di Clark-Wilson[2] e il modello Biba.

Il modello CW, teorizzato la prima volta nel 1987 e solo successivamente applicato al contesto blockchain, si basa su due assunzioni fondamentali: il concetto di transazione, identificato come una serie di operazioni che modificano un sistema da una forma ad un'altra, e che nel contesto della blockchain può essere inteso come ogni aggiunta di dati

[2] Da ora anche CW

alla catena e, dunque, la verifica e l'accertamento dei dati aggiunti; la separazione dei compiti e degli oneri tra le parti attive del sistema, che si sostanzia nel concetto di autorizzazione analizzato in precedenza dove vengono attribuiti poteri e vincoli ai diversi attori. Secondo il CW è possibile catalogare tutti i dati all'interno di due categorie: i CDI (Constrained data items) e gli UDI (Unconstrained data items), dove i CDI sono definiti constrained in quanto sono quei dati che possono essere modificati solo attraverso procedure definite e verificate e che al di fuori di esse sono verificati per assicurarne l'integrità, mentre gli UDI sono tutti gli atri dati meno rilevanti. Posta questa analisi preliminare il CW propone sei regole da rispettare per mantenere l'integrità di un sistema:

- Ogni processo trasformativo di un CDI deve mantenere l'integrità dello stesso.
- Solo alcuni soggetti sono autorizzati a compiere processi trasformativi dei CDI.
- Tutti i nodi del sistema devono essere autenticati.
- È necessario un file su cui siano registrate tutte le transazioni che si verificano nella rete.
- È possibile che un UDI diventi un CDI
- Solo un soggetto autorizzato può modificare le autorizzazioni degli altri nodi.

Un approccio alternativo al CW è rappresentato dal modello Biba, anch'esso antecedente alla catena a blocchi e in seguito adattato (1977). Il concetto chiave di questo modello è sintetizzabile nella frase "no read down, no write up"[3], il cui significato consiste in un vincolo per gli utenti che possono creare contenuti solo a o al di sotto del loro livello di integrità, mentre possono vedere contenuti solo a o al disopra del loro livello di integrità. Infatti secondo questo modello dati e soggetti sono suddivisi all'interno di livelli di integrità, e la struttura funziona in modo che nessuno possa corrompere dati di un livello superiore o essere corrotto da dati di livello inferiore.

*Crittografia e altri strumenti per il mantenimento dell'integrità.*

Quali strumenti esistono per far si che i principi e gli obiettivi appena analizzati vengano effettivamente rispettati? Oltre all'utilizzo fatto dalle due parti coinvolte nella transazione della doppia chiave pubblica e privata per la protezione dei dati, che rappresenta di per se

[3] Concetto opposto a quello di altri modelli come il Bell-Lapadula basati sul concetto "no write down, no read up".

un certo grado di protezione, un altro importante istituto rende la blockchain ancora più affidabile: il Timestamping.

Con questo termine intendiamo l'applicazione della marca temporale alle transazioni che si verificano su una blockchain. La marca temporale, o Timestamp, consiste in una stringa di caratteri immutabile e unica che individua un certo momento nel tempo in cui si è verificato un certo avvenimento o, nel nostro caso, una certa transazione. L'immutabilità di questo codice di collocazione temporale rende ancor più difficile la modifica di un dato successivamente alla sua approvazione e registrazione. Spesso il timestamping è una pratica attuata da terze parti fidate come ad esempio la TSA (Time Stamping Authorities) che offre una registrazione della marca temporale sicura, reale e garantita.

Un ultimo strumento di controllo che contribuisce a rendere quasi impossibile una modifica illecita del sistema blockchain è l'hash, una funzione matematica che processa i dati di ogni blocco consegnando un output rappresentato da una stringa di lunghezza sempre uguale, per cui l'hash corrispondente a una sola parola avrà la stessa dimensione dell'hash di una frase complessa. Le stringhe della stessa dimensione rendono quindi impossibile comprendere il contenuto delle stesse semplicemente osservandole. A ciò si aggiunge che ad ogni blocco non corrisponde un solo hash, bensì l'hash del blocco precedente, un Timestamp, un version number, e un target hash.

La pratica di risoluzione di questi complessi problemi matematici e di crittografia rientra nella sfera del mining. I miners sono infatti coloro che si occupano di aggiungere e congiungere i nuovi blocchi a quelli più vecchi e di garantire che questi siano protetti e sicuri. Nonostante anche nelle blockchain come in altri campi o nei sistemi del passato i miners operino sotto compenso, la nuova rete rappresenta ancora una volta una rivoluzione, in quanto in un contesto così decentralizzato l'attività di mining viene svolta con modalità che ben poco si discostano dalla filosofia e dal modo di operare dei contesti open source, contraddistinti da grande collaborazione e dialogo tra più parti che offrono il loro contributo.

### 1.3 AMBITI APPLICATIVI

Capita spesso che la blockchain venga associata automaticamente ed esclusivamente ai bitcoin. Tuttavia nonostante la blockchain trovi nelle criptovalute non solo il primo ma anche il suo più ampio utilizzo (della cui analisi ci occuperemo successivamente in maniera approfondita), è necessario trattare anche i numerosissimi nuovi campi in cui sta

trovando uno spazio sempre crescente la catena a blocchi, così da mettere in luce l'incredibile potenziale innovativo che essa offre. In particolare i campi in cui il processo per blocchi può trovare applicazione e portare benefici sono:

- Finanza
- Assicurazioni
- Sanità
- Pubblica Amministrazione
- Energia
- Mercato agroalimentare
- Media

*Settore Finanziario*

Trattando inizialmente il settore finanziario, possiamo individuare 3 principali contesti[4] nell'ambito della corporate finance in cui la blockchain offre possibilità innovative:

- Supply chain: creando un registro condiviso e sicuro delle transazioni così da intensificare la trasparenza nelle reti tra fornitori e clienti, riducendo la selezione avversa e riducendo i costi di transazione, di acquisizione di informazioni e di protezione legale, offrendo maggiori opportunità anche alle imprese più piccole riducendo gli impedimenti dati dalle scarse risorse.
- Finanziamenti: incrementando gli attuali mercati attraverso la decentralizzazione, riducendo rischi e costi di transazione e introducendo nuovi strumenti finanziari come "digital assets" con caratteristiche uniche rispetto agli strumenti già noti, e semplificando la monetizzazione liquidando i titoli attraverso i token. Particolare rilevanza assume l'ICO (initial coin offering), che ha contribuito molto allo sviluppo della blockchain in questo settore. L'ICO da alle imprese la possibilità di raccogliere capitale dando in cambio token o coin che rappresentano uno strumento nuovo e distinto sia dalle obbligazioni (in quanto spesso non hanno nessuna garanzia di restituzione del principal) sia dalle azioni (in quanto non concedono alcun diritto di voto), rappresentando quindi un grande vantaggio per le società che riducono gli oneri a cui sono sottoposti.

[4] Catalogazione tratta dallo studio di J.P. Morgan "Blockchain and the decentralization revolution, a CFO's guide to the potential implications of distributed ledger technology"

- Pagamenti di cupon e acquisto di titoli: incrementando la trasparenza delle transazioni che possono essere seguite in ogni fase dagli attori coinvolti, eliminando i costi di intermediazione e riducendo la distanza tra data di negoziazione e data di valuta dai 2 giorni lavorativi attuali (T+2) a T+0.

*Settore Assicurativo*

Un altro campo in cui la blockchain può rappresentare un grande risorsa è quello della lotta alle frodi in ambito assicurativo[5]. Il rischio di subire frodi di vario genere è un problema attuale e fino a pochi anni fa gli strumenti di difesa erano pochi e relativamente facili da eludere. L'accesso a transazioni sicure e decentralizzate permette di disporre di un miglior controllo e gestione dei dati, report e valutazioni più precise e possibilità di fare previsioni più realistiche. La blockchain consente inoltre alle compagnie assicurative di integrare i dati a loro disposizione in una rete con terze parti così da ridurre i costi e migliorare la gestione del rischio. In termini più "pratici" e entrando in campo più tecnologico che finanziario, un'altra via di applicazione della rete blockchain rappresenta un sistema antifrode sfruttando condivisione e immagazzinamento di informazioni raccolte tramite il GPS, fungendo anche da deterrente per i furti d'auto e portando benefici non solo per le compagnie assicurative, ma anche per il possessore medio di automobile nella quotidianità.

*Settore Sanitario*

In ambito sanitario la blockchain rappresenta una risorsa rilevante svolgendo la funzione di registro dati dei pazienti. Una rete condivisa tra medici di un'azienda ospedaliera o tra più strutture sanitarie permette di accedere rapidamente ai trascorsi e alla cartella clinica di ogni paziente, garantendo una maggiore rapidità decisionale e operativa che in campo sanitario è estremamente rilevante. Inoltre così come per qualsiasi organizzazione, questo sistema da l'opportunità anche per ospedali e cliniche di una condivisione documentale più accessibile e più sicura del passato.

[5]Tema approfondito da un report di Ernst&Young: Blockchain technology as a platformfor digitalization, implications for the insurance industry

*Settore Pubblico*

Nella pubblica amministrazione la blockchain potrebbe rappresentare la chiave di volta per l'implementazione dell'e-voting, ovvero il voto a distanza, tema molto discusso negli ultimi anni ma ostacolato da evidenti limiti di sicurezza come il rischio di manipolazione dei dati o degli elettori stessi e varie azioni di sabotaggio. Proprio la catena a blocchi potrebbe ridurre questi rischi verificando l'unicità del voto, l'identità del votante e garantendo l'immutabilità dei dati successivamente al voto.

*Settore Energetico*

Il "mercato" dell'energia è tradizionalmente visto come un settore fondato su una relazione univoca tra produttore e cliente dove il primo vende il prodotto al secondo. Nella realtà dei fatti il rapporto può essere approfondito e incrementato assumendo più vie, in ciò consiste il concetto di smart energy. La blockchain rappresenta uno strumento fondamentale per raggiungere questo obiettivo attraverso le relazioni P2P (peer to peer) che si instaurano tra i vari nodi della rete, che daranno a chi ne dispone in eccesso la possibilità di rivendere energia a chi manifesta invece urgenza nel breve termine rendendo il settore energetico più "democratico" rispetto a come si è abituati ad intenderlo.

*Settore Agroalimentare*

La blockchain si presta a risolutrice di problemi anche nel campo alimentare e agricolo. Un argomento rilevante ad oggi particolarmente nel nostro paese e nell'Unione Europea è legato alle norme sulla chiarezza riguardo l'origine di materie prime e prodotti in campo agricolo e alimentare. Il sistema a blocchi in questo contesto consente di raggiungere un grado di trasparenza molto elevato mettendo fine ai tentativi di eludere e ingannare il consumatore e le autorità grazie ad un sistema di tracciabilità del prodotto in termini di crescita, lavorazione, alimentazione e trattamento, trasporti, ecc.

