POLITECNICO DI TORINO

Facoltà di Ingegneria Gestionale

Corso di Laurea in Ingegneria Gestionale – Percorso Finanza

Tesi di Laurea Magistrale

Il Mercato Delle Criptovalute

Efficienza ed Opportunità di Investimento

Politecnico di Torino

Relatore:

Prof.ssa Laura Rondi

Correlatore:

Prof. Franco Varetto

Candidato:

Michelangelo Boezi

Anno Accademico 2021/2022

Ai miei genitori e a tutte le persone che mi hanno accompagnato in questo lunghissimo ma bellissimo percorso di vita durato cinque anni

Indice

Indice delle figure

Indice delle tabelle

Premessa e scopo del lavoro

Il presente lavoro di Tesi è volto ad offrire una panoramica su un nuovo tipo di asset finanziario digitale, nato e introdotto nei mercati internazionali da poco più di dieci anni, ossia le criptovalute.

A tal riguardo si evidenzia come la Banca D'Italia (rif. [29]) definisca le valute digitali come "*...rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente. Create da soggetti privati che operano sul web, le valute virtuali non devono essere confuse con i tradizionali strumenti di pagamento elettronici (carte di debito, carte di credito, bonifici bancari, carte prepagate e altri strumenti di moneta elettronica, ecc.). Le valute virtuali differiscono dalle piattaforme elettroniche finalizzate esclusivamente a favorire transazioni assimilabili a forme di baratto.*"

Da tale definizione emerge, quindi, chiaramente e nettamente come le criptovalute non debbano essere paragonate alle valute tradizionali rispetto alle quali, sebbene lo scopo ultimo sia lo stesso, differiscono in molte caratteristiche e principi.

L'obiettivo, dunque, di questo elaborato sarà proprio quello di analizzare la seconda parte della summenzionata definizione andando così ad approfondire tutte quelle differenze, teoriche e pratiche, tra valute tradizionali e valute digitali.

Questo lavoro, quindi, si articola in quattro macro-capitoli, ognuno dei quali aventi paragrafi e sottoparagrafi dedicati a concetti specifici. All'interno di essi viene affrontato un tema volto a mettere in evidenza gli aspetti salienti e le peculiarità tipiche delle criptovalute e a confrontarle, di conseguenza, con le valute tradizionali.

In particolare, il Capitolo 1 è dedicato alla digitalizzazione della moneta ed è incentrato su come, nel corso del tempo, l'utilizzo e la concezione della moneta siano cambiati fino a giungere ad una (quasi) completa digitalizzazione. Dal Capitolo 2 in poi si entra nel vivo della trattazione, più specifica e vicina al mondo della criptovalute, dove viene analizzata la tecnologia su cui le valute digitali si basano, ossia la blockchain. Verrà, quindi, specificato e illustrato come avviene una transazione di criptovalute e quali sono

gli attori presenti all'interno di questo network. Si prosegue poi con il Capitolo 3, dedicato all'analisi tecnica delle criptovalute, all'interno del quale vengono introdotte ed esaminate le regole tecniche di trading utilizzate e come queste si trasformino in indicatori di profittabilità per gli investitori. Si conclude con il Capitolo 4, dedicato al tema delle CBDC, valute digitali emesse dalle Banche Centrali, e alle implicazioni economiche che si potrebbero verificare qualora le banche decidessero di emettere una propria valuta digitale.

CAPITOLO 1
LA DIGITALIZZAZIONE DELLA MONETA

La digitalizzazione ha rivoluzionato e sta rivoluzionando tutt'ora la moneta e i sistemi di pagamento. Sebbene il concetto di moneta digitale si sia inserito da diverso tempo nelle economie moderne, la sua espansione non si è ancora sviluppata a tal punto da renderlo interscambiabile con altri sistemi di pagamento, nonostante le valute digitali semplifichino enormemente il trasferimento di valore tramite modello *peer-to-peer* in un modo impensabile fino a poco tempo fa. Le nuove valute digitali diverranno cardini centrali per i nuovi sistemi di pagamento ridefinendo il modo in cui interagiscono pagamenti e informazioni degli utenti. L'avvento di queste nuovi tipi di monete potrebbe riscrivere la natura della concorrenza tra valute, la struttura del sistema monetario internazionale e il ruolo del denaro emesso dai governi centrali. Il denaro digitale è già diffuso in molteplici realtà economiche. Si pensi, ad esempio, ai portafogli digitali di Alipay e WeChat in Cina, oppure al lancio di Libra, la valuta digitale di Facebook.
Prima di proseguire con la discussione, è importante aprire una breve parentesi sul ruolo della moneta nell'economia moderna; la moneta svolge tre funzioni (rif. [29]): unità di conto, riserva di valore e mezzo di pagamento.

1) Unità di conto: la moneta viene utilizzata per confrontare in maniera omogenea il valore di prodotti e servizi molto diversi tra loro, agevolando così le decisioni economiche e gli accordi contrattuali.
2) Riserva di valore: la moneta permette di spostare nel tempo la quota di reddito che non viene utilizzata immediatamente per consumare beni e servizi. In altri termini, consente di conservare (risparmiare) una quota del reddito corrente per spenderlo in futuro.

3) Mezzo di pagamento: la moneta può essere scambiata istantaneamente con beni e servizi: l'acquirente consegna moneta al venditore e in questo modo si libera da ogni obbligo nei confronti di quest'ultimo che, accettandola, ne riconosce il valore.

Lo scopo di questo capitolo è discutere degli aspetti chiave e delle implicazioni economiche delle valute digitali. La prima intuizione è relativa al fatto che le valute digitali possiedono caratteristiche che scindono le tre funzioni della moneta sopra descritte rendendo la competizione più agguerrita. Le valute digitali possono avere dei ruoli ben definiti ed agire esclusivamente come mezzo di pagamento o come riserva di valore. Il secondo pensiero consiste nel fatto che gli emittenti di denaro digitale agiranno cercando di "differenziare il loro prodotto" aggregando le funzioni della moneta con altre che normalmente non ne fanno parte, come la raccolta dati e funzioni fino ad ora riservati ai social network. La convertibilità tra le valute digitali e l'interoperabilità delle piattaforme possono essere necessarie per sfruttare al massimo i benefici di questo tipo di concorrenza. L'importanza della connessione digitale, che spesso sostituisce l'importanza dei legami macroeconomici, porterà alla creazione di "aree di valuta digitale" (*Digital Currency Areas*, DCAs) che collegano la valuta all'utilizzo di una particolare rete digitale piuttosto che a un Paese specifico. Il carattere internazionale di queste valute digitali renderà sia le economie emergenti che quelle avanzate vulnerabili alla "dollarizzazione digitale", in cui la valuta nazionale è soppiantata da un'altra valuta di una piattaforma digitale piuttosto che la valuta di un altro Paese sviluppato. Nella parte finale del capitolo verrà discusso come l'integrazione delle valute digitali nell'economia tradizionale pone importanti quesiti riguardanti la competizione tra denaro pubblico e privato. In un'economia digitale, l'eventuale scomparsa del denaro liquido potrebbe indebolire i canali tradizionali della politica monetaria, in quanto le transazioni sarebbero dipendenti da piattaforme decentralizzate e non più soggette al controllo delle banche.

1.1 I Sistemi Monetari

Per poter comprendere il significato di valuta digitale, è necessario prima descrivere la struttura ed il design dei sistemi monetari tradizionali. Successivamente, verrà discusso come le valute digitali si inseriscono nel sistema tradizionale.

1.1.1 L'Architettura dei Sistemi Monetari

Storicamente, i sistemi monetari tradizionali sono sempre stati legati ad un'"ancora". Qualsiasi strumento di pagamento nel sistema monetario è strettamente connesso ad un ammontare fisso di quest'ancora. L'ancora può assumere diverse forme, come una *commodity* o una *fiat currency*. Con il termine commodity si intende un bene per cui è presente domanda ma viene offerto senza differenze qualitative sul mercato ed è fungibile, cioè il prodotto è lo stesso indipendentemente da chi lo produce, come per esempio il petrolio o i metalli. Per fiat currency, invece, si intende uno strumento di pagamento non coperto da riserve di altri materiali e quindi privo di valore intrinseco. La moneta legale (tipicamente sotto forma di banconote) ha un valore grazie al fatto che esiste un'autorità (lo Stato) che agisce come se avesse questo valore. Se un'organizzazione abbastanza grande (ovvero una collettività) emette, utilizza e accetta qualcosa come pagamento, automaticamente quel qualcosa acquisisce valore, dato che gli è riconosciuta fiducia come mezzo di scambio. Attualmente, l'ancora in molti sistemi monetari è la fiat currency emessa dal governo di quel sistema (ad esempio dollaro, sterlina o euro).

Coloro che emettono moneta possono offrire convertibilità completa oppure possono coprirla con altri asset. Sotto un regime di convertibilità, colui che detiene uno strumento monetario si impegna legalmente a scambiarlo, ad un determinato tasso, con un altro strumento. La convertibilità ha come obiettivi quelli di mantenere costante il valore della valuta e di fare in modo che uno strumento di pagamento possa replicare la funzione di riserva di valore e l'unità di conto di un altro. Un sistema di convertibilità tra diversi tipi di moneta crea uniformità tra di loro, la cosiddetta "uniformità della moneta". L'esempio tipico di un'istituzione che offre piena convertibilità è la banca: i depositi bancari possono essere convertiti in eguale quantità in fiat currency emesse dai governi. Qualora la banca non adempiesse ai suoi obblighi, i depositi da essa detenuti cesserebbero di circolare e i titolari di questi potrebbero rivalersi sugli asset illiquidi della banca.

D'altro canto, anche la copertura (*backing*) della moneta favorisce il valore dello strumento monetario, ma garantisce a colui che lo detiene un grado di libertà più elevato. Un ente che copre la sua moneta con altri asset non sempre offre la piena convertibilità. Esempi di alcune coperture sono i cosiddetti *currency peg*, ovvero strategie attuate dai

governi che prevedono un tasso di cambio fisso per la valuta domestica nei confronti di una o più valute estere, e i *currency band*, ossia range di valori stabiliti dai governi all'interno dei quali il tasso di cambio può collocarsi.

Infine, la moneta può manifestarsi in più forme, di cui se ne evidenziano principalmente due: la forma basata sui conti correnti e la forma basata sui *token*. La differenza sostanziale tra le due è il processo di verifica dei pagamenti. Nella forma *account-based* è cruciale verificare l'identità di colui che paga. Per esempio, i depositi bancari sono basati sui conti correnti dei clienti e un pagamento da uno di questi viene considerato valido se la banca è in grado di confermare che la persona che effettua il pagamento è il titolare del conto. In un sistema basato sui token la verifica riguarda l'autenticità dell'oggetto di scambio. Le banconote e le monete sono degli esempi di token monetari ed in una transazione l'esercente accetta il denaro solo se questo non è contraffatto, senza verificare se appartiene effettivamente al cliente. Lo stesso principio si può applicare alle criptovalute: nelle transazioni è richiesta la chiave privata dell'utente affinché queste vengano accettate, ma non viene fatto nessun controllo sul detentore della chiave.

1.1.2 Caratteristiche di una Valuta Indipendente

Per poter comprendere cosa costituisce una valuta indipendente, è necessario definire il concetto di "appartenenza" di uno strumento di pagamento ad una valuta. Un insieme di strumenti di pagamento crea una valuta indipendente se le seguenti condizioni sono soddisfatte:

1) Gli strumenti di pagamento sono denominati nella stessa unità di conto
2) Ogni strumento di pagamento all'interno della valuta è convertibile in un altro

È necessario adottare questa definizione di valuta indipendente per fare in modo che gli strumenti monetari siano collegati ad una valuta attraverso la loro funzione di unità di conto piuttosto che al ruolo di mezzo di scambio. Quindi, per esempio, il denaro liquido, le riserve e i depositi bancari, denominati in una valuta ufficiale, sono tutti parte della stessa valuta nonostante abbiano caratteristiche molto diverse.