*Settore Media*

Un problema che spesso impegna chi lavora nel settore dell'intrattenimento, che si tratti di cinema, musica arte, ecc. è rappresentato dalla pirateria. L'ampia disponibilità di strumenti media e online, social network e piattaforme di ogni genere, rende complicato tenere sotto controllo la distribuzione dei contenuti multimediali, che spesso esce dalle vie autorizzate e predisposte per diffondersi gratuitamente attraverso strade parallele. La

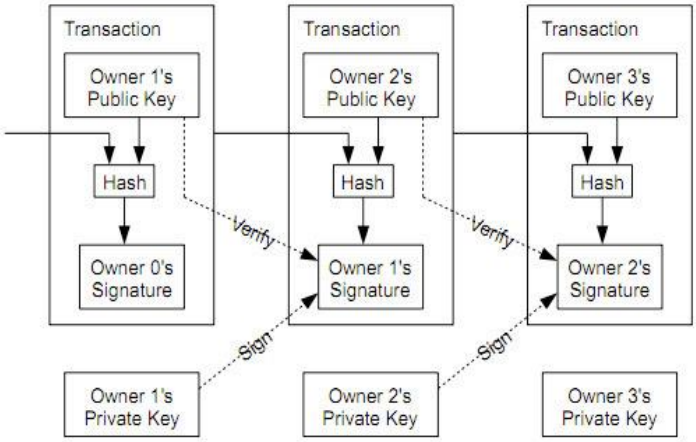
blockchain grazie alla crittografia offre ampie garanzie sulla proprietà intellettuale di un'opera artistica di qualsiasi genere riducendo le frodi e incrementando i profitti di chi opera nel settore

## 1.4 BLOCKCHAIN E CRIPTOVALUTE

Entriamo ora nel merito di quello che è il più grande campo di applicazione della tecnologia blockchain: le valute digitali. La prima blockchain nasce insieme alla prima valuta digitale valida e affidabile, il bitcoin. Altri tentativi in passato erano stati fatti per immettere sul mercato delle criptovalute ma i risultati si erano rivelati tutti fallimentari a causa dei limiti tecnologici a cui non si era in grado di far fronte. Non è dunque un caso che il bitcoin abbia preso piede in concomitanza all'avanzare della blockchain, in quanto proprio questa rivoluzionaria tecnologia ha permesso di superare ostacoli che apparivano prima insormontabili. Entrando maggiormente nel dettaglio, il più grande limite dei sistemi del passato era l'incapacità di far fronte al problema del double spending. Il problema del double spending è un potenziale errore in una criptovaluta a causa del quale la stessa singola moneta (token) può essere spesa più di una volta[6]. Infatti caratteristica tipica del digitale è quella di poter riprodurre una stessa cosa all'infinito con un costo marginale pari a zero[7], fattore che in molti campi rappresenta un'immensa risorsa ma che quando si tratta di moneta rappresenta un ostacolo da eliminare. In che modo dunque la blockchain technology ha segnato un punto di svolta? Con ciò che possiamo definire "l'identità della moneta". Attraverso la crittografia ogni moneta possiede un codice, un nome, che la distingue dalle altre.

[6] Definizione tratta dal discussion paper di Usman W. Chohan della University of new South Wales, Canberra

[7] In realtà S. Nakamoto nel suo white paper di presentazione del progetto blockchain e bitcoin sostiene che il problema del double spending possa verificarsi anche nell'economia reale, se non fosse che a evitare che dilaghi esiste l'istituzione della zecca di stato. Secondo la sua visione tuttavia la zecca rappresenta un'entità da cui l'economia reale dipende, e il suo obiettivo nel creare monete digitali è proprio l'eliminazione di questo genere di dipendenze da organi troppo accentrati.




*Dal white paper di S. Nakamoto, 2008, illustrazione del processo di verifica delle transazioni.*

Questo fa si che al verificarsi di una transazione di qualsiasi genere la moneta con un determinato codice deve passare di mano impedendo al vecchio detentore di riutilizzarla infinite volte. Inoltre con l'aggiornamento di tutti i blocchi visibili ad ogni nodo della rete, tutti saranno al corrente del trasferimento che non potrà in alcun modo essere occultato. In aggiunta, la moneta stessa, registrerà nella sua "memoria" la transazione di cui è stata oggetto, portandola con sé e mostrandola al potenziale beneficiario di una nuova transazione. Esso avrà infatti visione delle firme che vengono poste nel tempo ogni volta che la moneta passa di mano e che saranno a lui necessarie per conoscere il passato della moneta. Questo sistema sostituisce il controllo accentrato di un'autorità ad un rapporto peer to peer dove tutti controllano e sorvegliano la correttezza delle transazioni.

# CAPITOLO 2 – CRIPTOVALUTE

Nella seconda metà del 2008 la grande crisi finanziaria imperversava danneggiando l'economia mondiale. In questo contesto non tardò a diffondersi un comune senso di sfiducia nei confronti di banche e intermediari finanziari, additati come responsabili del disastro che stava causando immense difficoltà a stati e famiglie in ogni parte del globo. In questo contesto un anonimo programmatore noto con lo pseudonimo di Satoshi Nakamoto, proprio con l'intento di cercare un'alternativa ai grandi centri del potere finanziario e di gestione delle risorse monetarie, pubblica nell'ottobre del 2008 un white paper dal nome "Bitcoin: a Peer-to-Peer Electronic Cash System", in cui spiega i principi fondanti e i meccanismi di funzionamento della prima blockchain su cui si reggeva il sistema della prima moneta virtuale. Nel gennaio del 2009, solo 4 mesi dopo, venne introdotta la Bitcoin Cryptocurrency. Nonostante uno scetticismo iniziale questo sistema iniziò ad affermarsi trovando sempre più sostenitori, investitori e utilizzatori e nel giro di pochi anni il numero di criptovalute è aumentato in modo significativo. Oggi le valute digitali sul mercato sono 2677[8]. Per comprendere cos'è una criptovaluta ne analizzeremo di seguito i tratti caratteristici, la struttura e il funzionamento, focalizzando l'attenzione sull'impatto che ha avuto sulla moneta tradizionale e percorrendo un'analisi di alcuni esempi specifici.

## 2.1 TRATTI CARATTERISTICI E FUNZIONAMENTO

L'etimologia del termine criptovaluta è riconducibile a due parole distinte: cripto e valuta, che descrivono uno strumento di pagamento "nascosto" (dal greco κρυπτός), "nel senso che è visibile/utilizzabile solo conoscendo un determinato codice informatico"[9]. Perché una criptovaluta funzioni e mantenga la sua validità è necessario che il sistema che la governa rispetti tre principi fondamentali:

- Nessun soggetto deve poter essere in grado di pagare due volte con la stessa unità di moneta. (double spending)
- In nessuna occasione due o più parti devono poter rivendicare la proprietà di una stessa unità di moneta.

[8] Dato aggiornato a giugno 2020.
[9] www.consob.it

- Nessun nodo della rete e nessun altro in generale, al di fuori dell'emittente, deve essere in grado di creare nuova moneta.

*I Token e le Transazioni*

Lo strumento virtuale corrispondente alla banconota delle valute fisiche (o ad altri strumenti ed assets finanziari tradizionali) è definito token. Un token è infatti una stringa di informazioni digitali che conferisce un diritto di proprietà ad un soggetto. I token possono essere scambiati ad un valore intrinseco che cambia nel tempo rappresentando quindi lo strumento attraverso cui avvengono gli scambi nelle criptovalute. I differenti tipi di token possono essere catalogati in 3 classi:

- Token di classe 1: si presenta come "coin" che non prevede controparti e può essere utilizzato nelle transazioni che si verificano su una blockchain
- Token di classe 2: attribuiscono al detentore diritti esercitabili nei confronti dell'emittente degli stessi. Se i token di classe 1 sono uno strumento molto simile alla moneta fisica, quelli di classe 2 sono assimilabili a titoli di credito in particolare di 4 tipi:
    1. Token conferenti diritto a ricevere pagamenti futuri
    2. Token come asset
    3. Token per ricevere pagamenti standard futuri
    4. Token che danno diritto a ricevere una determinata prestazione.
- Token di classe 3: offrono diritti di comproprietà che conferiscono proprietà legata ad altri diritti come diritto di voto, diritto economici di vario tipo.

Occorre fare un'ulteriore precisazione. Gli strumenti simili a moneta disponibili sulle varie blockchain si distinguono tra token e coin. Capita spesso che questi due termini siano considerati come perfetti sinonimi ma così non è. I coin sono strumenti che fungono esclusivamente da mezzi di pagamento, come qualsiasi moneta fiat emessa dalle banche centrali, senza garantire al portatore nessun genere di diritto o servizio di altro tipo. Il concetto di coin è quindi assimilabile esclusivamente ai token di classe 1, mentre bisogna fare attenzione a non confonderlo con il token di classe 2 o 3. Il token ha dunque un ruolo centrale nel funzionamento efficace delle transazioni. Infatti esso trasporta due informazioni codificate fondamentali: l'identità del possessore attuale e quella del soggetto di provenienza. Il primo di questi codici fa si che il token sia protetto da una

chiave pubblica di cui solo il possessore conosce la corrispondente chiave privata, necessaria per poterne disporre e inserirlo in delle transazioni. Il secondo sull'identità del vecchio possessore è rappresentato in realtà dal codice identificativo del "vecchio" token. Infatti ogni volta che ha luogo uno scambio non si verifica un "passaggio di properietà" dello stesso token ma chi spende il proprio token ne genera uno nuovo che contiene la chiave pubblica del nuovo proprietario e il codice del vecchio token (ovvero quello che si sta spendendo). Questo renderà token posseduto "speso" e quindi non più utilizzabile, mentre invierà quello nuovo alla controparte dello scambio. Una critica mossa nei confronti di questo sistema sostiene che sia troppo "personale", ovvero che per garantire la correttezza dei processi e limitare le frodi trascuri il diritto comunque spettante ai soggetti attivi di mantenere un certo grado di anonimità. Allo stato dei fatti ciò non è del tutto vero, in quanto l'identità provata dal codice è virtuale ed è rappresentata da uno pseudonimo in alcun modo riconducibile all'identità reale di un soggetto che desideri operare in segreto e per cui è sufficiente scegliere uno pseudonimo di fantasia.

*Initial Coin Offering*

Per quanto riguarda l'emissione e vendita di token presso il pubblico, questa si svolge in modo simile all'Initial Public Offering tipica delle azioni e prende il nome di Initial Coin Offering (ICO). Mediante un'ICO, nuove società e startup innovative hanno la possibilità di reperire capitale per avviare e sviluppare la loro attività vendendo token su una blockchain agli investitori interessati, per questo la ICO è assimilabile a un processo di crowdfunding. Non essendo regolamentate le ICO possono assumere caratteristiche ben diverse tra loro. In particolare il prospetto di ogni ICO è rappresentato dal suo white paper, un documento che riassume aspetti fondamentali di un'ICO come obiettivi di raccolta, progetto della società, informazioni e dati sulla governance, un calendario con gli scopi che si desidera raggiungere. In questo documento si trova inoltre la durata dell'ICO che generalmente si svolge in un range temporale molto vario che va da alcune settimane a qualche mese. La correttezza e la precisione del white paper sono molto importanti ai fini della serietà e dell'affidabilità del progetto. Un'altra importante caratteristica delle ICO è che, differentemente da ciò che si potrebbe pensare, spesso a queste non si partecipa con valute tradizionali ma con altre criptovalute, che sono definite dalla società che la organizza e solitamente comunicate attraverso il White paper.

Superata la fase dell'ICO, come nel mercato azionario, anche i token hanno un attivo mercato secondario su cui hanno luogo gli scambi e le transazioni tra diversi investitori che grazie all'elevata volatilità del valore dei token compiono in questo mercato forti azioni speculative. L'analisi del fenomeno ICO è ad oggi complessa poiché le ICO rispetto alle IPO non hanno una piattaforma di negoziazione dedicata e sono sottoposte a minori obblighi di registrazione dati e partecipanti, per cui risulta piuttosto difficile riuscire ad avere una visione d'insieme completa e precisa.