Se uno strumento di pagamento non fa parte di una valuta esistente, allora viene considerato valuta indipendente. Secondo questa definizione, un accordo di scambio valutario, come il dollaro di Hong Kong, costituisce una valuta indipendente dal dollaro

statunitense, in quanto è denominata nella propria unità di conto e l'ancoraggio mantenuto dalla banca centrale non è legalmente vincolante. I depositi bancari denominati in dollari non sono una valuta indipendente poiché l'accordo di convertibilità è legalmente valido e applicabile. In altre parole, il fattore che distingue le valute indipendenti è il livello di impegno dell'emittente. Un emittente di una valuta indipendente denominata in un'unità di conto esistente mantiene l'opzione di non adempiere a nessun impegno di convertibilità concordato in passato. Gli emittenti di strumenti di pagamento che non sono valute indipendenti perdono i diritti residui sulle loro attività se non rispettano le loro promesse.

Questa definizione suggerisce che diverse forme di denaro digitale siano, di fatto, valute indipendenti. Per esempio, il paniere sottostante la valuta Libra di Facebook consiste di molte valute ufficiali, ragion per cui Libra viene denominata nella sua propria unità di conto e quindi viene considerata indipendente. Anche le criptovalute sono valute indipendenti, in quanto non possono essere convertite, e possiedono una propria unità di conto. Questo include tutte le criptovalute più popolari, come il Bitcoin ed Ethereum. Perfino alcune monete stabili, sostenute da un conto bancario di proprietà dell'entità emittente, sono valute indipendenti, perché potrebbero continuare ad esistere in uno scambio anche nel caso in cui l'emittente abbandoni unilateralmente il supporto della moneta.

Altri tipi di denaro digitale non sono valute completamente indipendenti, ma tuttavia consentono trasferimenti di valore che prima non erano possibili. Per esempio, molte applicazioni mobili ora permettono trasferimenti digitali peer-to-peer, mentre gli stessi trasferimenti digitali attraverso il sistema bancario tradizionale erano tipicamente limitati agli acquisti. Queste applicazioni, come Alipay in Cina, permettono alle valute esistenti di circolare in un nuovo modo e tra nuove popolazioni, ma i loro emittenti sono legalmente vincolati a mantenere convertibilità nelle valute dei loro Paesi.

1.2 Il Cambiamento nella Competizione tra Valute

1.2.1 I Ruoli della Moneta

Tradizionalmente la moneta è sempre stata definita come un asset che svolge le tre funzioni precedentemente descritte. In particolar modo, il ruolo di unità di conto è molto importante poiché è stato sviluppato per mitigare il problema relativo al tracciamento dei prezzi dei diversi beni. In un'economia con n beni, in assenza di unità di conto, dovrebbero essere tracciati $n(n-1)/2$ prezzi. Nella realtà, essendo presente tale funzione, i prezzi da tracciare sono solamente $n-1$, ossia il prezzo di ciascun bene. Questa breve descrizione permette di capire come il ruolo di unità di conto permetta agli agenti economici di comunicarsi a vicenda il valore dei beni in modo comprensibile. In altre parole, è una sorta di linguaggio comune.

La necessità della funzione di riserva di valore deriva dalla difficoltà da parte degli operatori economici di accettare denaro in quanto non sicuri che questo possa mantenere il suo valore nel futuro. Il ruolo di questa caratteristica è assicurare che la moneta mantenga il suo valore costante nel tempo in modo tale da poter essere proposta e accettata dalle parti coinvolte. La competizione si gioca in larga parte sotto questo ruolo; infatti, le valute emesse da enti credibili saranno più inclini a mantenere costante il loro valore e di conseguenza a sopravvivere nel mercato.

Infine, la funzione di mezzo di scambio è necessaria per risolvere il problema di equivalenza nelle trattative. Per poter capire questo concetto, si supponga per assurdo che la moneta non sia un mezzo di scambio valido. Questa ipotesi è estremamente improbabile nelle economie avanzate ma, qualora fosse vera, significherebbe che, nelle compravendite, sia necessario trovare beni o servizi equivalenti in termini di valore al fine di concludere la trattativa. Per esempio, in assenza di tale funzione, un medico che desidera prendere un taxi potrebbe farlo solamente nel caso in cui trovasse un tassista che necessita di una visita medica. Il denaro permette il commercio in assenza di equivalenza nelle trattative. Quando un operatore (il compratore) vuole un bene o un servizio che un altro (il venditore) produce, l'acquirente può semplicemente trasferire denaro al venditore in cambio del bene.

1.2.2 Forme di Competizione

L'avanzamento tecnologico e le piattaforme digitali stanno alterando profondamente la natura della competizione e, a questo proposito, è utile distinguere due forme di competizione monetaria:

1) Competizione completa: sotto questo regime, le valute competono anche assumendo la funzione di unità di conto. La competizione avviene tra strumenti monetari che differiscono in tipologia di unità di conto, con differenti sistemi di prezzi e diversi tassi di inflazione. Le valute possono competere con altre estere, come avviene con le valute fiat, oppure internamente, dal momento in cui ad enti privati è concesso emettere valute proprie.
2) Competizione ridotta: sotto questo regime, gli strumenti monetari con la stessa unità di conto competono nel ruolo di mezzo di scambio. Questa tipologia di competizione è largamente diffusa all'interno dei Paesi. Tipicamente i regolatori incoraggiano questa competizione per perseguire l'efficienza.

1.2.3 La Scissione dei Ruoli della Moneta

L'utilizzo della moneta da parte degli individui genera un effetto noto come esternalità di rete. Tale effetto si manifesta nel momento in cui l'utilità percepita dal consumo di un bene dipende dal numero di utenti che hanno acquistato quel prodotto o usufruiscono di quel servizio. Applicando il concetto alla moneta, la necessità di un'unità di conto dà luogo a esternalità di rete nello stesso modo in cui, per utilizzare una metafora, avviene con una lingua comune. Sarebbe difficile interagire parlando solo italiano in una società in cui tutti parlano solo inglese; allo stesso modo, sarebbe difficile contrattare usando l'euro in una società dove beni e servizi sono quotati in dollari. Proprio come imparare più lingue è difficile, adottare più valute e seguire i loro valori relativi può essere altrettanto difficile. Per questo motivo, sono presenti forti incentivi ad adottare una sola valuta.

La convertibilità potrebbe rivelarsi una caratteristica capace di scindere il ruolo di riserva di valore e di mezzo di scambio. Il primo a teorizzare questa possibilità fu Thomas Gresham, mercante inglese del XVI secolo che affermò l'assunto per cui "la moneta

cattiva scaccia quella buona". Tale concetto, in altre parole, definisce, da una parte, la tendenza degli operatori economici a pagare solamente con monete danneggiate, e quindi con minor valore intrinseco (in termini di metallo prezioso costituente) rispetto al loro valore nominale, e, dall'altra, ad accettare solo monete nuove, il cui valore intrinseco rispecchiasse quello nominale. Questo comportamento fa sì che sempre più monete "buone" saranno trattenute da chi le ha ricevute, mentre le monete utilizzate per le transazioni saranno in sempre maggior numero quelle "cattive". Si ipotizzi di applicare questo concetto ad un contesto in cui sono presenti due aziende che si accordano per emettere token digitali convertibili uno a uno. Ciascuna compagnia assicurerà la propria valuta con il proprio bilancio e la valuta emessa dall'azienda con il bilancio più solido sarà quella che manterrà meglio il suo valore, mentre l'altra fungerà principalmente come mezzo di scambio.

Oltre alla convertibilità, anche i costi di cambio (*switching costs*) generano esternalità di rete. Nel passato, i costi di transazione rendevano difficili effettuare transazioni cambiando valuta, incentivando così ad operare utilizzandone solo una. Questo comportamento non permetteva alle valute di competere con efficacia principalmente per due motivi: in primo luogo, le valute ufficiali in carica hanno un grande vantaggio in termini di fiducia rispetto ad altre che entrano in competizione; il secondo motivo è conseguenza del primo in quanto, anche qualora fossero presenti più valute all'interno di un territorio, la competizione risulterebbe essere più confusionaria che benefica. Ne è un esempio il fatto che fino alla metà del XIX secolo in molti Stati (inclusi gli Stati Uniti), il commercio era basato su molteplici valute alquanto bizzarre, alcune delle quali risultavano praticamente inutilizzabili a causa delle diverse stime di solvenza delle banche.

La competizione economica nei network digitali e tra le valute digitali differisce nettamente dalla competizione tradizionale affrontata finora. Internet fornisce l'infrastruttura su cui le reti digitali, sia commerciali che sociali, possono essere costruite. Per esempio, Amazon ha creato un nuovo ecosistema all'interno del quale possono essere scambiati beni di ogni tipo; Facebook è un social network con più di tre miliardi di utenti. Le informazioni presenti in questi colossi possono essere scambiate facilmente e istantaneamente per poter poi essere convertite in un output nella forma più appropriata

per il ricevente. Le moderne tecnologie non contengono frizioni né intermediari e sono basate su transazioni di token digitali in formato peer-to-peer.

Le esternalità di rete che, di norma, ostacolano la competizione nei modelli tradizionali agiscono a supporto della stessa in contesti digitali. Una qualsiasi istituzione che emette una propria valuta è in grado di sfruttare i principi di comunicazione dei network e i sistemi di transazione per avere accesso immediato ad informazioni riguardanti potenziali competitor in molteplici Paesi. I network facilitano la diffusione e l'adozione della valuta, dal momento in cui ogni competitor è in grado di conoscere se altri sono connessi a reti di pagamento comuni. La struttura dei network digitali riduce le barriere all'entrata presenti nei sistemi tradizionali.

Un altro fattore che limita la competizione negli ambienti tradizionali è la presenza dei costi di cambio, il cui impatto è notevolmente ridotto in contesti digitali. La capacità di scambiare denaro direttamente in valute diverse (peer-to-peer) all'interno dei network elimina di fatto la necessità di un intermediario, e di conseguenza viene eliminata anche la tassa richiesta da quest'ultimo. Per un livello di accessibilità ancora più immediato, gli utenti potrebbero configurare i loro telefoni per eseguire scambi di valute in ogni momento qualora ne avessero necessità. D'altra parte, l'utilizzo di applicazioni mobili riduce il livello di conoscenza in materia finanziaria per poter eseguire tali operazioni.

In passato, a causa del commercio limitato in zone geografiche limitrofe, la diffusione di una specifica valuta risultava pressoché impossibile, salvo rarissimi casi come l'euro o il dollaro. I network digitali sono risolutivi anche per ovviare a questo problema in quanto capaci di oltrepassare i vincoli geografici imposti dallo scambio di valute fisico, per cui sono fruibili da centinaia di milioni di utenti.

La conseguenza della diminuzione dei costi di cambio è il tema centrale di questo sottoparagrafo: la scissione dei ruoli della moneta, che si manifesta come una delle caratteristiche chiave della competizione tra valute digitali. Nel momento in cui i costi di cambio sono bassi, non vi è più incentivo a utilizzare una valuta come riserva di valore, mezzo di scambio e unità di conto. Infatti, gli utenti possono cambiare valuta senza soluzione di continuità e convertirla in unità quando necessario.

Per comprendere questo concetto, si supponga che esista una valuta *A* competitiva come riserva di valore ma non come mezzo di scambio, e una valuta *B* con proprietà opposte ad *A*. Un utente generico, conscio di queste caratteristiche, decide di detenere *A* e

convertirlo in *B* solo pochi istanti prima di una transazione, ignorando il rischio di cambio. Così facendo, la caratteristica di *B* di essere poco prestante come riserva di valore non danneggia l'utente, dal momento che *B* viene detenuto solo per pochi istanti. Lo stesso ragionamento può essere applicato nel caso in cui siano presenti due operatori economici che desiderano scambiare valore attraverso un network ma utilizzando unità di conto diverse. In questo caso, la tecnologia alla base della rete converte facilmente l'offerta di uno dei due agenti in unità accettabili per l'altro. Come già discusso precedentemente, in questo modo vengono ridotti al minimo anche i costi di transazione, per cui non c'è incentivo a utilizzare una sola valuta. Nel complesso, quindi, la scissione dei ruoli della moneta riduce la necessità di coordinamento su una valuta unica. Tale risultato si ottiene permettendo agli utenti di ottenere i diversi servizi forniti dalla moneta da molteplici asset e mitigando l'importanza del coordinamento su un asset comune tra gli utenti.

Prima dell'avvento della tecnologia, le valute si sono sempre confrontate come riserva di valore, ma storicamente questo tipo di competizione è stata limitata a causa dei costi di cambio e delle esternalità di rete. La scissione porta le valute a specializzarsi in un ruolo ben delineato. Alcune che si comportano come riserva di valore possono competere tra loro mentre altre che fungono da mezzo di scambio avranno una competizione a parte. Frizioni, vincoli ed esternalità di rete ridotti fanno in modo che la competizione si sposti su diversi livelli di dettaglio invece che su un'unica dimensione.

1.2.4 Le Piattaforme di Pagamento e la Riaggregazione dei Ruoli della Moneta

Il ruolo delle piattaforme nell'economia delle valute digitali è molto diverso dal ruolo di scissione nelle reti digitali. L'economia delle piattaforme rappresenta uno dei fenomeni sociali ed economici più praticati e discussi degli ultimi anni. Provando a darne una definizione ampia, essa può essere intesa come un insieme variegato di pratiche e modelli che utilizzano le tecnologie digitali per facilitare il contatto, lo scambio e la collaborazione tra le persone. Nella letteratura economica, le piattaforme sono tipicamente considerate mercati in cui si interfacciano acquirenti e venditori scambiandosi diversi prodotti. Gli strumenti di pagamento digitali, associati alle

piattaforme, sono in grado di combinare le funzioni tradizionali della moneta con le funzionalità della piattaforma, arrivando così ad una "ricostruzione" dei ruoli della moneta.

1.2.4.1 Le Piattaforme Digitali

La logica sottostante le piattaforme è la loro abilità di sviluppare e ottimizzare i rapporti tra le diverse attività che possono essere svolte sulle stesse. In questo ambito, le piattaforme giocano un ruolo fondamentale perché riescono a sfruttare e veicolare l'input che gli viene dato, ossia i dati. I dati e le informazioni inseriti vengono registrati e riutilizzati dalla piattaforma sotto forma di output per poter suggerire, ad esempio, nuovi prodotti in linea con le ricerche, o per far interagire più utenti tra loro. Oggigiorno, molte piattaforme, come Amazon, comprendono queste funzioni. Tra queste, la più importante è il pagamento: tutte le altre attività dipendono dal pagamento e la maggior parte dei dati utili viene generata attraverso questa fase. Per cui, avere una funzione di pagamento sicura ed efficace è cruciale per il valore e la crescita della piattaforma.

La funzione di pagamento assume una maggior rilevanza quando sulla piattaforma è presente molta diversità nei dati: vale a dire che i benefici di un *database* non derivano solamente dalla sua dimensione, ma soprattutto dalla sua diversità in quanto è largamente preferibile avere informazioni su un milione di persone prese casualmente rispetto ad un milione di persone della stessa città.

Dal momento in cui il pagamento è utilizzato essenzialmente in tutte le attività di natura economica, sarebbe impensabile per una piattaforma rivaleggiare con un'altra specializzata in strumenti di pagamento, sul piano della raccolta e aggregazione di informazioni economiche. Si pensi, ad esempio, ad una banca che deve valutare una richiesta di prestito. Se la banca avesse a disposizione l'accesso a tutti i movimenti dell'utente nelle varie piattaforme, riuscirebbe a tracciare introiti e pagamenti, con un livello di dettaglio che include frequenze, luoghi e natura dei pagamenti. In altre parole, sarebbe in grado di stimare con grande precisione la probabilità di vedersi restituito il proprio capitale prestato (e quindi il grado di insolvenza dell'utente). I dati sui pagamenti generati dalle piattaforme sono strumenti efficaci per prevedere preferenze e comportamenti degli utenti. Non è inusuale, infatti, che molti algoritmi per tracciare i

prezzi dei beni, selezionare pubblicità mirata e prodotti suggeriti siano presenti su piattaforme basate sui pagamenti.

1.2.4.2 Il *Re-bundling* della Moneta

L'economia delle piattaforme digitali ha importanti implicazioni per la competizione valutaria. Le valute digitali associate alle piattaforme saranno molto più differenziate rispetto alle valute ordinarie e differiscono non solo nelle loro funzioni tradizionali, ma anche nelle funzionalità offerte dalle piattaforme stesse. Vale a dire che le valute non garantiscono più semplicemente servizi di pagamento, ma concedono anche l'accesso alle interazioni con altri utenti della piattaforma. Quindi, una valuta digitale è inseparabile dalle caratteristiche della piattaforma su cui viene scambiata.

Le caratteristiche tradizionali di una valuta, come la sua capacità di immagazzinare valore, potrebbero non essere sufficienti per determinare il suo successo in un mondo in cui queste caratteristiche possono essere separate. Piuttosto, il fascino di una valuta sarà probabilmente determinato da altre caratteristiche della piattaforma, come gli algoritmi di elaborazione delle informazioni, le sue politiche sulla privacy dei dati e l'insieme di controparti disponibili sulla piattaforma. La concorrenza tra valute sarà effettivamente una concorrenza tra informazioni e servizi di rete. Questa ipotesi prende il nome di *re-bundling* della moneta.

Il re-bundling ha ulteriori implicazioni per la concorrenza valutaria. Con valute ordinarie, la maggior parte degli utenti ha preferenze uniformi per quanto riguarda le loro proprietà fondamentali. Gli utenti vorrebbero valute che siano largamente accettate e che possano essere usate per immagazzinare valore in modo sicuro. Le esternalità della rete sono la barriera alla competizione tra valute. Con le valute digitali "potenziate" dalle funzioni delle piattaforme, invece, le preferenze degli utenti possono essere molto più eterogenee. Alcuni utenti potrebbero volere garanzie assolute di privacy, mentre altri potrebbero preferire una piattaforma che faccia un uso maggiore dei loro dati per fornire migliori raccomandazioni. Le esternalità di rete sono meno restrittive, dato che le funzioni monetarie sottostanti le valute digitali possono essere disaggregate. Questa eterogeneità nelle preferenze, quindi, incentiva i grandi emittenti a differenziare i loro prodotti, creando mercati segmentati in cui diverse piattaforme si rivolgono a diversi tipi di consumatori.

1.2.5 La Struttura dei Mercati basati sulle Piattaforme

Un'economia incentrata sulle piattaforme digitali è strutturata diversamente dall'attuale sistema. L'organizzazione del sistema finanziario e l'assegnazione della proprietà dei dati cambierebbero entrambe. La natura delle piattaforme potrebbe anche cambiare il panorama competitivo dell'economia. Mentre le piattaforme creano connessioni precedentemente impensabili, possono tendere verso monopoli o mercati frammentati; quindi, la questione dell'interoperabilità tra piattaforme assume una importanza reale.

1.2.5.1 L'Inversione dell'Organizzazione delle Attività Finanziarie

La centralità dei pagamenti e dei dati sulle piattaforme sociali e commerciali può portare a un'inversione dell'attuale organizzazione industriale delle attività finanziarie. In molte economie moderne, i servizi di pagamento sono offerti come un'estensione delle attività di intermediazione delle banche nel loro ruolo di punto di contatto per tutti gli utenti del sistema di pagamento. In molti paesi, il dominio delle banche nelle attività finanziarie si estende fino alla fornitura di servizi di assicurazione e servizi di gestione patrimoniale. Il sistema finanziario, e il modo in cui i consumatori immagazzinano e scambiano valore, è organizzato intorno alle banche e al credito. Come illustrato in Figura 1.1, le banche possono essere pensate come il vertice della gerarchia finanziaria, mentre i pagamenti, essendo dipendenti dal ruolo centrale delle banche, sono posti alla base. In un'economia basata sulle piattaforme, questa gerarchia potrebbe essere ribaltata: i pagamenti verrebbero collocati al centro di qualsiasi piattaforma economica, e tutte le altre attività si organizzerebbero intorno alla funzionalità di pagamento centrale. Il punto di contatto dei consumatori sarebbe l'entità che possiede la piattaforma piuttosto che una banca. In questo nuovo tipo di gerarchia finanziaria, le istituzioni finanziarie tradizionali come le banche potrebbero essere sostituite da filiali *fintech* di sistemi di pagamento, come ad esempio avviene già in Cina dove Yu'e Bao, filiale di Ant Financial (il ramo finanziario di Alibaba), è diventato il più grande fondo comune di mercato monetario del mondo.

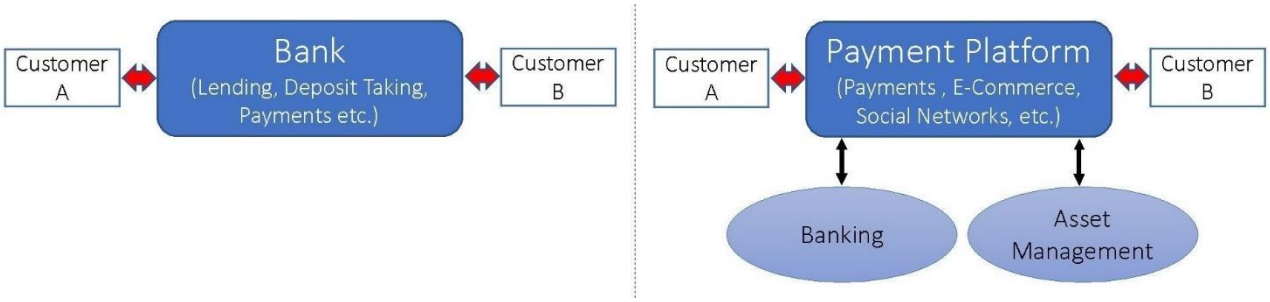

Figura 1.1 – L'Inversione Organizzativa nei Servizi Finanziari

1.2.5.2 Proprietà e Regolamentazione dei Dati

Le economie si stanno muovendo verso un regime in cui le grandi aziende tecnologiche agiscono come intermediari di dati. Anche oggi, è presente la preoccupazione che queste aziende abbiano un eccessivo potere sui dati degli utenti, il che porta a regolamentazioni come il *General Data Protection Regulation* (GDPR). Queste apprensioni saranno inevitabilmente destinate ad aumentare qualora le attività di intermediazione dei dati si diffonderanno attraverso tutti gli aspetti del sistema dei pagamenti. Nel sistema attuale, le banche e le società di carte di credito hanno il maggiore accesso ai dati delle transazioni, tant'è che ogni volta che viene effettuata una transazione, la banca (o la compagnia proprietaria della carta di credito) può vedere esattamente quando, dove e in che modo è avvenuta la transazione. Questi dati sono utilizzati principalmente per valutare la solvibilità degli utenti, parametro che permette agli istituti di credito di decidere i tassi di interesse da proporre ai diversi individui. La struttura della proprietà dei dati di pagamento potrebbe cambiare drasticamente in un'economia dominata da piattaforme digitali. Una considerazione che può essere fatta riguarda gli emittenti di valuta digitale e la possibilità che questi emergano come operatori importanti nei mercati valutari, ma che allo stesso tempo le banche continuino ad interagire con le valute digitali in modo rilevante. Questo concetto può essere compreso con un esempio pratico, facendo riferimento ad un'economia attualmente operativa in Cina. Alipay e WeChatPay emettono grandi quantità di valuta digitale e gestiscono applicazioni che permettono trasferimenti da e verso conti bancari. Come conseguenza, sia gli emittenti di valuta

digitale che le banche hanno accesso ad alcuni dati sulle transazioni. Un allontanamento più radicale dal sistema è quello in cui i grandi emittenti di moneta digitale sostengono le loro valute con depositi detenuti presso le grandi banche, ma i consumatori detengono esclusivamente moneta digitale. Questo tipo di struttura è affine a quello attuale, in cui i consumatori detengono depositi che sono coperti da riserve, ma non detengono le riserve direttamente. Tuttavia, le implicazioni per la proprietà dei dati sono molto diverse poiché se i consumatori detengono esclusivamente moneta digitale, allora gli emittenti di moneta digitale agiscono come oligopolisti dell'informazione. Le banche non sono in grado di monitorare i dati delle transazioni senza acquistarli. Infatti, gli emittenti di valuta digitale potrebbero trovare più efficiente istituire banche come filiali al fine di evitare di cedere i loro dati. In questo caso, lo scopo principale e il valore derivato dai dati delle transazioni non sarebbe quello di fornire credito in modo più efficiente, ma piuttosto di monitorare i gusti e le tendenze dei consumatori. Le considerazioni sulla privacy e sull'efficienza che la politica dovrebbe soppesare sarebbero molto diverse in questo tipo di sistema, e forse sarebbero necessari regolamenti atti a limitare i tipi di dati che potrebbero essere raccolti.