## 2.2 IL DENARO PRIMA E DOPO LE CRIPTOVALUTE

La differenza principale tra questa forma di moneta e quelle classiche è l'inesistenza di questa dal punto di vista fisico, sia in formato cartaceo che metallico. Le monete virtuali inoltre, a differenza di quelle tradizionali, non hanno corso legale (principio per cui ognuno è obbligato ad accettarle come mezzo di pagamento), per questa ragione l'accettazione delle stesse come forma di pagamento è su base prettamente volontaria. Come sappiamo le monete tradizionali svolgono poi il compito di unità di conto. Le criptovalute invece, a causa dell'elevata volatilità che le contraddistingue, sono inidonee a svolgere questo genere di ruolo. Per quanto riguarda la funzione di riserva di valore, poichè il numero di unità di criptovaluta producibili è limitato il loro valore aumenterà all'incremento dell'utilizzo fatto della stessa, ma se questa cade in disuso il loro valore precipita. Quindi, per quanto rappresentino un mezzo per la riserva di valore, sono rischiose in termini di volatilità del valore stesso nel lungo termine. Le criptovalute inoltre hanno un approccio molto diverso nei confronti del loro detentore, e il modo in cui un individuo le guarda, le usa e vi si rapporta è del tutto diverso da quello delle valute tradizionali. Ad esempio una persona comune e non avvezza a questo genere di moneta, estranea al mondo delle valute digitali ed al settore delle innovazioni tecnologiche e finanziarie, tende a tenere in grande considerazione il rapporto fisico con il denaro e necessita di un certo grado di educazione ed abitudine prima di essere disposto a distaccarvisi.

Le monete virtuali sono inoltre basate su un principio di attribuzione del valore completamente innovativo rispetto alle sue predecessore. Infatti il valore delle valute

tradizionali, successivamente alla fase storica del gold exchange standard[10] e agli accordi di Bretton Woods[11], è garantito dalle banche centrali, per cui non godono più di alcun valore intrinseco ma sono protette dalle istituzioni finanziarie statali che si occupano di preservarne e stabilizzarne il valore controllandone l'emissione. Questo principio non vale per le valute digitali. Infatti in questo caso ci troviamo di fronte ad un sistema in cui la quantità emessa è predeterminata e fissa indipendentemente dagli andamenti del mercato e non esiste un effettivo impegno di un organo centrale per stabilizzarne il valore. Da ciò la causa dell'alta volatilità delle criptovalute, dipendenti interamente dai movimenti del mercato e dalla domanda di moneta.

## 2.3 VANTAGGI, RISCHI E SFIDE DELLE VALUTE DIGITALI

Analizziamo, prima di trarre delle conclusioni sulle criptovalute, quali sono i vantaggi e i problemi legati a questo genere di strumento, dando la giusta attenzione anche all'effettivo sviluppo della tecnologia e alle opportunità di crescita future che potrebbero offrire nuove vie di risoluzione dei problemi riscontrati. Molti degli aspetti positivi delle valute digitali coincidono con quelli già citati trattando la blockchain[12] (che costituisce infatti la base del funzionamento delle criptovalute). In particolare:

- Trasparenza
- Sicurezza
- bassi costi di transazione
- finanziamento per l'innovazione

La trasparenza è relativa al fatto che tutte le transazioni siano svolte pubblicamente e possano essere liberamente consultate e verificate da tutti. Il che rende quasi impossibile commettere frodi o transazioni poco chiare in questo sistema senza attirare l'attenzione altrui.

La sicurezza della tecnologia hash (versione 256-bit) usata dal sistema bitcoin e dalle principali criptovalute offre ampie garanzie in termini di integrità della rete ma anche di

[10] Rimasto in vigore dall'800 al 1944, garantiva la convertibilità di ogni banconota in una certa quantità di oro che poteva essere ritirata in qualsiasi momento.

[11] Che prevedevano un sistema di collegamento tra i vari tassi di cambio dei diversi paesi che dovevano essere mantenuti stabili per evitare il verificarsi di fenomeni inflazionistici fuori controllo

[12] Vedi in particolare i paragrafi 1.1 e 1.2

protezione dei wallets e garantisce che ogni transazione venga effettivamente svolta dal proprietario del wallet.

I minori costi di transazione sono una risorsa tipica delle attività online. Nel settore delle valute digitali questo è particolarmente evidente grazie alla possibilità di svolgere ogni transazione attraverso un contatto diretto tra gli interessati senza alcuna necessità di intermediazione. Una totale assenza di organi di sorveglianza e di "addetti ai lavori" (essendo la verifica della regolarità e del funzionamento dei processi nelle mani degli stessi nodi della rete) riduce notevolmente i costi dell'intero sistema che ricadrebbero altrimenti sugli utenti. Per concludere, un vantaggio economico attuale (anche se presumibilmente momentaneo, sopratutto in caso di crescita del fenomeno), è legato al vuoto normativo odierno, causato da incapacità delle istituzioni di regolare il fenomeno e rifiuto stesso di volerlo accettare e che comporta spesso un'assenza di tassazione dei proventi ottenuti con questo tipo di strumenti.

Un ultimo aspetto di grande rilevanza consiste nella spinta innovativa che il sistema delle criptovalute offre alle società che possono, attraverso le ICO, attirare nuove categorie di investitori, incrementando i capitali raccolti e accedendo più opportunità di investimento. Inoltre una tecnologia innovativa apre sempre la via a nuove opportunità di sviluppo rappresentando un motore per il progresso.

I problemi legati a questo strumento sono legati in parte ad uno stato ancora primordiale della tecnologia su cui si fonda (soprattutto se si considerano le effettive opportunità di sviluppo), e in parte al rischio che una crescita incontrollata del fenomeno possa far venire meno i vantaggi che adesso rappresentano un pilastro della tecnologia.

Nello specifico individuiamo otto attuali e potenziali rischi e difficoltà:

1. Mercato limitato
2. Perdita di Trasparenza
3. Perdita dell'anonimità
4. Instabilità
5. Deflazione
6. Problema dei Lost Coins
7. Crescita dei poteri centrali
8. Inefficienza Computazionale

Allo stato attuale dei fatti, il mercato si presenta ancora come un contesto elitario, in cui solo alcuni sono disposti ad investire, che mette in circolazione uno strumento la cui

accettazione è ancora su base volontaria e che l'autorità si rifiuta in molti casi di disciplinare. Questi aspetti devono necessariamente essere affrontati e superati affinché la fiducia nei confronti della moneta digitale aumenti e si diffonda. Complice sarà anche il tempo che serve alle persone per accettare un cambiamento nel loro rapporto con il denaro.

Alla soluzione dell'espansione del mercato, sono strettamente legati tre problemi successivi, ovvero la perdita di Trasparenza e/o dell'anonimità e la crescita dei poteri centrali. Un'espansione del mercato delle criptovalute, qualora non venisse condotto in maniera corretta e perfettamente bilanciata, rischierebbe infatti di andare ad abbattere una delle tre colonne di valore su cui l'intero sistema si regge: un immenso incremento delle transazioni quotidiane, necessario per accrescere il mercato e conseguenza logica del fatto in sé, renderebbe chiaramente più complesso portare avanti il controllo di verifica di tutte le operazioni svolte, le identità degli attori. Allo stesso modo il tentativo di garantire maggiore sicurezza e trasparenza potrebbe eliminare la possibilità per gli utenti di operare sotto pseudonimo così da proibire attività illecite svolte sotto falso nome. Questo tuttavia eliminerebbe ogni possibilità di operare in modo anonimo, "ricostruendo" la colonna della trasparenza ma abolendo quella dell'anonimato, tenuta in grande considerazione dagli utenti. Inoltre, per garantire un miglior controllo, potrebbe risultare necessario istituire organi di sorveglianza centrale, nonostante essi rappresentino quel tipo di potere da cui Nakamoto desiderava allontanarsi programmando questa rete.

Un ulteriore problema molto attuale e che genera difficoltà a far avvicinare le persone alle monete virtuali è dato dalla forte volatilità del valore della moneta. Come abbiamo visto in precedenza, sono solitamente gli organi centrali con la gestione della politica monetaria a tenere sotto controllo la stabilità delle monete fisiche. Proprio l'assenza di un organo di governo, oltre al principio basato non sul variare la quantità di moneta in circolazione bensì sul mantenerla costante indipendentemente dalla domanda, rende il valore delle monete virtuali estremamente volatile e incerto.

Un altro problema, attualmente piuttosto diffuso ma presumibilmente risolvibile con una soluzione che stravolga di poco il funzionamento del sistema, è rappresentata dai lost coins. I lost coins sono quei token che rimangono sospesi e dispersi nella rete. Come sappiamo i coins sono contenuti all'interno del wallet, un portafogli digitale identificato con chiave pubblica e protetto con chiave privata. La perdita della chiave privata prova l'inutilizzabilità del wallet e di tutti i coins in esso contenuti. In questo modo il numero

finito e limitato di unità emesse di una criptovaluta, si riduce in realtà nel corso del tempo a causa di una percentuale crescente di quelle unità divenuta inutilizzabile.
Questa scarsità di unità di moneta che cresce nel corso del tempo conduce alla deflazione, un fenomeno dannoso nei termini in cui comporta un aumento eccessivo del valore della moneta che spinge investitori e speculatori a farne un uso ben diverso da quello per cui è stato creato, ovvero lo rende molto più idoneo alla speculazione che al pagamento di beni e servizi.
Un'ultima questione critica da analizzare è rappresentata dal fatto che i sistemi di criptovalute, se sviluppati e implementati, potrebbero apparire inefficienti dal punto di vista energetico. Il sistema richiede infatti che chi vi partecipa impieghi del tempo a verificare la validità delle transazioni, il quale ovviamente all'espandersi della rete aumenterebbe di conseguenza. In termini più specifici il tempo dedicato all'attività di mining è calcolato con un indice definito Hash Rate, misurato come:

$$Hash\ Rate = \frac{\text{Hash}}{Secondi}$$

Questo indice misura la quantità di calcoli computazionali svolti al secondo all'interno della rete ed è risultato un valore in crescita costante nel corso del tempo, e crescerebbe ulteriormente se la rete assumesse le dimensioni necessarie a rendere le criptovalute un fenomeno di massa.
Attualmente dunque la moneta digitale si presenta come uno strumento innovativo e pieno di possibilità di sviluppo. Tuttavia lo sviluppo non è solo un'opportunità ma anche una necessità affinché il vero potenziale dello strumento emerga, e deve avvenire rispettando certi canoni perentori non solo risolvendo i limiti tecnologici e logistici attuali, ma anche facendo attenzione a non calpestarne i principi fondanti che ne stanno garantendo il successo. Nonostante ciò sembra chiaro come, nonostante tutte le cure e le attenzioni del caso mirate a non mutare i principi fondanti, prima o poi sarà necessario accettare qualche compromesso come un potere più accentrato o l'individuazione di ruoli definiti che si occupino della sicurezza e stabilità della moneta, due traguardi che devono essere raggiunti affinché le criptovalute diventino un prodotto utilizzato su larga scala.

## 2.4 ESEMPI E CASI DI CRIPTOVALUTE

Nel corso degli anni il numero di monete digitali sul mercato è notevolmente aumentato, differenziandosi differenziandosi anche dall'emittente e dallo scopo originali e assumendo caratteristiche specifiche.