1.2.5.3 Interoperabilità, Convertibilità e Incentivi di sconto delle Piattaforme

La diversità dei servizi offerti dalle piattaforme le porta a svilupparsi come ecosistemi chiusi. I consumatori vorrebbero essere in grado di utilizzare la valuta di una piattaforma per acquistare una vasta gamma di beni e servizi di cui hanno bisogno nella vita quotidiana.

Dal punto di vista del proprietario della piattaforma, è auspicabile che i consumatori usino la piattaforma stessa per tutte le attività poiché il valore del monopolio della piattaforma si basa sui dati che transitano attraverso di essa. D'altra parte, è preferibile per i consumatori distribuire le loro attività su più piattaforme, dal momento in cui queste siano specializzate in funzioni diverse. Il disinteresse del proprietario della piattaforma nella promozione dell'interoperabilità con altre è quindi in conflitto con l'efficienza economica. In aggiunta, i proprietari delle piattaforme vorrebbero introdurre dei "costi di uscita" che renderebbe oneroso il passaggio ad una valuta o ad un servizio di un'altra piattaforma.

Una mancanza di interoperabilità può creare eccessive barriere al commercio attraverso le reti. Cercare degli incentivi per impedire l'interoperabilità dovrebbe, quindi, essere una

preoccupazione primaria per la politica considerando, in particolar modo, che le grandi piattaforme mostrano riluttanza ad accettarla in alcuni casi. Per esempio, in Kenya, il governo ha approvato un regolamento che obbliga i grandi fornitori di pagamenti mobili, come Safaricom e Orange, a integrare i loro servizi di pagamento dopo che le società si erano inizialmente rifiutate di farlo.

L'importanza della convertibilità per le valute digitali è simile all'importanza dell'interoperabilità per le piattaforme. Le reti e le piattaforme tendono a creare mercati frammentati, ma l'integrazione è fondamentale per il funzionamento efficiente di un sistema monetario e, in particolare, le reti di pagamento non dovrebbero creare barriere onerose al commercio. Un rigoroso regime di convertibilità verso una valuta ufficiale abbassa queste barriere poiché, sotto un regime di questo tipo, sono presenti difficoltà trascurabili per trasferire valore all'interno o all'esterno di una rete digitale. I nuovi utenti possono trasferire valore in una rete senza doversi preoccupare della stabilità della valuta della rete. Quando gli utenti necessitano di scambiare valore con operatori al di fuori della rete, questi possono facilmente trasferire i loro averi fuori dalla rete ad un tasso noto. In un certo senso, la logica della convertibilità è abbastanza simile alla logica che sta alla base delle aree valutarie ottimali, ma in questo caso le linee di demarcazione che devono essere considerate sono i confini delle reti digitali piuttosto che i confini regionali.

Una concorrenza efficiente tra le valute è particolarmente importante quando queste sono abbinate ad altre piattaforme e servizi di dati. La convertibilità permette alle valute di competere sulla base dei pacchetti di servizi che offrono piuttosto che sulla base della reputazione degli emittenti. I nuovi imprenditori che vogliono approcciarsi a questo mondo possono, quindi, beneficiare di un regime in cui tutte le piattaforme devono offrire la convertibilità della valuta.

Dato il valore di una posizione di mercato dominante, le piattaforme possono anche adottare strategie di espansione aggressive che siano vantaggiose per gli utenti nel breve periodo ma non nel lungo: vale a dire che una piattaforma può tentare di espandere le sue operazioni facendo accordi con altri fornitori di servizi nell'economia. Per esempio, una piattaforma può unirsi a grandi catene per offrire sconti ogni volta che la sua valuta viene utilizzata per un acquisto, come ha già provveduto a fare Alipay in Cina. Queste strategie possono essere efficaci per far crescere la rete, ma i benefici per gli utenti possono alla

fine dissiparsi, quando la piattaforma diventa così sistematicamente importante che loro non possono più abbandonarla. Ad oggi questi sviluppi sono nella loro fase iniziale e sono piuttosto limitati nella loro portata geografica. La tecnologia, tuttavia, porta con sé una rapida espansione geografica, e le reti di pagamento si stanno già espandendo in paesi vicini come la Malesia e le Filippine.

1.3 La nuova Forma del Sistema Monetario Internazionale

La digitalizzazione può alterare le basi del sistema monetario internazionale tradizionale poiché le valute digitali hanno il potenziale per rimodellare le interazioni economiche, trascendendo i limiti delle cosiddette "Aree valutarie ottimali" (*Optimal Currency Areas*, OCAs) e creando nuove barriere per il commercio. Esse permettono anche di introdurre il concetto di valuta sintetica internazionale.

1.3.1 Aree di Valuta Digitale

In un'economia digitale, le interazioni tra gli operatori avverranno entro i confini di quella che viene definita "Area di valuta digitale" (*Digital Currency Area*, DCA). Questa si definisce come una rete all'interno della quale i pagamenti e le transazioni vengono effettuate digitalmente utilizzando una valuta specifica per quella rete. Con "specifica", si intende che tale rete sia in possesso di una o entrambe le caratteristiche elencate di seguito:

1) Nella rete viene utilizzata un'unità di conto propria, distinta dalle valute ufficiali esistenti. Per esempio, Facebook ha lanciato la propria valuta chiamata Libra, che si configura come una rappresentazione digitale di un paniere di valute esistenti e definisce, quindi, una nuova unità di conto. Di conseguenza, a seguito di quanto discusso nella sezione 1.2.2, in queste DCA la competizione è completa.
2) Nella rete è presente un mezzo di pagamento, che funge da mezzo di scambio, utilizzabile solo internamente tra gli utenti del network. Per cui, anche nel caso in cui nella rete si utilizzino valute ufficiali fiat come unità di conto e come sostegno allo strumento di pagamento, quest'ultimo non può essere utilizzato al di fuori del network. Tipicamente, questo avviene nelle reti di alcuni grandi emittenti di denaro elettronico quando queste non sono interfacciabili con altre.

> L'esempio, oggigiorno, è dato dalla Cina dove Tencent e Ant Financial hanno sviluppato molti network con milioni di utenti ma senza la possibilità di comunicare con altri. In riferimento a questa seconda caratteristica, si è in presenza di una competizione ridotta poiché le valute non svolgono la funzione di unità di conto.

Com'è facilmente intuibile, le DCA sono molto diverse dalle OCA poiché quest'ultima è caratterizzata dalla prossimità geografica degli individui ed il suo design si focalizza sulla capacità dell'autorità monetaria di appianare gli shock economici, nella misura in cui questi siano comuni a tutti gli operatori, e di migliorare la condivisione del rischio, dal momento che i mercati nelle OCA sono incompleti.

Le DCA, d'altra parte, si basano sull'interconnessione digitale ed il focus non è sull'autorità monetaria, bensì sulla reciproca complementarità delle attività e sulla connessione dei dati che emerge in un ecosistema digitale. La funzione di pagamento permette il pieno sfruttamento di queste connessioni in quanto la tecnologia sottostante al pagamento digitale nelle reti favorisce l'interazione diretta tra gli utenti, che possono effettuare trasferimenti di valore in modo peer-to-peer attraverso applicazioni mobili, mentre fino a poco tempo fa i trasferimenti digitali riguardavano esclusivamente transazioni tramite carte di credito o di debito.

Nel momento in cui i partecipanti condividono la stessa forma valutaria, espressa come unità di conto o meno, si creano forti legami monetari. Per esempio, la trasparenza sul prezzo è più limpida all'interno della rete e la conversione ad altri strumenti di pagamento è meno probabile. Questi legami creano incentivi ad accumulare risorse nella valuta della rete e questo comportamento vale indipendentemente dal fatto che la DCA sia associata ad una piattaforma multifunzione o ad una rete digitale più specifica, come ad esempio un servizio di messaggistica.

Tuttavia, ragionando più approfonditamente, si arriva ad un paradosso quando si parla di DCA, che è bene evidenziare. Si potrebbe pensare che il potenziale delle DCA di espandersi attraverso i confini nazionali porterebbe alla nascita di valute digitali globali. Ma questa ipotesi è facilmente scongiurabile dal momento in cui lo scopo prefissato dalle DCA può essere limitato attraverso quadri normativi specifici. Le reti digitali associate alle DCA potrebbero gestire i dati e la privacy degli utenti in modi molto diverso. Dal momento in cui l'Europa, gli Stati Uniti e la Cina utilizzano normative diverse in merito

di gestione della privacy, è probabile che alcune reti di pagamento digitali siano praticabili solo all'interno di un gruppo ristretto di giurisdizioni. Queste limitazioni portano al paradosso della digitalizzazione: questa avrebbe l'abilità di rompere le barriere e di superare ostacoli tradizionali, come la prossimità geografica, ma a causa delle sue dimensioni inscindibili, potrebbe portare ad una maggiore frammentazione del sistema finanziario internazionale.

1.3.2 La Dollarizzazione Digitale

La digitalizzazione può fornire nuovi modi per "internazionalizzare" valute già esistenti e per trasformare le relazioni monetarie internazionali. Sono presenti, tipicamente, due soluzioni attraverso le quali è possibile internazionalizzare una valuta: renderla una riserva di valore globale oppure renderla un mezzo di scambio per i pagamenti. Storicamente, i due ruoli si sono sempre più avvicinati fino a convergere. Ad ogni modo, è preferibile pensare a diverse strategie per dare uno status internazionale ad una valuta nel XXI secolo. Analizzando l'attuale posizione dominante del dollaro nel sistema monetario internazionale, alcuni economisti enfatizzano la sua funzione di riserva di valore, basandosi su dimensione, profondità e liquidità dei mercati finanziari americani. Altri, invece, danno maggior importanza alla sua funzione di mezzo di scambio. Proprio in riferimento al dollaro nasce il concetto di dollarizzazione: si ha dollarizzazione quando gli abitanti di un Paese utilizzano la valuta emessa da uno Stato straniero in parallelo o in sostituzione della propria. Il termine dollarizzazione non si riferisce necessariamente all'utilizzo del dollaro statunitense, ma, più in generale, vale per ogni valuta straniera che viene preferita ad una moneta nazionale.

La distinzione tra i due ruoli diventa rilevante in un contesto digitale. Svolgere la funzione di riserva di valore è dispendioso in quanto questa implica la piena convertibilità del capitale. Tuttavia, assumendo che lo status internazionale può essere raggiunto attraverso il commercio, è lecito pensare che le reti digitali possano essere un metodo alternativo per internazionalizzare una valuta. Si pensi, ad esempio, ad un commerciante: questo vorrà effettuare acquisti in una valuta e a sua volta vorrà vendere merce nella stessa valuta per assicurarsi di poter effettuare quegli acquisti. Le reti digitali sono particolarmente efficaci nell'aprire nuove possibilità di commercio e nel proliferare un mezzo di scambio oltre i confini nazionali. La natura chiusa degli ecosistemi delle

piattaforme incentiva ulteriormente il commercio utilizzando la valuta della piattaforma. Un Paese sede di grandi reti digitali potrebbe quindi trovare nuovi modi per far sì che la sua valuta ottenga il consenso su larga scala internazionale sfruttando gli effetti di integrazione di una DCA. La digitalizzazione può quindi servire come un potente veicolo per internazionalizzare alcune valute come mezzi di scambio.

Allo stesso modo, altri Paesi possono essere esposti a una concorrenza valutaria più intensa derivante dalle valute straniere attraverso le reti di pagamento oltre confine. I sistemi transfrontalieri utilizzano le valute nazionali come mezzo di scambio e unità di conto. Tuttavia, questo potrebbe cambiare e l'esempio di Facebook, con la valuta proprietaria Libra, mostra come possono essere create reti private che darebbero accesso a nuove e specifiche unità di conto a persone in molti Paesi. Anche le valute ufficiali potrebbero progressivamente entrare nelle economie di altri Paesi se supportate da una forte rete digitale. All'interno di grandi reti, gli stessi strumenti digitali di pagamento possono facilmente essere usati in diverse giurisdizioni. Se così fosse, le reti oltre confine potrebbero avere l'effetto di promuovere l'uso di una specifica unità di conto al di fuori del Paese in cui ha corso legale.

È importante notare che, mentre le piccole economie (specialmente quelle con un'inflazione interna elevata o instabile) sono passibili di una dollarizzazione tradizionale e digitale con una valuta stabile, le economie che sono favorevoli e socialmente aperte alle grandi DCA saranno unicamente sensibili alla dollarizzazione digitale. Lo stesso vale per i Paesi più piccoli in quanto non forniscono la stessa scala di esternalità di rete che le grandi realtà possono offrire. In altre parole, anche le economie con valute stabili potrebbero essere digitalmente dollarizzate se i loro cittadini si trovassero spesso a dover effettuare transazioni con gli utenti di una piattaforma digitale con la sua stessa valuta. Man mano che l'importanza dei servizi forniti digitalmente aumenta, e le reti sociali si intrecciano sempre più con i modi in cui le persone scambiano valore, l'influenza delle grandi valute digitali nelle economie più piccole crescerà.

1.3.3 Una Valuta Sintetica Internazionale

La prospettiva della dollarizzazione digitale crea la possibilità che una valuta digitale sintetica, sostenuta da una varietà di valute ufficiali, possa internazionalizzarsi. L'ascesa di una valuta sintetica internazionale, come Libra, ha profonde implicazioni

macroeconomiche. Negli ultimi decenni, le relazioni internazionali hanno creato una scarsità di beni sicuri in dollari e grandi ricadute transfrontaliere della politica monetaria statunitense attraverso il "ciclo finanziario globale" (*Global Financial Cycle*, GFC). Entrambe queste forze hanno, a loro volta, contribuito a tassi d'interesse stabilmente bassi.

Una valuta internazionale sintetica, collegata a diverse unità di conto, potrebbe giocare un ruolo nel rimediare alla carenza di beni sicuri, poiché il valore del debito denominato in più valute ufficiali fluttuerebbe insieme al valore della valuta sintetica. Tuttavia, nessuna singola valuta ufficiale sarebbe perfettamente sicura, il che significa che gli emittenti di debito denominato nella valuta sintetica possono assumere il rischio di cambio se le loro attività sono denominate nella valuta locale.

Se il commercio internazionale fosse scambiato nell'unità di conto della valuta sintetica, si ridurrebbero anche le correlazioni globali nei flussi commerciali. Attualmente, i prezzi del commercio internazionale sono espressi in dollari, quindi gli shock e la politica monetaria degli Stati Uniti hanno effetti critici nello stimolare o ostacolare il commercio internazionale. In un mondo con una valuta sintetica, tali shock del dollaro creerebbero minori deviazioni dall'efficienza nel commercio. Una valuta sintetica creerebbe, naturalmente, ricadute da shock alle altre valute sottostanti, ma nella misura in cui i Paesi affrontano shock idiosincratici, la diversificazione potrebbe smorzare tali ricadute.

1.4 La Competizione tra Denaro Pubblico e Privato

In un mondo economico costituito da valute digitali, la politica dovrà affrontare una varietà di problemi impegnativi e differenziati in confronto all'economia tradizionale. Il denaro non sarà più un mero mezzo di scambio come in passato: ogni valuta digitale sarà accompagnata da una serie di servizi di dati e sarà associata a un insieme di attività economiche. Il sistema tradizionale di intermediazione potrà essere capovolto, con i fornitori di pagamenti posti al di sopra, gerarchicamente, alle filiali che forniscono intermediazione e altri servizi finanziari. In questa sezione viene discussa la competizione tra denaro pubblico e privato.

1.4.1 Denaro Pubblico e Privato

L’avvento delle valute digitali solleva nuovi quesiti riguardanti la concorrenza tra denaro privato e denaro pubblico. Storicamente, una ragione per cui i governi hanno cercato di regolare il denaro privato è stato quello di frenare l'instabilità finanziaria. Infatti, una mancata regolamentazione del denaro privato nella società occidentale è spesso vista come una grande problematica. Il sistema di banche libere è un sistema monetario nel quale l'emissione di moneta è lasciata alle singole banche private e all’interno del quale non esistono monete a corso legale e banche centrali. Negli Stati Uniti tale struttura è durata meno di 30 anni. L'unico caso in cui fu raggiunta una certa stabilità fu in Scozia, dove il sistema di banche libere prevalse per poco più di un secolo. Tuttavia, ci sono alcuni episodi in cui le valute private non regolamentate hanno avuto successo e sono persino sopravvissute alla valuta ufficiale del governo. Uno degli esempi più interessanti è quello del “swiss dinar” in Iraq, che ha continuato a circolare nella parte curda del paese anche dopo che il governo l'aveva rinnegata. Tale episodio ha fornito ulteriori prove sull'importanza dell'appoggio del governo, poiché il dinaro svizzero iniziò ad apprezzarsi quando sembrò che gli Stati Uniti avrebbero deposto Saddam Hussein e riconosciuto quindi ufficialmente il vecchio dinaro svizzero. Negli ultimi anni, le criptovalute, come il Bitcoin, hanno nuovamente sollevato la questione riguardante il fatto se il denaro emesso privatamente e quindi non supportato da alcuna istituzione ufficiale, possa avere successo. Sebbene oggi le criptovalute siano ancora poco efficaci come riserva di valore e mezzo di scambio, tuttavia queste trovano utilità come valute veicolo in transazioni internazionali.

Gli economisti spesso attribuiscono il fallimento delle valute private non garantite da un’autorità centrale alla mancanza di un’ancora fiscale come discusso nel Paragrafo 1.1.1. Una valuta privata non garantita è posta davanti ad un problema di instabilità dinamica: può perdere improvvisamente il suo valore come mezzo di scambio se gli individui credono che in futuro gli altri non l'accetteranno. Questa instabilità può portare a iperinflazioni in seguito alle quali la moneta si sfalda. Un governo, d'altra parte, può garantire il valore della moneta attraverso la tassazione. Lo stesso governo può raccogliere risorse reali attraverso la tassazione, e offrirsi di acquistare (anche in piccola quantità) moneta usando quelle risorse, ponendo un limite rigido al livello dei prezzi. Se

il governo dichiara la sua moneta a corso legale, questa politica esclude la possibilità di un'inflazione sempre più rapida. Allo stesso modo, il potere di tassazione del governo può essere usato per acquistare riserve estere. Quindi, le valute sostenute dai governi non hanno lo stesso problema di instabilità tipico delle valute private. La volontà del governo di accettare la propria valuta come pagamento rafforza ulteriormente una valuta emessa pubblicamente. La teoria fiscale del livello dei prezzi suggerisce che la capacità di pagare le tasse in una valuta emessa dal governo pone un limite inferiore al valore della valuta. Nel momento in cui ci si aspetta che il governo esegua surplus primari, il settore privato deve risparmiare in debito pubblico poiché le loro tasse superano il reddito che si aspettano di ricevere dalla spesa pubblica; quindi, il valore della moneta in circolazione non può essere inferiore al valore attuale dei surplus del governo.

Tuttavia, le argomentazioni sul perché il denaro privato non supportato abbia fallito in passato possono essere meno rilevanti oggi perché il denaro pubblico è spesso un sostituto poco adatto per le moderne valute digitali, ragion per cui queste possono essere molto meno suscettibili di fallimento. Per esempio, le criptovalute possono essere usate per condurre grandi transazioni internazionali in un modo che non sarebbe possibile con il denaro ordinario. Alcuni soldi emessi privatamente inoltre garantiscono l'accesso ad accordi di pagamento automatizzati ("contratti intelligenti") o mercati di previsione che sono specifici di una particolare piattaforma. Ancora più importante, il proprietario di una piattaforma potrebbe effettivamente imporre che la sua moneta sia l'unica forma di valuta che possa essere utilizzata su quella piattaforma a meno che il governo non intervenga.

La prospettiva di valute indipendenti solleva anche preoccupazioni per la politica monetaria. La politica monetaria è solitamente considerata una funzione pubblica che gli emittenti privati condurrebbero in modo inefficiente. Il timore che un'entità, capace di condurre la propria politica monetaria, agisca a proprio favore è ciò che è alla base del "peccato originale" affrontato dai Paesi emergenti nei mercati del debito sovrano. I grandi emittenti privati di valuta digitale si troverebbero, allo stesso modo, ad affrontare la preoccupazione riguardante il fatto che, qualora gli fosse permesso di condurre liberamente la politica monetaria, questa sarebbe adattata per beneficiare l'azienda piuttosto che il pubblico. Allo stesso modo, la fornitura di liquidità è stata solitamente considerata come una funzione essenziale della banca centrale. In un sistema bancario

incentrato sulla valuta di una rete digitale, sarebbe necessario, probabilmente, che qualche entità sia in grado di fornire liquidità direttamente sulla rete, e non è affatto scontato che il proprietario della rete sia disposto a fornire la struttura ottimale di finanziamento. Queste preoccupazioni presentano un ulteriore motivo per l'applicazione di un regime di interoperabilità e convertibilità: la convertibilità vincolerebbe la politica monetaria degli emittenti, e l'interoperabilità con la valuta nazionale permetterebbe alla banca centrale di fornire liquidità.

1.4.2 L' Indipendenza Monetaria

Tradizionalmente, un importante quesito in macroeconomia riguarda il fatto di come un governo possa mantenere l'autorità monetaria quando è sfidato dalla prospettiva della dollarizzazione. Questa domanda è probabile che diventi ancora più rilevante con la possibilità della dollarizzazione digitale. Nelle economie moderne, non è presente, essenzialmente, alcuna interazione monetaria diretta tra il governo e i cittadini. Il denaro liquido rappresenta una piccola frazione del denaro in circolazione e la maggior parte dei consumatori detiene la maggior parte del proprio denaro sotto forma di depositi bancari. Il governo è in grado di esercitare una certa influenza sul pubblico influenzando i tassi di interesse ai quali le banche possono prendere e prestare denaro. Riesce in questo attraverso operazioni di mercato aperto, che cambiano i tassi di prestito interbancari, o può fissare direttamente il tasso di interesse sulle riserve e il tasso dello sportello di sconto. Qualora l'avvento di valute basate su piattaforme digitali alterasse la gerarchia finanziaria, il ruolo delle banche potrebbe risultare meno centrale. La scomparsa del contante ed il ruolo ridotto delle banche rappresentano serie minacce per l'indipendenza monetaria.