*Bitcoin*

Il Bitcoin è senz'altro l'esempio più noto e conosciuto di moneta virtuale, tanto che in molti contesti si assiste ad un fenomeno di volgarizzazione del marchio in cui il nome specifico viene usato per riferirsi al concetto generico di criptovaluta. Questa fama come abbiamo visto è legata al fatto che il Bitcoin rappresenta la prima forma di criptovaluta collocata con successo sul mercato e che ha prestato lo spunto, le tecnologie necessarie alla moltitudine di strumenti simili introdotti sui mercati negli anni successivi. Nonostante alcune difficoltà specifiche di questo sistema, le caratteristiche del Bitcoin sono in tutto assimilabili a ciò che abbiamo visto sino ad ora in quanto vista la dimensione e la notorietà del fenomeno, le modalità d'uso e il funzionamento sono spesso presi come termine generale. Sono invece gli esempi successivi a rappresentare in certi aspetti una distinzione dal mercato Bitcoin.

*Bitcoin cash*

Bitcoin Cash è una forma di moneta virtuale scaturita da un vero e proprio conflitto di secessione tra gli utilizzatori di Bitcoin. Uno dei problemi principali di Bitcoin che ne limita largamente la diffusione su ampia scala, è infatti rappresentato dalla lentezza di esecuzione delle transazioni (circa 7 scambi al secondo contro i 24000 eseguiti da visa quotidianamente). La causa del problema è individuabile dalla dimensione dei blocchi nella blockchain di cui fa uso bitcoin, pari a circa 1MB inizialmente e a 2MB oggi. Un aumento di dimensioni dei blocchi comporta una minore sicurezza e un'impossibilità per i soggetti più "lenti" di "circolare" agevolmente sulla rete (in termini più tecnici i nodi più piccoli non sarebbero in grado di elaborare le informazioni e verrebbe eliminata la decentralizzazione). Di fronte a questo problema un gruppo di utilizzatori di Bitcoin nel 2017 ha deciso di separarsi dalla moneta principale creando Bitcoin Cash, un sistema molto simile a Bitcoin ma che si serve di blocchi di 8MB consentendo un forte incremento delle prestazioni e una maggior rapidità delle transazioni.

*Ethereum*

Nel 2015 un nuovo sistema funzionante attraverso criptovalute viene introdotto da Vitalik Buterin, prima di attirare l'attenzione di Microsoft e di un vastissimo numero di altri investitori: Ethereum. Questo sistema si basa sulla stipulazione e sul funzionamento di smart contract, veri e propri accordi e contratti di vario genere stipulati senza alcun intervento di avvocati, notai o organi di intermediazione e la cui sicurezza è garantita dalla protezione offerta dalla crittografia. Questo sistema funzionante su una blockchain parallela e distinta da quella di Bitcoin, funziona anche con una valuta diversa, che traendo il nome dal sistema stesso su cui opera è chiamata Ether ed è la seconda moneta digitale in termini di dimensione del mercato dopo Bitcoin. Possiamo tuttavia concludere che lo scopo di Ether sia ben diverso da quello di Bitcoin. Se infatti quest'ultima vuole affermarsi come valida sostituta del denaro, Ether si occupa semplicemente di mantenere attivo ed efficiente il mercato degli smart contract, unico contesto in cui è attualmente utilizzabile, garantendone un funzionamento rapido e completo.

*Ripple*

Ripple è sia il nome una compagnia open source, che quello del network blockchain a cui questa compagnia ha dato vita, e rappresenta dunque un'ulteriore rete di circolazione per criptovalute. La moneta digitale usata in questo sistema è chiamata XRP. Lo scopo di Ripple è ancora una volta diverso da quello di Bitcoin. Mentre quest'ultimo aspira a creare uno strumento di riserva del valore lo scopo di Ripple è quello di ridurre i costi di transazione e di "Enabling the world to move value like it moves information today[13]", semplificando i sistemi utilizzati da Bitcoin per ridurre tempi, costi e rischi. Per realizzare questo scopo Ripple ha modificato una delle colonne portanti del sistema Bitcoin, ovvero il processo di mining introducendo un meccanismo di consenso attraverso una rete di server (Ripple Consensus) che si occupano di verificare la validità delle transazioni molto più velocemente di quanto impieghino a farlo i miners in persona di Bitcoin, consentendo in tal modo alle transazioni di essere eseguite in pochissimi secondi. Tutte le transazioni sono inoltre catalogate in un registro pubblico che non esiste sul sistema Bitcoin (Ripple Consensus Ledger). Grazie a questo sistema Ripple si presenta come un sistema molto

[13] Mission di Ripple estratto dal sito web ufficiale della compagnia www.Ripple.com

più efficiente senza perdere la decentralizzazione che contraddistingue le blockchain. Per quanto concerne la funzionalità della valuta XRP, essa rappresenta l'unica moneta autorizzata a circolare sul sistema Ripple, ma la sua funzione è quella di trasportare un valore facilmente convertibile nelle valute tradizionali, che attraverso questo sistema possono essere quindi trasferite rapidamente e a basso costo.

*Libra di Facebook*[14]

Come sappiamo Facebook, creando il social network di maggior successo nella storia di internet, ha dato un enorme contributo allo sviluppo di quello che abbiamo in precedenza definito "internet of people". Dal 2019 dall'headquarter della società un nuovo progetto ha iniziato a prendere piede: la creazione di una criptovaluta di nome Libra, il cui obiettivo principale è un "empowerment finanziario del popolo". Infatti, come afferma il white paper dell'organizzazione, attualmente i servizi finanziari e i costi di gestione del denaro sono più alti per coloro che meno possono permetterselo. Introducendo un sistema come quello pensato da Libra, disintermediato e basato su rapporti fiduciari, i costi potrebbero essere ridotti quasi a zero apportando enormi vantaggi alle persone. Ciò che rende particolarmente innovativo il progetto Libra è l'obiettivo di coprire la valuta con una riserva, attribuendole quel valore intrinseco che manca a tutte le altre monete digitali ma che è fondamentale per offrire sicurezza e garanzie, soprattutto a chi non lavora nel settore finanziario e trarrebbe più benefici da questa nuova rete. Inoltre il sistema Libra mira a collaborare con i colossi finanziari e dei pagamenti come Visa o Paypal, con società di telecomunicazione, di blockchain e venture capital. La vera innovazione di libra è quindi nel mindset su cui nasce. Non vuole essere uno strumento di opposizione ai poteri finanziari tradizionali, ma l'anello mancante tra le grandi istituzioni del passato e i sistemi blockchain del futuro. Già dalla prima pubblicazione del white paper Libra è stata fortemente criticata, soprattutto in Europa dove i ministri delle finanze dei principali paesi non hanno tardato a esprimere i loro dubbi in termini di sicurezza e di impatto disastroso sulla stabilità dell'Euro e del Dollaro e sul corretto funzionamento delle banche centrali qualora il fenomeno non fosse correttamente e approfonditamente regolato. L'introduzione di Libra, inizialmente prevista per il 2020, potrebbe dunque essere

[14] Libra non è ancora una valuta in circolazione. Tuttavia a causa del suo scopo rivoluzionario si è scelto di inserirla nell'elenco in questione come caso degno di nota in quanto anche qualora il progetto non vedesse mai la luce comunica ed insegna la forza innovativa della tecnologia blockchain.

rimandata di qualche tempo a causa dei contrasti con le istituzioni, ma senz'altro la sua realizzazione sembra rappresentare un punto di svolta senza precedenti.

*Petromoneda*

Non si può non concludere questo elenco di esempi meritevoli di nota senza citare una delle prime monete digitali di stato. Il Petro, che tratteremo in modo più approfondito successivamente, è infatti una moneta digitale emessa dal Venezuela nel 2018. La moneta è garantita attraverso il petrolio e pertanto ogni token è stato venduto al prezzo di un barile. La ICO della moneta e la sua circolazione non hanno avuto luogo su una nuova piattaforma apposita in quanto hanno usufruito del sistema Ethereum.

# CAPITOLO 3
# APPROCCI NORMATIVI E ATTEGGIAMENTO DI STATI E BANCHE CENTRALI VERSO LE CRIPTOVALUTE

Come appare dall'analisi delle caratteristiche condotta precedentemente, la struttura delle blockchain e il principio della decentralizzazione su cui si cui si basa il sistema delle criptovalute rende molto difficile, se non apparentemente impossibile, una forma di regolazione che disciplini in modo corretto questo strumento senza corromperne i fondamenti e suscitare il malcontento dei sui utilizzatori. Tuttavia, le difficoltà che frenano l'espansione del fenomeno bitcoin e affini è riscontrabile spesso proprio nell'assenza di una normativa che faccia sentire tutelato il grande pubblico e lo spinga a scegliere questo mezzo per conservare e trasmettere valore. Per questa ragione molti governi in tutto il mondo hanno dato il via ad un'opera di regolamentazione di questi sistemi, sia perché comprendono il potenziale innovativo che essi possiedono, sia perché temono che una crescita improvvisa ed incontrollata possa generare una bolla capace di arrecare danni enormi alle finanze pubbliche e private. Inoltre le criptovalute, nate come alternativa al potere delle banche centrali, rischiano di sottrarre dal controllo delle stesse la circolazione del valore e della ricchezza. In un contesto non regolato ciò potrebbe rivelarsi molto pericoloso. Nonostante l'impegno profuso una regolamentazione completa, precisa e universale rappresenta ancora un miraggio. Se infatti alcuni paesi, soprattutto nel continente asiatico, si stanno muovendo a grandi passi in questa direzione, altri, come vedremo nel contesto europeo, hanno ancora molto lavoro da svolgere.

## 3.1 GLI APPROCCI NORMATIVI NAZIONALI

### *3.1.1 Asia*

I paesi dell'Asia sono contraddistinti da culture, forme di governo, orientamenti politici, rapporti con l'occidente e modalità di approccio al progresso marcatamente diverse. queste differenze hanno portato i vari contesti nazionali a rapportarsi in modo molto vario al fenomeno delle valute digitali. Le differenze principali sono riscontrabili in Cina e Giappone che rappresentano i due estremi che cedono il passo a vari casi intermedi.

La Cina rappresenta il paese più ostile alle criptovalute nel continente asiatico e sin dalla loro comparsa non ha ambito a regolarne il mercato ma ha concentrato ogni possibile sforzo a combatterle. La Banca Popolare Cinese[15], ovvero la Banca Centrale in Cina, ha istituito il 25 marzo del 2016 il NIFA, ovvero il National Internet Finance Association of China, che è l'ente che regola il mercato delle valute digitali e che si occupa soprattutto di proibire lo scambio di questo genere di strumento. Nel settembre del 2017 la PBC ha vietato ogni genere di acquisizione di fondi tramite ICO, sia cinesi che estere, in tutta la Cina. Inoltre le piattaforme che avevano acquisito fondi da investitori cinesi hanno dovuto restituire le somme raccolte agli acquirenti della loro criptovaluta. Le piattaforme online sono state oscurate e le app rimosse dai digital stores. La NIFA ha inoltre messo in atto un sistema di controllo e verifica volto ad evitare pratiche illegali di questo tipo e ha istituito un programma per consentire di denunciare le stesse ad autorità o polizia. Infine la PBC ha proibito a banche e organizzazioni finanziarie di investire in criptovalute. Per quanto ciò possa apparire un controsenso, contemporaneamente a queste azioni la Cina ha iniziato i lavori per istituire la propria criptovaluta nazionale, controllata dalla PBC, che darà più garanzie in termini di trasparenza al governo cinese che ne deterrà il controllo e sarà garantita attraverso una somma corrispondente in valuta reale. I lavori per la creazione e regolazione della stessa sono stati affidati al Digital Currency Research Lab e la moneta prenderà il nome di Yuan digitale. Ad oggi essa è uno strumento sempre più concreto, che il governo e la PBC vorrebbero rendere pienamente operativo entro le olimpiadi di Pechino del 2022. Per questa ragione si presume che la moneta debutterà sul mercato entro la fine del 2021. Il Contesto giapponese è molto diverso da quello cinese. Il Giappone infatti presenta il più attivo mercato di criptovalute a livello mondiale e il fenomeno è ampiamente regolato, non con l'obiettivo di impedirne lo sviluppo ma di consentirne un utilizzo su larga scala e garantendo non solo trasparenza per lo stato ma anche sicurezza per gli investitori. In questo contesto la responsabilità della stabilità dei mercati finanziari (in termini generali e non solo per le valute digitali) ricade sulla Financial Services Agency[16] che, dal momento del loro debutto, si occupa anche della gestione e regolazione di ICO e criptovalute. Quest'organo per la regolazione delle ICO ha rimandato a due emendamenti distinti in base alla natura delle ICO e alle caratteristiche

[15] Da adesso in sigla PBC
[16] Da adesso in sigla FSA

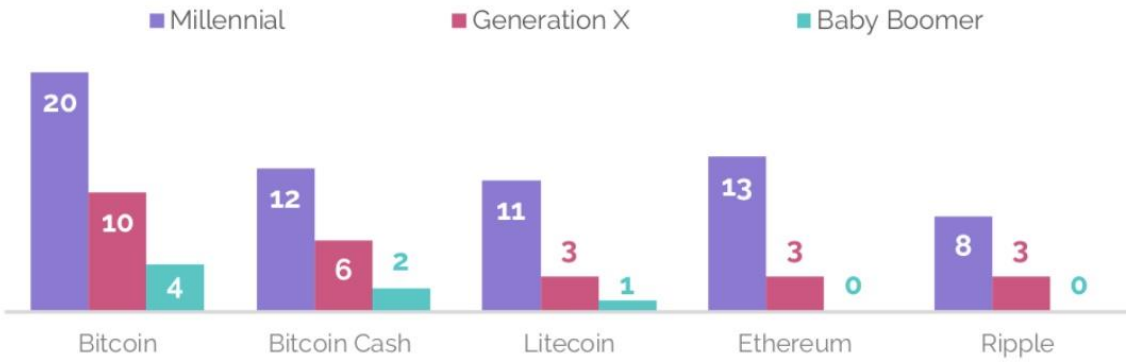
del token che promuovono. Le due normative in questione sono il Japanese Payment Services Act (anche Virtual Currency Law) e il Financial Instruments and Exchange Act. Saranno regolate secondo il primo di questi due le ICO che promuovono token identificabili come valuta utilizzabile per l'acquisto di beni e servizi. L'emendamento stabilisce che ogni ICO rientrante in questa categoria è soggetta a registrazione presso l'FSA. Lo stesso Payment Services Act disciplina e regola anche i processi di acquisto e vendita, nonché i servizi di intermediazione tra queste due azioni. Per i soggetti che ricoprono questi tre ruoli (venditori, acquirenti, intermediari) è richiesta la registrazione presso l'FSA.

Le ICO saranno invece regolate secondo il secondo emendamento nel caso in cui i token posti sul mercato sono acquistabili con moneta reale o altre criptovalute e stabilisce che i ricavi da essi ottenuti sono considerate alla stregua di dividendi azionari. In questo caso la registrazione presso l'FSA è obbligatoria sia per il promotore dell'ICO che per l'organizzazione che sta emettendo token per raccogliere fondi da investire.

In campo tributario la tassazione giapponese prevede che vengano tassati i ricavi percepiti tramite criptovalute solo quando superiori a 200.000 Yen reali.

### *3.1.2 Stati Uniti*

Negli Stati Uniti i pareri inerenti alle valute digitali sono piuttosto discordanti, fatto che è possibile riscontrare nella legislazione del fenomeno, che consente lo sviluppo del mercato lasciando trasparire i dovuti timori sui rischi e sui danni che la diffusione dello strumento potrebbe apportare alla finanza americana. Il presidente in carica Donald Trump ha più volte dichiarato la sua avversità nei confronti delle valute digitali affermando che esse non possono essere considerate propriamente denaro e che rappresentano una minaccia da cui il governo deve difendersi e dichiarandosi intenzionato ad inasprire la legislazione e la sorveglianza su questo tipo di mercato. Contrariamente al punto di vista della Casa Bianca tuttavia moltissimi americani reputano le criptovalute un'opportunità di investimento e circa l'81% della popolazione dimostra una certa familiarità con questo strumento. Nonostante la stringente legislazione volta per lo più ad evitare frodi e il parere presidenziale contrario, gli Stati Uniti mostrano interesse verso il fenomeno delle valute digitali e offrono sussidi e strumenti di ricerca per l'implementazione di nuove soluzioni e nuovi strumenti.




*Fonte: dati del 6/9/19 da yougov.com*

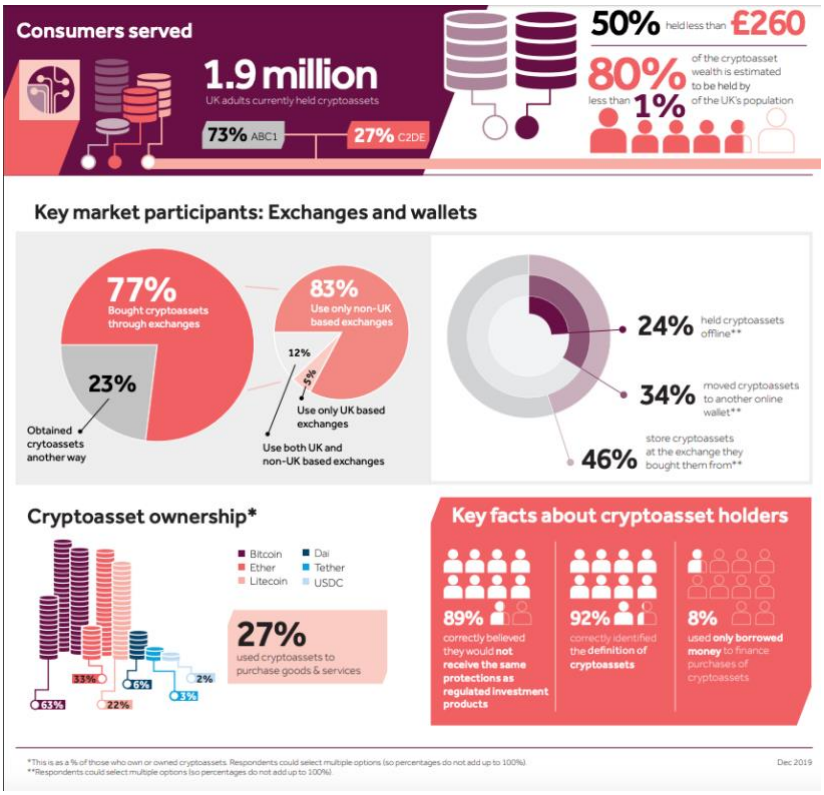
Negli Stati Uniti gli organi che supervisionano la conformità delle attività finanziarie alle leggi federali sono la Security Exchange Commission[17] e il Financial Crimes Enforcement Network[18]. In particolare il FinCEN verifica la concordanza con il Bank Secrecy Act che incentra la propria disciplina sull'individuare e combattere le frodi fiscali. Nel tentativo di disciplinare le ICO la SEC propende verso un'integrazione delle stesse nella legislazione federale sui titoli finanziari, che concentra la propria attenzione sugli interessi degli investitori che devono essere messi nelle condizioni di prendere decisioni riguardo la vendita e l'acquisto di token sulla base di informazioni trasparenti e garantite. La SEC, inizialmente impreparata alla gestione del fenomeno, nel corso del tempo ha ampiamente rafforzato la legislazione inerente alle ICO per punire le attività illecite attuate attraverso di esse, imponendo ai trasgressori pene molto elevate[19]. Riguardo la classificazione delle criptovalute, la SEC afferma che esse potrebbero essere confuse e considerate alla stregua di titoli. È onere dell'emittente evitare che ciò si verifichi o adattare l'intera emissione e le caratteristiche dei token a quelle richieste per i titoli dalla legge americana. La normativa imposta dal FinCEN in termini di frodi può colpire ogni tipo di soggetto coinvolto in un'ICO o in uno scambio successivo di criptovalute, come creatori, acquirenti, venditori e chiunque accetti o invii questo strumento.

[17] Da adesso in sigla SEC.
[18] Da adesso in sigla FinCEN

[19] Alla pagina https://www.sec.gov/ICO e affini sul sito ufficiale della SEC è possibile consultare la regolazione del fenomeno, il punto di vista del governo americano su rischi, frodi, pene imposte, opportunità e aggiornamento degli emendamenti del passato per la ricezione del fenomeno delle criptovalute.

*3.1.3 Regno Unito*

Il contesto britannico è uno dei più accondiscendenti in occidente verso le valute digitali. Lo strumento, rapidamente accettato e utilizzato dal pubblico e tuttora in forte crescita, è stato in breve tempo regolato con una normativa che continua ad espandersi ma mirata ad uno sviluppo controllato ma veloce di questo settore. L'espansione del settore è stata incentivata da veri e propri annunci pubblicitari, quasi del tutto assenti in altri paesi, che spingevano all'acquisto di criptovalute.




*Dati ufficiali diramati dall'FCA inerenti alla diffusione delle valute digitali nel Regno Unito relativi a dicembre 2019*

L'organo che si occupa della regolazione del fenomeno è il Financial Conduct Authority (FCA). Ogni operazione od operatore devono essere registrati presso l'FCA. Per quanto concerne la normativa a cui ci si riferisce per la regolazione delle criptovalute, a parte alcune dovute eccezioni rappresentate da quel tipo di moneta che per le sue caratteristiche merita di rientrare in una categoria specifica e regolata secondo una determinata disciplina, quasi tutte le valute informatiche subiscono la regolazione finanziaria applicata agli strumenti derivati come futures e opzioni. Nonostante ciò il governo ha dichiarato che l'emanazione di una disciplina appropriata e specifica è un elemento

rilevante dell'agenda dei prossimi lavori per il parlamento inglese. Particolarmente rilevante e di recente introduzione è la normativa fiscale britannica sulle criptovalute, dettagliata e precisa rispetto alle altre grandi economie mondiali. La rilevanza è data dal fatto che l'Her Majesty's revenue and customs (o HMRC, l'ente di riscossione delle imposte britannico), non riuscendo ad attribuire le criptovalute a nessuna categoria esistente le ha definite come un nuovo asset diramando una modalità di tassazione specifica piuttosto che lasciare il vuoto normativo o la vaghezza tipici di molti paesi.

*3.1.4 Unione Europea*

Nel contesto europeo il mantenimento della stabilità dei mercati finanziari e la tutela dei consumatori ricadono sullo European Securities and Markets Authority[20] e sulla Banca Centrale Europea[21].