CAPITOLO 2
LE CRIPTOVALUTE E IL BITCOIN

La nascita delle criptovalute è spesso associata alla nascita del Bitcoin, dal momento che quest'ultimo rappresenta la valuta digitale per eccellenza. Ma è importante sottolineare che il Bitcoin non è stata la prima criptovaluta, bensì la prima ad avere successo. Tante altre criptovalute sono state sviluppate prima della più nota valuta digitale, fino al suo completo sviluppo e implementazione nel 2009.

Nel 1993 David Chaum creò il primo sistema di pagamento basato sull'utilizzo della moneta elettronica chiamato "eCash". Alla base del suo funzionamento risiedeva l'intento di scambiare denaro elettronico (diverso dall'utilizzo delle carte di credito) fornito da diverse banche affiliate al sistema che avevano il dovere di certificarne l'autenticità.

Successivamente, nel 1995, "eCash" divenne "DigiCash" il quale richiedeva l'utilizzo di un software da parte dell'utente per poter procedere alle transazioni. Uno dei requisiti preliminari per il corretto funzionamento di tale software consisteva nel possedere un conto corrente virtuale presso una delle banche affiliate, dotato di una chiave pubblica necessaria per la codifica della firma dell'acquirente. Il passaggio successivo consisteva nel possedere del denaro virtuale sul dispositivo su cui si utilizzava il software, per cui, si richiedeva all'utente di aver prelevato presso la banca di riferimento e aver trasferito il denaro dal conto al dispositivo. Capire il meccanismo di questo trasferimento è fondamentale poiché esso rappresenta non solo l'idea di Chaum, ma anche il concetto posto alla base delle criptovalute odierne.

Il prelievo non si configura tecnicamente come un semplice trasferimento di moneta virtuale tra la banca e il dispositivo dell'utente. Infatti, è il software che una volta

calcolato quante monete sono necessarie per ottenere la somma richiesta, crea tali monete assegnando ad ognuna di esse ed in modo casuale un numero di serie. Successivamente, il software spedisce queste monete alla banca, ed ognuna di esse viene inserita in una particolare busta che rappresenta il "fattore cecità"; la banca codifica i numeri ciechi con la propria chiave segreta applicando la firma digitale attraverso la busta e addebita la somma prelevata sul conto dell'utente.

Le monete sono dunque restituite all'utente che potrà rimuovere il fattore cecità introdotto senza alterare la firma della banca, in modo tale che i numeri di serie rappresentino ora la moneta digitale il cui valore è garantito dalla banca stessa.

Quando, in seguito, l'utente effettuerà delle spese, la banca accetterà le monete grazie alla firma digitale precedentemente da lei apposta anche se non sarà in grado di riconoscere chi ha effettuato il pagamento.

Il punto principale di questo meccanismo è la presenza e coesistenza di chiavi pubbliche e private, che permettevano alle transazioni elettroniche di non essere tracciabili dalle banche emittenti, dai governi o da terze entità.

Questo sistema di "Blind Signatures" impediva di poter accedere alle informazioni personali.

Nonostante l'intuizione visionaria di Chaum, DigiCash non ebbe la crescita sperata e in un'intervista del 1999 lo stesso Chaum dichiarò che il suo progetto entrò in un mercato dove la presenza dell'e-commerce non era ancora perfettamente integrato nel mondo di internet.

Nel 1998 DigiCash fallì facendo ricorso al Chapter 11 e nel 2002 l'azienda fu ceduta per singoli asset.

2.1 Origini del Bitcoin

Il Bitcoin è un metodo di pagamento online lanciato per la prima volta nel 2009 da Satoshi Nakamoto. Nonostante i molti sforzi fatti, l'identità di Satoshi rimane tuttora sconosciuta al pubblico e non è noto se sia una singola persona o un gruppo. In data 31 Ottobre 2008, Nakamoto pubblicò sul Web un documento contenente la sua invenzione intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (rif. [1]), descrivendo come

il Bitcoin si comporta esattamente come una moneta, per cui può essere scambiato (in questo caso sottoforma di stringa di codice) per ottenere in cambio un bene o un servizio. La criptovaluta inventata da Satoshi Nakamoto è fatta circolare utilizzando software open-source. Può essere scaricato da chiunque e il sistema funziona su una rete peer-to-peer decentralizzata e completamente distribuita. Ciò significa che ogni nodo o terminale di computer sono interconnessi tra di loro con i singoli componenti che possono lasciare e ricongiungersi alla rete a piacimento.

Il 9 gennaio 2009 venne rilasciato il primo client di Bitcoin e il 12 Gennaio avvenne la prima transazione, il cui risultato portò al cosiddetto "*genesis block*", ovvero il blocco iniziale della Blockchain del Bitcoin, generando 50 BTC.

Sebbene il Bitcoin sia una valuta digitale, lo si potrebbe assimilare metaforicamente al risultato finale di decadi di ricerca nel campo della crittografia, in particolar modo a studi riguardo il "*Merkle tree"*, le funzioni hash e le chiavi pubbliche e private. Tutte queste tecnologie sono state perfettamente convogliate e amalgamate per creare la prima valuta decentralizzata al mondo.

Il Bitcoin non rappresenta solo un asset digitale, ma lo si può considerare anche come un'elegante soluzione a due problematiche che per lungo tempo sono state oggetto di studi in campo informatico, ossia *il Problema dei Generali Bizantini* e *il Double-Spending*, che verranno discussi in seguito nei relativi paragrafi.

2.2 La Tecnologia delle Criptovalute: la Blockchain

Nella sua pubblicazione, Nakamoto descrisse il funzionamento del Bitcoin introducendo per la prima volta il concetto di blockchain.

Si può pensare alla blockchain come ad un *registro distribuito a rete paritetica* ("peer-to-peer distributed ledger") *crittograficamente sicuro, di tipo append-only, immutabile e modificabile solo tramite consenso o accordo tra le parti* ("peers") (rif. [3]).

La piena comprensione di tutti i concetti presentati nella definizione sopra riportata è di primaria importanza per capire i motivi per cui la blockchain risulta essere la chiave di volta per il successo delle criptovalute, e al tempo stesso uno strumento tecnologico primario utilizzato anche in molti altri ambiti.

La prima parola chiave della definizione di blockchain è il cosiddetto registro distribuito (distributed ledger), il quale sta ad indicare che la blockchain è del tutto assimilabile ad un registro ripartito tra tutti gli utenti del network, del quale ciascuno di essi ne possiede una copia completa.

Il registro distribuito si basa su un modello di architettura informatica noto come Peer-to-Peer (P2P) il cui funzionamento si fonda sul concetto di decentralizzazione del network. Non si è infatti in presenza di un server centrale che raggiunge i client (gli utenti), bensi' ogni utente agisce da server e al tempo stesso da client in modo da decentralizzare il sistema. Questa proprietà permette agli utenti di effettuare transazioni senza il coinvolgimento di intermediari terzi, come ad esempio una banca.

Asserire che la blockchain è crittograficamente sicura significa far riferimento al concetto di *crittografia asimmetrica* (o crittografia a chiave pubblica), la quale si basa sull'utilizzo di una chiave pubblica e una chiave privata per ogni utente nel network. Le transazioni in una blockchain avvengono grazie alla coesistenza di questi due requisiti, senza i quali non sarebbe possibile trasferire i beni. La chiave pubblica ("address") funge da "indirizzo" visibile e identifica ogni utente all'interno della blockchain. Ciascuno di essi è anche in possesso di una propria chiave privata che serve sia per autorizzare la transazione (per il mittente) sia per decriptarla (per il destinatario).

Per esempio, si ipotizzi per semplicità che nel network siano presenti solamente due utenti, A e B. Entrambi hanno a disposizione due chiavi, una pubblica e una privata. A vuole inviare un bitcoin a B e per farlo, si serve della chiave pubblica di B. A avvia e autorizza, attraverso la sua chiave privata, la transazione inviando un BTC a B. Da questo momento in poi, solo B è in grado di decriptare la transazione e ricevere il bitcoin, poiché solo lui è in possesso della sua chiave privata.

Altra caratteristica della blockchain è quella di essere append-only. Questa proprietà può essere spiegata in questo modo: i nuovi dati vengono aggiunti nella blockchain in modo sequenziale e, una volta inseriti, non possono essere più modificati se non in specifici casi molto particolari, come ad esempio rivendicando *il Diritto all'Oblio* ("Right to be forgotten") regolato negli articoli 17, 21 e 22 del *Regolamento Generale Della Protezione dei Dati* (GDPR). In ogni caso, situazioni simili sono da trattarsi separatamente e richiedono soluzioni tecniche ad hoc. Per questo motivo, è consuetudine considerare la blockchain come una struttura immutabile.

Alla fine, si trova la parte più delicata e critica della definizione, ovvero la caratteristica di essere modificabile solo tramite consenso o accordo tra le parti. Comprendere questo aspetto significa comprendere il potenziale della decentralizzazione. Secondo questa definizione, non vi è alcuna autorità centrale che ha il potere di modificare il registro, bensì ogni aggiornamento o variazione viene approvata solo dopo aver rispettato i criteri imposti dal protocollo della blockchain ed è aggiunta alla catena solo quando viene raggiunto un accordo tra tutti gli utenti del network. Esistono diversi algoritmi che facilitano il raggiungimento dell'accordo, assicurando che tutte le parti siano allineate riguardo lo stato finale dei dati contenuti nel network della blockchain.

2.2.1 La Blockchain nel Bitcoin

La struttura di una blockchain è molto simile a quella di alcune strutture informatiche quali la *lista concatenata* o l'*albero binario,* all'interno dei quali le informazioni sono collegate tra loro attraverso i puntatori, il cui ruolo è quello di contenere un riferimento ai vari elementi presenti nella lista.
La Figura 2.1 rappresenta lo schema di una blockchain e come questa si basi sull'utilizzo dei puntatori:

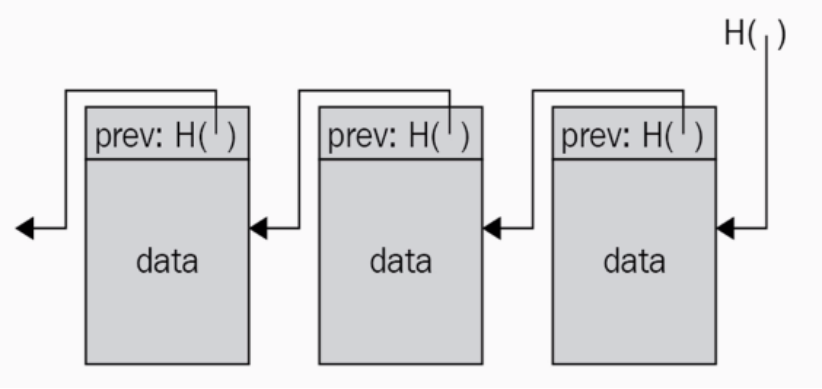

Figura 2.1 – Schematizzazione di una blockchain

Il principio di funzionamento della blockchain è analogo a quello delle strutture similari sopra menzionate, con la grande differenza che fa uso di puntatori "hash". Un puntatore hash esegue lo stesso compito di un puntatore normale, ovvero quello di indicare il luogo dove è immagazzinata l'informazione, ma con una peculiarità in più, ossia crittografare l'informazione a cui fa riferimento. Questa è la ragione per cui, sebbene sia affine ad

altre strutture, la blockchain risulta essere più resistente ai tentativi di manomissione e corruzione dei dati immagazzinati al suo interno.
L'applicazione pratica più famosa e di maggior successo della blockchain è senza dubbio il Bitcoin. La Tabella 2.1 mostra i componenti di ciascun blocco della catena del Bitcoin.