Dopo una prima fase in cui l'UE rifiutava di considerare le criptovalute una moneta e per questa ragione non si sentiva in dovere di regolarne l'uso, la crescita del fenomeno ha reso necessaria l'introduzione di una normativa adeguata. In particolare la disciplina applicabile varia a seconda che le ICO riguardino l'emissione di strumenti finanziari o meno. Nel primo caso la disciplina applicata è quella del MiFID II, delle direttive sulla trasparenza e sugli abusi di mercato e della Short Selling Regulation. Più precisamente, la normativa applicabile alla singola ICO varia a seconda della conformazione della stessa che può renderla più soggetta ad una regolazione piuttosto che ad un'altra tra quelle citate. Per ciò che invece concerne le ICO non riguardanti strumenti finanziari, esse non sono soggette a questo normative e sono meno regolate, per questo comportano più rischi per gli investitori. Esse vengono talvolta categorizzate come "fondi di investimento alternativi" o come "electronic money". Quando rientrano nella prima categoria sono assoggettate all'Alternative Investment Fund Managers Directive (AIFMD), mentre quando sono considerate alla stregua di electronic money sono regolate dall'Electronic Money Directive (EMD2).

L'Unione Europea presenta una normativa sulle criptovalute piuttosto confusa che consiste per lo più in una serie di adattamenti e interpretazione di norme precedenti. Per evitare che la crescita del fenomeno comporti la nascita di vuoti normativi, casi confusi e

[20] Da adesso in sigla ESMA

[21] Da adesso in sigla BCE

opportunità di frode sarà presto necessaria, più che in altri paesi, l'introduzione di una normativa più precisa. Per raggiungere questo traguardo è necessario superare definitivamente la tendenza a rifiutare e sminuire questo strumento e accettarne il valore e il potenziale. Dopo anni l'UE sembra aver intrapreso la strada giusta in questo senso. Nel 2018 per lo sviluppo e la ricerca delle blockchain è stato introdotto dalla Commissione Europea in accordo con il Parlamento l'EU Blockchain Obesrvatory and Forum che consiste una condivisione di informazioni a livello comunitario per raggiungere nuove frontiere tecnologiche e creare mercati più sviluppati e sicuri nell'ambito della moneta digitale. Dalla diffusione della notizia del tentativo di Facebook di emettere la valuta Libra l'Unione Europea ha scelto di iniziare a lavorare per l'introduzione di una moneta virtuale comunitaria.

### 3.2 LE BANCHE CENTRALI

A questo punto è necessario abbandonare la suddivisione geografica e compiere un'analisi sugli effetti che le criptovalute e la tecnologia blockchain avranno o potranno avere sulle banche centrali a livello globale e su come il ruolo di queste ultime potrebbe mutare. Come ribadito più volte, la moneta digitale nasce come alternativa alle tradizionali valute emesse e gestite dalle banche centrali, ragione per cui inevitabilmente ne osteggia la stabilità, ma questo non è l'unico scenario possibile. Se le banche centrali si dimostrassero in grado di accettare e sfruttare a loro vantaggio questa nuova tecnologia e strumento potrebbero trarne enormi benefici e avere accesso a nuove opportunità. La prima cosa a cui va incontro una banca centrale quando deve "competere" con una valuta digitale è una possibile perdita di efficacia delle attività di politica monetaria. Se il pubblico è insoddisfatto della politica messa in atto da una banca ha la possibilità di cambiare il proprio denaro con una criptovaluta, così da risultare immune ad ogni variazione di prezzo della valuta tradizionale del suo paese e quindi riparandosi da un eventuale svalutazione. Ovviamente ciò può rappresentare un vantaggio per quei popoli che sono soggetti a comportamenti delle banche centrali sconsiderati e dannosi per la collettività poiché impedisce ad esse di compiere abusi nell'utilizzo della politica monetaria. Nel 2015 il governo argentino usò eccessivamente l'inflazione del Peso per causare un incremento dei tassi di interesse sui propri investimenti. La popolazione argentina stanca della continua svalutazione patrimoniale che era costretta a subire investì la liquidità in Bitcoin.

Tuttavia ciò comporta un grande rischio per tutti, poiché se il pubblico riuscisse ad eludere ed evitare le conseguenze delle attività messe in atto dagli organi di governo, la stabilità sino ad ora piuttosto garantita dagli stati inizierebbe a venire meno.

Sebbene le criptovalute rappresentino un'alternativa alle istituzioni con cui tendono a porsi in competizione, è sempre più diffuso il caso di banche centrali che scelgano di emettere la loro propria valuta digitale. Nel febbraio del 2018, per esempio, venne introdotta in Venezuela dal presidente Maduro la petromoneda (o semplicemente petro) come criptovaluta garantita dal prezzo di un barile di petrolio e che è stata istituita tra numerose critiche con la finalità di raccogliere fondi per ripagare parte del debito venezuelano con gli Stati Uniti nel periodo di iperinflazione del Venezuela. A parte questo caso eccezionale, sono molte le banche centrali che stanno lavorando per emettere una versione digitale della propria moneta, e varie sono le ragioni che le spingono. La maggior parte delle banche centrali mirano a emettere una valuta digitale semplicemente per non perdere il loro ruolo centrale nella gestione monetaria di un paese. Nei paesi scandinavi è in crescita continua il fenomeno della digitalizzazione del denaro. In sostanza sono sempre di più i contesti e le attività che si rifiutano di accettare contanti ma ricevono pagamenti solo attraverso mezzi digitali. Per una banca centrale è necessario inserirsi nel mercato delle monete informatiche per non perdere la propria rilevanza.

Un'altra valida ragione, propria in questo caso di paesi emergenti come l'Ecuador o l'India, per emettere una criptovaluta è la possibilità di raccogliere vastissimi capitali da milioni di persone da ogni parte del mondo per poter investire sulla crescita e lo sviluppo del paese. Infine, come abbiamo già notato dall'analisi del contesto cinese, alcuni paesi potrebbero emettere monete digitali per sfruttare l'alta tracciabilità delle transazioni garantita dal sistema blockchain per esercitare un maggior controllo.

Ad ogni modo, questo può essere un mezzo a disposizione degli stati per usufruire dei vantaggi dello strumento piuttosto che correre ai ripari cercando di evitare le conseguenze dannose della sua esistenza. Le criptovalute di stato non sono del tutto assimilabili a quelle tradizionali. La differenza principale è legata chiaramente al fatto che, a differenza delle tradizionali criptovalute decentralizzate, in questo caso abbiamo a che fare con un centro di potere ben individuabile rappresentato dalla banca centrale emittente. Inoltre le monete digitali statali hanno un valore garantito e stabile come le valute tradizionali e non volatile come le altre criptovalute. L'introduzione di criptovalute di stato e di un sistema blockchain renderebbe realizzabili e molto più semplici iniziative ad oggi

impossibili. le banche centrali potrebbero accettare depositi direttamente dal pubblico, eliminando la consuetudine attuale obbligatoria che porta il privato a passare attraverso una banca commerciale. Ciò è realizzabile in quanto, se oggi appare impossibile gestire un così ampio scambio di valuta tra operazioni di deposito, cambio e prelievo, attraverso un sistema tecnologico blockchain è possibile utilizzare algoritmi di controllo e conteggio rapidi, autonomi ed efficienti. un rapporto diretto tra investitori e banca centrale rappresenterebbe un enorme vantaggio per quest'ultima che non sarebbe più tenuta a mettere in pratica azioni di recupero e salvataggio, che ad oggi vengono messe in atto per lo più a tutela degli investitori, e sarebbe libera da ogni responsabilità e dovere di controllo e gestione delle banche commerciali. A seguito di questo processo rivoluzionario si eliminerebbe la necessità dell'intermediazione e con essa i costi connessi. Verrebbero inoltre eliminati problemi attuali come i tempi di attesa per l'esecuzione di un bonifico o la gestione di un conto dall'estero e le banche commerciali, divenute obsolete, perderebbero a tal punto la loro funzione che finirebbero per scomparire.

Inoltre un sistema di conteggio algoritmico informatico permetterebbe di valutare elettronicamente il tasso di cambio più corretto e gestire automaticamente la quantità di moneta in circolo per far si che questo tasso sia raggiunto. I principali danni di questo possibile scenario rischiano di ricadere sulla collettività. Se la blockchain nasce come mezzo di indipendenza dalle banche centrali, il quadro dipinto nelle righe precedenti conduce ad un esito del tutto opposto. La realizzazione di un simile sistema porterebbe ad uno strapotere delle banche centrali che avrebbero un elevatissimo controllo sulle finanze personali dei privati. È chiaro come la situazione attuale rappresenti un bivio che conduce da una parte a uno sminuimento del ruolo della banca centrale così come oggi la conosciamo e dall'altra uno strapotere della stessa. Entrambe le situazioni sembrano danneggiare infine la collettività. La sfida del futuro deve essere quella di trovare una condizione intermedia, bilanciata e stabile per sfruttare al meglio i vantaggi di questa innovazione senza creare situazioni insostenibili.

# CAPITOLO 4
# VALUTAZIONE DI INVESTIMENTI IN CRIPTOVALUTE

Come analizzato, le criptovalute attualmente esistenti sono rappresentate da un numero molto elevato e in continua crescita. Tuttavia questo numero non è composto interamente da valute stabili, solide e abbastanza sicure come gli esempi citati in precedenza[22], ma anche da molteplici valute di scarsa stabilità e durata. In conseguenza di ciò per valutare un potenziale investimento che coinvolga valute digitali è necessario condurre uno studio sullo strumento specifico su cui si desidera investire, sull'efficienza del sistema su cui si fonda e sulla sua potenziale sopravvivenza nel mercato. L'efficienza di una blockchain e la sua capacità di operare senza problemi è definita status, un valore rappresentato dalla serie di transazioni valide eseguite consecutivamente. Tutte le blockchain mirano ad accrescere il loro status per diffondersi e coinvolgere un numero di utenti crescente. Le vie di accrescimento e consolidamento dello status sono di due tipologie:

- Proof of Work: metodo ideato precedentemente alla nascita dei sistemi blockchain nel 2002 da Back. Il metodo richiede che i soggetti risolvano complessi problemi matematici per poter compiere le operazioni e, nel caso in questione, aggiungere blocchi di informazioni alla blockchain. il concetto è strettamente legato all'uso della crittografia e serve ad evitare frodi. La sostanza è che il "lavoro" svolto per poter compiere l'operazione è "prova" della limpidità della stessa.
- Proof of Stake: teorizzato da King e Nadal nel 2012 richiede uno sforzo decisamente inferiore rispetto al caso precedente. Se infatti nel Proof of Work la "prova" che non si stesse abusando del sistema era rappresentata dalla mole di lavoro compiuta per svolgere l'operazione, in questo caso la "prova" è fiduciaria, in quanto si attribuisce automaticamente agli utenti al crescere della quantità di valuta detenuta. Secondo questo concetto, un abuso che potrebbe causare un malfunzionamento del sistema andrebbe a danneggiare coloro che detengono una quantità di valuta maggiore, i quali sarebbero dunque disincentivati a condurre opere di questo tipo.

[22] Vedi capitolo 2 paragrafo 2.4

## 4.1 SURVIVAL ANALYSIS

La valutazione delle valute non può tuttavia basarsi esclusivamente sul funzionamento del sistema blockchain. È necessario condurre una Survival Analysis, che consiste in uno studio dei dati inerenti a prezzo, utilizzo e previsioni sul futuro per stimare statisticamente le probabilità di sopravvivenza sul mercato di una criptovaluta, decidendo se l'investimento abbia possibilità di successo o sia maggiormente destinato a fallire. Per spiegare il metodo di funzionamento dell'analisi definiamo in termini generali:

- C: tutte le criptovalute sul mercato in un certo momento
- S: tutte le criptovalute presenti sul mercato (Sopravvissute) in un certo momento
- E: tutte le criptovalute scomparse dal mercato (Estinte) in un certo momento

Da qui in termini insiemistici deduciamo che:

$$C = S \cup E \quad \text{e che} \quad S \cap E = 0$$

Più nello specifico possiamo scrivere che:

$$C = \cup C_i$$

Indicando con ciò che C è formato dalla somma di tutte le $C_i$ dove i corrisponde al un numero di giorni in cui una certa criptovaluta è stata scambiata.

Questo significa che ad esempio $C_{12}$ fa riferimento all'insieme di tutte le valute scambiate per 12 giorni mentre i corrispondenti $S_{12}$ ed $E_{12}$ si riferiscono alle valute scambiate per esattamente 12 giorni e a quelle non più presenti sul mercato ma scambiate in passato per esattamente 12 giorni.

Per esprimere dunque la probabilità che una criptovaluta uscirà dal mercato esattamente 12 giorni dopo $p(x \in E_{12})$ è necessario calcolare il rapporto tra numero storico di criptovalute estinte dopo 12 giorni e numero storico di criptovalute scambiate per almeno 12 giorni. Ciò risulterà dalla formula:

$$p(x \in E | x \notin \cup C) = \frac{|E|}{\Sigma|C|}$$

Conseguentemente la probabilità opposta che una valuta sia scambiata per più di 12 giorni può essere calcola semplicemente come:

$$1-(x \in E)$$

Questa formula, prettamente teorica, ha un uso molto limitato nella realtà e da risultati poco precisi. Nonostante ciò essa rappresenta una parte molto rilevante di una formula con un uso molto più vasto:

$$p(x \in \cup E | x \notin \cup C) = 1-\Pi\,(1-p\,(x \in E | x \notin \cup C))$$

Questa formula mostra la probabilità che una certa valuta venga dismessa dal mercato non in uno specifico giorno ma in un periodo che va da un momento preciso ad un altro e permette di dare soluzioni meno accurate ma più realistiche.

| Vita | 1 anno | 2 anni | 3 anni | 4 anni | 5 anni |
|---|---|---|---|---|---|
| 0 anni | 35,1% | 52,7% | 61,6% | 66,4% | 70,9% |
| 1 anno | 27,1% | 40,9% | 48,2% | 55,2% | |
| 2 anni | 18,9% | 28,9% | 38,6% | | |
| 3 anni | 12,4% | 24,3% | | | |
| 4 anni | 13,6% | | | | |

Fonte: Lansky (2020)

Dal grafico che mostra la probabilità che una valuta venga dismessa rapportata agli anni di vita si riscontra come storicamente la probabilità maggiore di fine di una criptovaluta sia 5 anni e come più una valuta si avvicina a questa fase della sua esistenza più la probabilità cresce. Si evidenzia inoltre che più è "vecchia" una criptovaluta (valore espresso in colonna) minore è la probabilità che esca dal mercato in futuro (valore orizzontale). Infatti ogni valore delle righe più in basso (rappresentanti le valute nate prima) è inferiore a quelli corrispondenti ma nelle righe superiori (relativi alle valute più giovani). Il calcolo si ferma a 5 anni in quanto i dati che è possibile raccogliere attualmente non consentono di fare stime precise su periodi più lunghi.

## 4.2 CRIPTOVALUTE, EQUITY E FOREX, RELAZIONI E CAPM

Superata la valutazione sulle probabilità di sopravvivenza o meno di una valuta, è necessario valutare i suoi rendimenti, così da comprendere se l'investimento risulti vantaggioso o utile sia rispetto ad altre valute digitali che agli strumenti finanziari più classici. Compiere questo tipo di operazione può risultate meno semplice del previsto per diverse ragioni. Per prima cosa la classificazione delle criptovalute è ancora piuttosto incerta e molta è l'indecisione sul classificare le stesse come valute o come titoli, decisione fondamentale per valutare effettivamente i risultati conseguiti e poterli rapportare agli strumenti tradizionali. Inoltre alcuni metodi ampiamente utilizzati per la valutazione di strumenti tradizionali non sembrano utilizzabili e validi con le valute

digitali. Infine la breve storia di questi strumenti e la conseguente carenza di dati storici rende difficili previsioni, stime e valutazioni. Per il complesso di queste ragioni cresce costantemente l'insieme di coloro che ritengano che la criptovaluta non sia assimilabile a un titolo oppure a una valuta tradizionale, ma che debba essere considerata come un tipo di strumento a sé stante, con le proprie caratteristiche e di cui è più utile valutare risultati e benefici in relazione ai mezzi di investimento classici e non in contrapposizione ad essi.
Per approfondire e indagare su un legame di dipendenza o relazione tra criptovalute ed equity è possibile condurre uno studio basato sul Capital Asset Pricing Model a 5 fattori di Fama e French. Questo modello applicato alle criptovalute dice che il ritorno (r) della valuta i al tempo t si calcola come:

$$r_{it}=\alpha_i + \beta_i(R_{mt}-R_{ft}) + s_iSMB_t + h_iHML_t + r_iRMW_t + c_iCMA_t + \varepsilon_{it}$$

fonte: Glas T. investments in cryptocurrencies:Handle with care!(2019)

dove $\alpha$ rappresenta il ritorno anormale, $\beta$ la variazione del ritorno al variare del mercato, SMB il fattore dimensione, HML il fattore valore, RMW il fattore redditività, CMA il fattore investimenti ed $\varepsilon$ la regressione residuale. Applicando questo modello sia in termini di aggregato al complesso delle criptovalute, sia alle singole monete digitali, non otteniamo nessun dato o valore ricorrente o degno di nota e nessun tipo di parallelismo con il mercato dell'equity, ciò comporterebbe che tra i due strumenti non ci sia nessun tipo di correlazione a cui affidarsi con sicurezza.
Per quanto concerne invece il possibile legame con il mercato forex, dobbiamo prendere in esame la forza da cui questo è mosso, ovvero il campo macroeconomico e i fattori che in esso agiscono. Prendiamo un'ulteriore regressione che illustra che il rendimento (r) della criptovaluta i al tempo t è dato da:

$$r_{it}=\alpha_i+c_iCrescitaConsumo_t + g_iGDP_t + \beta_iMercato_t + t_iTERM_t + d_iDEF_t + \varepsilon_{it}$$

fonte: Glas T. investments in cryptocurrencies:Handle with care!(2019)

dove TERM e DEF rappresentano la crescita tra 10anni rispettivamente tra government bond e t-bills e tra corporate bond e government bond. Anche in questo caso le correlazioni effettive riscontrate applicando il modello di regressione sia al complesso delle criptovalute che singolarmente sono scarse, con qualche debole legame riscontrato

tra la crescita delle valute digitali e la crescita del GDP. Nonostante ciò si può rilevare che le criptovalute non dipendono e non hanno correlazioni evidenti sia con il mercato dei titoli che con quello delle valute tradizionali.

Vista l'inadeguatezza dei modelli propri di equity e forex è possibile applicare un terzo modello di CAPM più consono alle criptovalute e che trae la sua origine dal modello di Fama e French fondato su 3 fattori: inversione di breve termine, illiquidità e dimensione. L'applicazione proprio delle criptovalute presenta anche un quarto fattore mercato per cui i fattori che determinano l'esito del modello sono:

- Crypto market (CMKT)
- Crypto size (CSMB)
- Crypto illiquidity (CILQ)
- Crypto short term reversal (CSTR)

Che conducono alla regressione espressa in termini formulistici:

$$r_{it} = \alpha_i + \beta_i CMKT_t + s_i CSMB_t + h_i CILQ_t + v_i CSTR_t + \varepsilon_{it}.$$

fonte: Glas T. investments in cryptocurrencies:Handle with care!(2019)

## 4.3 COEFFICIENTE DI CORRELAZIONE

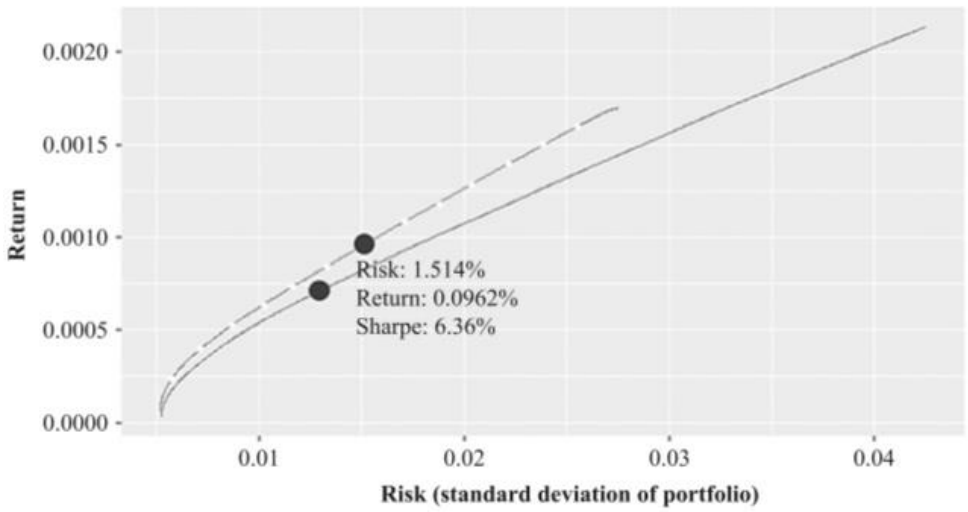
Inquadrate le criptovalute nel panorama finanziario odierno come uno strumento nuovo e a sé stante è necessario rispondere alla domanda principale: quali siano i vantaggi e i rischi di un investimento che coinvolga le criptovalute e in che termini e limiti investirvi possa portare benefici all'investitore.

Partendo dall'analisi svolta nel paragrafo precedente è possibile affermare con ragionevole certezza che le criptovalute non fanno parte degli strumenti di investimento tradizionali. Esse rientrano piuttosto in una terza ampia e varia area definita investimenti alternativi, che possiamo individuare come una categoria residuale in quanto ricomprende tutti quegli asset che non sono per qualsiasi ragione riconducibili agli strumenti classici, ed è questa l'unica caratteristica che li accomuna tutti. Rientrano nello stesso ambito anche materie prime, investimenti immobiliari, opere d'arte ed altre tipologie.

Gli investimenti alternativi sono caratterizzati da una ridotta correlazione storica con gli strumenti di investimento tradizionali, il che li rende ottimi mezzi per incrementare la diversificazione del proprio portafoglio. Nel caso specifico delle valute digitali, uno

studio sul loro coefficiente di correlazione in relazione ancora una volta a Equity e Forex Market ha sottolineato questo tratto caratteristico. L'analisi condotta da T. Glas (2019) mostra come le criptovalute tendano a muoversi spesso in modo opposto a quello degli strumenti classici al variare del mercato, offrendo quindi grandi opportunità di diversificazione. Nel dettaglio, l'analisi mostra come la correlazione tra monete digitali ed equity si attesti in media intorno allo 0,13, mentre tra valute tradizionali e informatiche la diversificazione possibile è ulteriormente accentuata e si riscontra persino una correlazione inversa.