Tabella 2.1 – Componenti della blockchain del Bitcoin

Elemento	**Dimensione**	**Descrizione**
Dimensione del blocco	4 byte	Rappresenta la dimensione del blocco.
Block header	80 byte	Nel block header sono contenuti gli elementi analizzati di seguito separatamente.
Counter delle transazioni	Variabile	Questo elemento contiene il numero totale delle transazioni nel blocco. La dimensione varia tra 1 e 9 byte.
Transazioni	Variabile	Elenco di tutte le transazioni nel blocco.

Il block header, a sua volta, può essere decomposto in più parti che identificano il blocco stesso, come dettagliato nella seguente Tabella 2.2.

Tabella 2.2 – Componenti del block header

Elemento	**Dimensione**	**Descrizione**
Versione	4 byte	Il numero della versione del blocco indica quali set di regole devono essere seguite affinché il blocco risulti valido.
Hash del block header precedente	32 byte	Hash del block header precedente crittografato secondo l'algoritmo SHA-256.
Hash del Merkle root	32 byte	Hash del Merkle tree crittografato secondo l'algoritmo SHA-256 contenente tutte le transazioni del blocco.

Timestamp	4 byte	Il timestamp contiene un'approssimazione del tempo di creazione del blocco, scritto in linguaggio Unix. Per essere più corretti, corrisponde al tempo impiegato dal miner per codificare il blocco.
Complessità	4 byte	Indica una misura della complessità della rete.
Nonce	4 byte	Indica un numero che i miner cambiano frequentemente per produrre un hash valido per generare un blocco.

Tra gli elementi del block header, di particolare rilevanza è il Merkle tree (conosciuto anche come "binary hash tree"). Introdotto per la prima volta da Ralph Merkle e brevettato nel 1979, si tratta di una struttura utilizzata per verificare l'integrità di grandi ammontare di dati assicurando, in questo modo, che l'informazione contenuta nel blocco sia sicura e non abbia subito manomissione.
Nella Figura 2.2 viene mostrata la schematizzazione del Merkle tree.

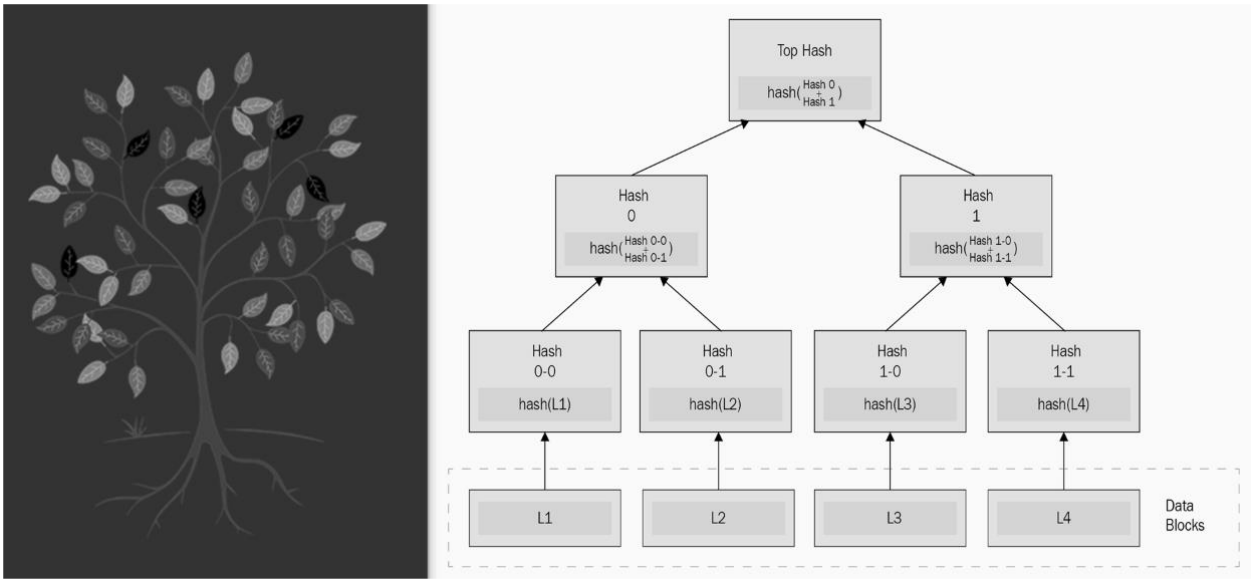

Figura 2.2 – Schematizzazione del Merkle tree

Come si evince, il Merkle tree è rappresentato come una struttura alla cui sommità troviamo il nodo radice, denominato “Top Hash” o “Merkle root”, da cui si diramano i nodi foglie dell’albero. Alla base troviamo i “data blocks”, ossia transazioni che sono state immagazzinate e codificate più volte. Codificando più volte i data blocks, si riescono a creare i nodi intermedi per risalire verso l’alto fino ad arrivare al Merkle root dell’albero. Con questa struttura, qualora si verificasse un cambiamento o un tentativo di manomissione, si è sempre in grado di capire in quale parte della catena tale evento possa essersi verificato. Ne consegue che il Merkle tree è una delle maggiori implementazioni della blockchain ed è la caratteristica che contribuisce in maggior modo alla sicurezza e all’integrità delle informazioni.

Le due tabelle sopra riportate aiutano a capire di cosa siano composti i blocchi e soprattutto quali siano gli elementi che li identificano. La seguente Figura 2.3, invece, aiuta a comprendere, con un livello di dettaglio più aggregato, come siano legati tra di loro i blocchi e, in questo modo, si riesce a capire il motivo per cui la caratteristica tipica di ogni blocco di fare riferimento al precedente è così importante a tal punto da rendere di fatto la blockchain immutabile a meno che non si modifichino tutti i blocchi della catena, operazione di fatto impossibile. L’unico blocco della catena che non possiede tale peculiarità è il primo blocco, noto come genesis block.

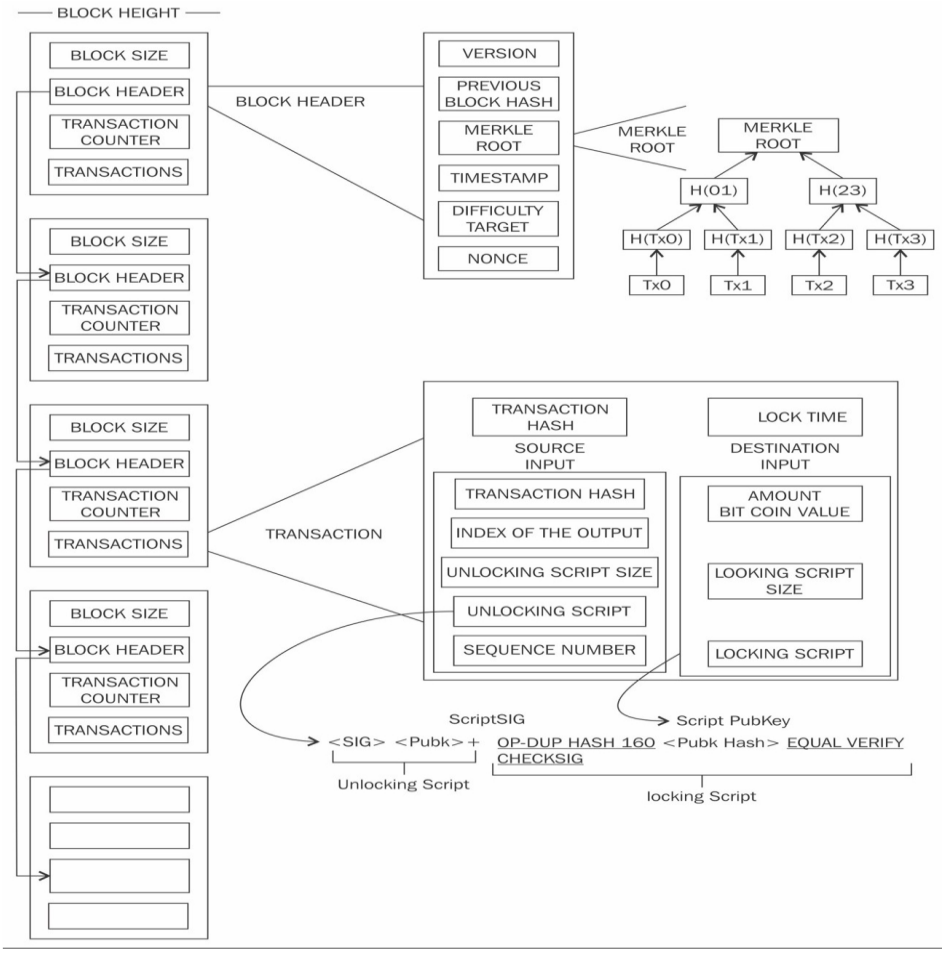

Figura 2.3 – Schema di alto livello della blockchain del Bitcoin

Nella parte sinistra della figura si trovano i blocchi ordinati dall'alto verso il basso. Ciascuno di essi contiene il block header, di cui si è discusso precedentemente, scomposto nei suoi componenti nel lato destro del diagramma. Nella parte bassa è raffigurata la suddivisione della struttura delle transazioni con gli elementi in essa contenuti.

2.2.2 Le Transazioni nella Blockchain del Bitcoin

Nell'ecosistema del Bitcoin, le transazioni non sono tutte uguali e non necessariamente riguardano il trasferimento di moneta tra due utenti del network. Infatti, la blockchain viene impiegata per scambiare molti altri tipi di asset digitali. Tuttavia,

indipendentemente dalla loro natura, ogni transazione è composta da almeno un dato di input e uno di output.

Il ciclo di vita di una transazione può essere schematizzato nel diagramma mostrato in Figura **2.4** e si può articolare in più punti:

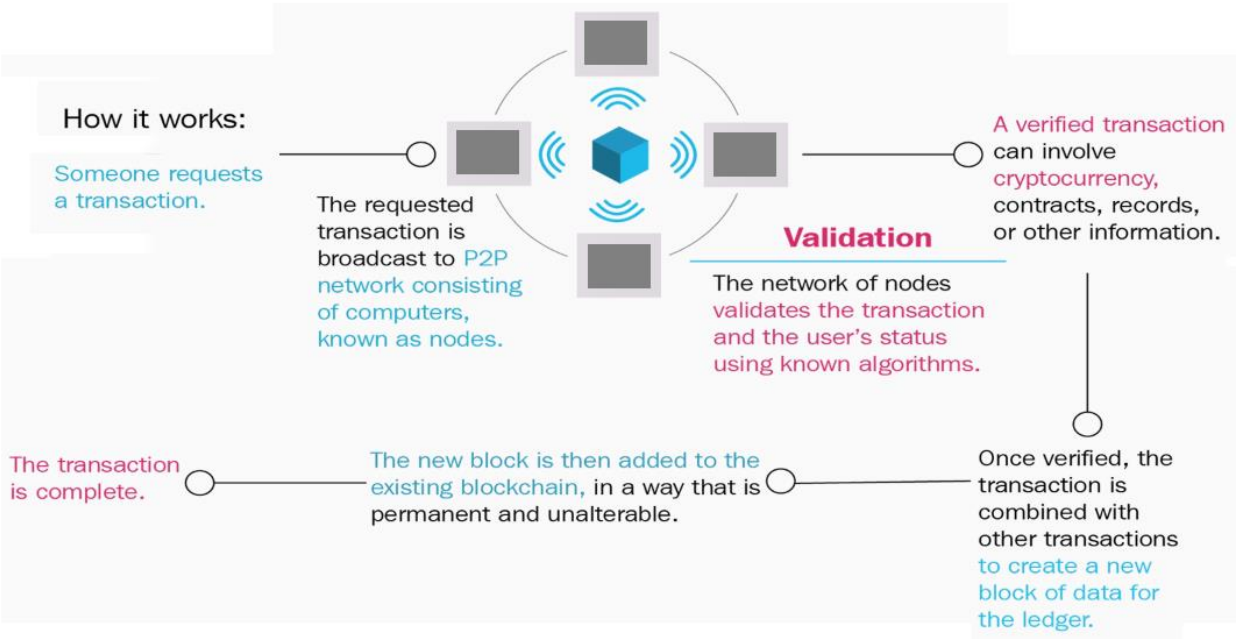

Figura 2.4 – Ciclo di vita di una transazione in una blockchain

1) Un utente avvia la transazione attraverso l'utilizzo di un software (può essere un'applicazione mobile o per computer).
2) Il software appone la firma sulla transazione utilizzando la chiave privata del mittente.
3) La transazione viene propagata verso il network del Bitcoin attraverso un algoritmo di propagazione.
4) I nodi del network, i cosiddetti "*miners*", approvano e aggiungono la transazione nel nuovo blocco che verrà creato successivamente. Tuttavia, poco prima di essere aggiunta, la transazione staziona in una memoria di buffer speciale chiamata "*transaction pool*".
5) Il mining (processo mediante il quale la blockchain viene resa sicura) inizia e vengono generate nuove unità di moneta per i miners stessi come ricompensa per

aver concesso al network risorse computazionali per poter approvare la transazione.