Di conseguenza sembrerebbe chiaro come l'inserimento di criptovalute in un portafoglio tradizionale consenta di raggiungere un ritorno più elevato per ogni grado di rischio. Gli autori suppongono di detenere un portafoglio costruito in gran parte con S&P500 a cui sono state aggiunti investimenti in REITs, oro e private equity. Inoltre a questo portafogli viene aggiunto uno strumento avente come sottostante l'indice CRIX, computato presso l'università di Berlino e composto dalle 10 principali criptovalute scambiate sul mercato.




*Fonte: Cryptocurrency: a new investment opportunity? Di Kuo Chen, Guo e Wang*

Come possiamo vedere dal grafico, dove la linea continua rappresenta il portafoglio senza l'inserimento di un investimento in CRIX mentre la linea tratteggiata il portafoglio completo di una parte di CRIX, l'inserimento delle monete digitali nel portafoglio consente di ottenere una frontiera efficiente più elevata e un portafoglio ottimo più vantaggioso.

## 4.4 VOLATILITÀ ED EFFETTI DELLA BEHAVIOURAL FINANCE

Nonostante i vantaggi in termini di diversificazione e rendimento che abbiamo appena analizzato, le valute digitali presentano una serie di rischi che devono essere tenuti in considerazione legati alla sfera percettiva dell'investitore e causati dall'instabilità di questo tipo di asset. La prima questione da considerare è la credenza piuttosto diffusa che le valute digitali non siano altro che una bolla pronta ad esplodere da un momento all'altro. I ritmi di crescita incessanti e in parte inspiegabili del valore di queste monete è infatti ben più elevato di quello che in genere viene usato per individuare una bolla con sufficiente convinzione. Se queste fossero una bolla, al momento causerebbero una quantità di danni relativamente limitata ad un valore e ad un contesto circoscritti, ma è proprio il timore della crisi che limita la diffusone dello strumento.

Un secondo aspetto rilevante è rappresentato dal fatto che le valute digitali a differenza degli asset tradizionali non hanno un valore garantito e provato corrispondente ad un asset reale. Di conseguenza il valore che gli viene attribuito è legato esclusivamente al sentimento degli investitori, e per questa ragione è contraddistinto da altissima volatilità. Il sentimento degli investitori rappresenta sostanzialmente i movimenti nei prezzi causate dalle previsioni o da sentimenti degli investitori nei confronti di un determinato asset in un certo periodo. Nel caso delle criptovalute la situazione si complica a causa di un mercato in grande sviluppo e molto giovane, che rende ancora più complicato comprendere, quantificare e controllare i sentimenti degli investitori. Un primo tentativo in questa direzione utilizzato sull'interno mercato (infatti nasce nel 2007 prima delle stesse criptovalute) è stato teorizzato da Tetlock e consiste nell'individuare un legame quantitativo e quantificabile tra le notizie quotidiane sui titoli azionari pubblicate sul Wall Street Journal e le conseguenti variazioni nei prezzi. Tetlock notò la presenza di una relazione diretta fra crescende pessimismo dei media e calo dei prezzi dei titoli, seguito da un rendimento di valori più equilibrati.. Questo rialzo dei prezzi rispetto a un primo momento rende evidente l'effetto del sentimento degli investitori.

Un secondo metodo per misurare l'effetto dei sentimenti è il ritorno overnight, proposto e teorizzato da Berkman (2012). Il modello si basa sul principio per cui gli investitori tendono ad acquistare titoli fuori dall'orario di mercato cosi che questi vengano eseguiti effettivamente solo all'apertura il mattino seguente. Berkman notò inoltre come gli eventi positivi degni di nota conducessero a una maggior domanda dei titoli connessi all'evento stesso. Questi due fattori portano ad una concentrazione di domande d'acquisto

all'apertura del mercato che alza i prezzi più del livello di equilibrio, finché questi non si ribassano nel corso della stessa giornata. Questo metodo non è però del tutto applicabile al contesto delle criptovalute, commerciate 24 ore su 24 weekend incluso e dunque non soggette a fenomeni che coinvolgano prezzi di chiusura e/o di apertura. Non potendosi servire di queste differenze di prezzo per la misurazione, nel contesto delle monete digitali gli investitori si tendono a basarsi esclusivamente sui risultati storici, acquistando quelle con ritorno passato elevato e vendendo quelle con rendimento storico minore e portando i prezzi a deviare dal livello razionale. La misurazione del sentimento in questo caso è misurabile con la formula:

$$\text{Sentimento}_{j,t}=\frac{\sum_{n=0}^{N-1} R\mathit{endimento}_{j,t-n}}{N}$$

Fonte: Kuo Chen D., Guo L., Wang Y. Cryptocurrency: a new investment opportunity?(2017)

Dove $\text{Rendimento}_{j,t-n}$ è il rendimento della criptovaluta j n giorni prima del giorno t in cui vuole calcolarsi il sentiment effect, mentre N il periodo in cui si forma il sentimento dell'investitore. Conducendo uno studio sulle 10 valute ancora una volta parte dell'indice CRIX vediamo come il rendimento maggiore atteso per sentimenti positivi e quello minore atteso per sentimenti negativi sono rispettivamente positivo e negativo, entrambi significativamente diversi da 0. Tuttavia nella maggior parte dei casi il giorno successivo vediamo un'inversione che riduce i rendimenti troppo elevati ed aumenta quelli eccessivamente negativi, in quanto gli investitori razionali correggono l'errore causato dai sentimenti.

# CONCLUSIONI

Al termine di questo elaborato appare chiaro come la blockchain e le criptovalute risultino risorse uniche con immense opportunità di sviluppo. La prima offre maggior efficienza, sicurezza ed economicità nei processi di quasi ogni settore, le seconde potrebbero cambiare le modalità di approccio al denaro a cui siamo abituati e le basi dei sistemi finanziari globali, oltre che offrire nuove opportunità di investimento al pubblico e nuovi strumenti di finanziamento alle imprese. Appare altrettanto evidente come questo sviluppo sia piuttosto "rischioso" per la società, poiché le vie sbagliate sono molte, facili da intraprendere ed estremamente dannose. Tuttavia i rischi principali sono tutti accomunati dal fatto di poter essere in gran parte risolti da una regolamentazione accurata, dedicata e possibilmente universale. Se governi e banche centrali varassero una normativa accurata potrebbero infatti non solo disciplinare il quotidiano funzionamento dei mercati, ma anche intervenire su frodi e attività illecite che attualmente sono la causa della titubanza di pubblico e governi. Una normativa precisa a cura delle istituzioni è inoltre necessaria per definire il ruolo delle banche. L'emanazione di una normativa che favorisca lo sviluppo di questa innovazione appare però più complesso di quanto sembri. La prima difficoltà si riscontra nell'astio manifestato da alcuni paesi che come si è visto rifiutano di accettare i potenziali benefici delle criptovalute intimoriti dal rischio di perdere il controllo monetario o preoccupati delle conseguenze qualora il fenomeno dovesse rivelarsi una bolla. Un ulteriore fattore critico è l'inflessibilità degli investitori che navigano e scambiano criptovalute sul sistema da molto tempo e non sono disposti ad alcun genere di compromesso. Come si è visto infatti una regolamentazione può essere realizzata nel momento in cui gli utilizzatori delle monete virtuali, per consentire un utilizzo del programma su più larga scala, accettano di rinunciare a alcuni benefici di cui attualmente godono, come un certo grado di anonimato o l'assenza di autorità superiori. Fino ad oggi il rischio di perdere questi o altri privilegi ha spinto gli investitori a minacciare l'abbandono della criptovaluta.

Tornando dunque alla domanda posta inizialmente, le criptovalute rappresentano una risorsa per il nostro futuro? Senz'altro. I risultati degli studi finora condotti sulla gestione di portafoglio hanno evidenziato i vantaggi di rendimento conseguibili usufruendo nel modo corretto di questo strumento, mentre l'analisi delle conseguenze qualora la moneta riuscisse a prendere piede nella vita quotidiana di ognuno ha mostrato vantaggi in termini

di costi, efficienza e comodità. Per poterne usufruire al meglio è necessario il contributo di tutti: a) le istituzioni, che devono vedere nel digitale una risorsa e non una minaccia, accettarlo e aiutare gli investitori a conoscere e a fidarsi dello strumento, accettando di regolarlo dall'esterno senza la necessità di detenere un ruolo di dominio; b) gli investitori che devono accettare, ove necessario, compromessi con il fine di ampliare l'uso delle piattaforme e raggiungere l'obiettivo di un utilizzo di massa.

# BIBLIOGRAFIA E SITOGRAFIA

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. *Available at SSRN 2709713*.

Custers, B., & Overwater, L. (2019). Regulating Initial Coin Offerings and Cryptocurrencies: A Comparison of Different Approaches in Nine Jurisdictions Worldwide. *Custers, BHM, Overwater, LJ (2019) Regulating Initial Coin Offerings and Cryptocurrencies: A Comparison of Different Aprroaches in Nine Jurisdictions Worldwide, European Journal of Law and Technology*, *10*(3), 29.

Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of Business Venturing*, *34*(1), 1-22.

Glas, T. N. (2019). Investments in cryptocurrencies: Handle with care!. *The Journal of Alternative Investments*, *22*(1), 96-113.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, *35*(1), 220-265.

Guadamuz, A., & Marsden, C. (2015). Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, *20*(12-7).

Lansky, J. (2019). Cryptocurrency Survival Analysis. *The Journal of Alternative Investments*, *22*(3), 55-64.

Mas, I. (2016). Strains of Digital Money. *Capco Journal of Financial Transformation*, (44).

Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking beyond banks and money* (pp. 239-278). Springer, Cham.

Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing.

Raskin, M., & Yermack, D. (2018). Digital currencies, decentralized ledgers and the future of central banking. In *Research Handbook on Central Banking*. Edward Elgar Publishing.

Trautman, L. J., & Harrell, A. C. (2016). Bitcoin versus regulated payment systems: What gives. *Cardozo L. Rev.*, *38*, 1041.

Williams, V. (2020). Fintech Regulations in the United States Compared to Regulations in Europe and Asia.

Bellini M., *"Blockchain: cos'è, Come Funziona e gli Ambiti Applicativi in Italia"*, www.blockchain4innovation.it, 2020.

Crawford S., Piesse D., *"Blockchain Technology as a platform for digitalization"*, Ernst&Young Global Limited, 2016.

*"Enabling the world to move value like it moves information today"*, www.ripple.com, 2013.

*"Ethereum for Enterprise"* , www.Ethereum.org, 2020

*"European Commission Launches the EU Blockchain Observatory and Forum"*, ec.europa.eu, 2018.

Libra Association Member, *"Libra White Paper: An Introduction to Libra"*, 2019.

Mason B., *"La Prossima Evoluzione nel Mondo delle Criptovalute: i Paesi Emettono le loro Valute Digitali"*, www.fxempire.it , 2017.

Nakamoto S., *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, 2008.

Nicotra M., *"Le Norme su Bitcoin e Crittovalute nei Diversi Paesi: il Quadro"*, www.agendadigitale.eu , 2018.

Reiff N., *"Bitcoin vs. Ripple: What's the Difference?"*, www.invedtopedia.com , 2020.

Variankaval R., Junek E., Saperia A., Moy C., *"Blockchain and the Decentralization Revolution, A CFO's guide to the potential implications of distributed ledger technology"*, J.P.Morgan Chase, 2018.