6) Non appena un miner risolve un "PoW" (*Proof of Work*), il processo di mining termina e il nuovo blocco appena creato viene trasmesso all'intero network.
7) I nodi verificano il nuovo blocco e lo propagano ulteriormente, in modo tale che il processo di validazione possa iniziare.
8) A questo punto, le notifiche di conferma vengono inviate al software del destinatario e, approssimativamente dopo tre "conferme", la transazione viene considerata ultimata e convalidata. Il numero di conferme può variare da tre a sei, ma è puramente convenzionale, tant'è che la transazione può essere considerata terminata anche solo dopo la prima conferma. La *ratio* alla base di questa attesa trova argomentazione nel fatto che, dopo tre conferme, la probabilità che si verifichi il fenomeno del double-spending è pressoché nulla.

Nel punto 5) si è specificato che i miner vengono remunerati per le risorse offerte alla collettività, e sono loro stessi che determinano il costo (per loro definisce di fatto un guadagno) della transazione. Tale costo dipende dalla dimensione e dal peso della transazione ed è calcolato come differenza tra la somma degli input e la somma degli output. In termini di formula possiamo esprimere il costo come:

$$Costo = \sum(input) - \sum(output)$$

Il costo viene usato come incentivo per incoraggiare i miner a processare le transazioni che si susseguono e ad aggiungerle ai blocchi. Tutte le transazioni convergono nella transaction pool, chiamata anche memory pool, che ha lo scopo di gestire una lista temporanea di tutte quelle transazioni che non sono ancora state convalidate. Da qui, i miner possono prendere in carico le diverse transazioni secondo il loro ordine di priorità. È intuitivo comprendere che le transazioni che portano un maggior guadagno verranno processate per prime. Tuttavia, non sempre le transazioni generano ricavi per i miner, poiché il valore delle ricompense non è fissato dal protocollo del Bitcoin ed è possibile che tale valore sia anche nullo. Ciò nonostante, oggigiorno ogni transazione determina un guadagno, seppur minimo, per il miner, in considerazione dell'alto volume di dati processati e dell'elevata competitività della rete del Bitcoin.

Una delle fasi cruciali del ciclo di vita di una transazione è la fase di verifica, la quale viene svolta dai vari nodi del network e prevede più passaggi che si possono articolare come segue:

1) Verifica che la sintassi e la struttura dei dati della transazione siano conformi alle regole previste dal protocollo del Bitcoin
2) Verifica che nessun input e output siano valori vuoti
3) Controllo che la dimensione in byte sia minore della massima dimensione consentita del blocco
4) Verifica che l'output sia compreso nel range previsto (da 0 a 21 milioni di BTC).
5) Tutti gli input devono avere un riferimento specifico ad un output precedente, fatta eccezione per la prima transazione
6) Verifica che la dimensione della transazione sia almeno pari a 100 byte, pena l'invalidità della stessa
7) Negare le transazioni non-standard: una transazione viene negata se l'output generato per ogni input esiste in un'altra transazione nella pool
8) Negare la transazione nel caso in cui il costo sia troppo piccolo per far in modo che la transazione venga processata.

2.2.3 Il Mining

Il mining è il processo al termine del quale i nuovi blocchi generati vengono aggiunti alla blockchain. I blocchi contengono transazioni verificate e validate dai nodi del network attraverso il processo di mining, e contribuiscono ad accrescere la catena del Bitcoin.
La dimensione attuale della blockchain del Bitcoin, di cui l'ultimo dato disponibile risale all'11 ottobre 2021, si assesta intorno a 350 GB, come evidenziato nella Figura 2.5.

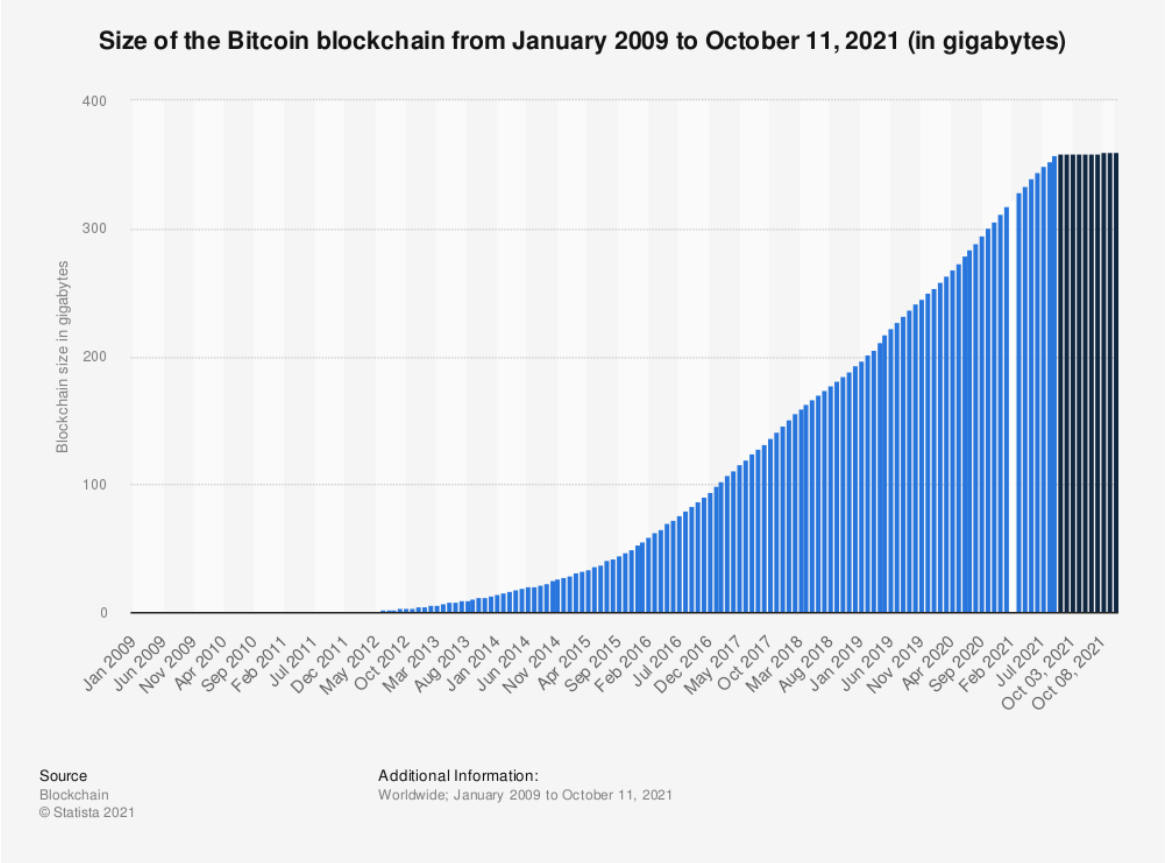

Figura 2.5 – Andamento della dimensione della blockchain del Bitcoin

Nuovi blocchi vengono aggiunti alla catena approssimativamente ogni 10 minuti e la complessità della rete viene ricalibrata dinamicamente ogni 2016 blocchi per mantenere una condizione adeguata in tutta la blockchain.
La complessità della blockchain può essere calcolata con la seguente equazione:

$$Target = Previuos\ target * \frac{Time}{2016} * 10$$

dove *Target* è sinonimo di complessità; *Previous target* è la complessità precedente e *Time* è il tempo speso per generare 2016 blocchi.
La complessità del network indica sostanzialmente quanto sia complicato e dispendioso per i miner riuscire a generare un nuovo blocco. In altri termini, indica quanto sia

complesso risolvere l' "*hashing puzzle"* (o Proof of Work, PoW), che verrà discusso in seguito.

Una volta che un nodo si aggiunge alla rete del Bitcoin, questo incorre in alcuni task necessari con cui ogni miner deve interfacciarsi:

1) Sincronizzarsi con il network: il miner scarica la blockchain richiedendo lo storico dei blocchi che la compongono
2) Validare le transazioni: le transazioni trasmesse alla rete devono essere validate dai nodi verificando e convalidando firme e output
3) Validare i blocchi: i miner possono validare i blocchi dimostrando che questi rispettino le regole imposte dal protocollo
4) Generare nuovi blocchi: i miner generano nuovi blocchi combinando le diverse transazioni che ricevono dal network
5) Risolvere i Proof of Work: questo task è il cuore dell'intero processo ed il motivo per cui i miner sono essenziali. Il block header di ogni blocco contiene un nonce di 32 bit e ai miners viene richiesto di trovare un nuovo valore finché l'hash risultante sia minore della complessità attuale della rete
6) Ottenere le ricompense: quando un miner risolve un hash puzzle (PoW), la soluzione viene immediatamente trasmessa al network, permettendo agli altri nodi di verificarla e di accettare il blocco.

Da quanto detto finora emerge che un fattore di fondamentale importanza che fa da comun denominatore a tutto il processo di mining è il Proof of Work. Il PoW consiste essenzialmente in un problema da risolvere, attraverso l'utilizzo di risorse più o meno ingenti a seconda della prova, al fine di generare un blocco valido da aggiungere alla blockchain. Il PoW si basa sulla scelta casuale di un nodo ogni volta che un nuovo blocco deve essere creato. In questo modello, i nodi "competono" tra di loro per poter essere designati alla risoluzione del problema in proporzione con la loro capacità computazionale. La seguente equazione riassume i requisiti del PoW nel bitcoin:

$$H\,(\,N\,||P_{hash}\,||\,Tx\,||\,Tx\,||\,\ldots Tx)\;<\;Target$$

Dove *N* è un nonce, P_{hash} è un hash del blocco precedente, *Tx* rappresenta le transazioni nel blocco e *Target* è la complessità del network. L'equazione è un vincolo la cui

soluzione è trovare un hash, dipendente dalla combinazione dei fattori precedentemente descritti, minore dell'hash target.

Seppur non molto raffinato, l'unico modo per soddisfare tale vincolo è il cosiddetto *trial and error*, ossia l'applicare più volte lo stesso metodo finché un determinato pattern non viene trovato dal miner.

Il processo di mining può essere schematizzato come mostrato nella

Figura **2.6**.

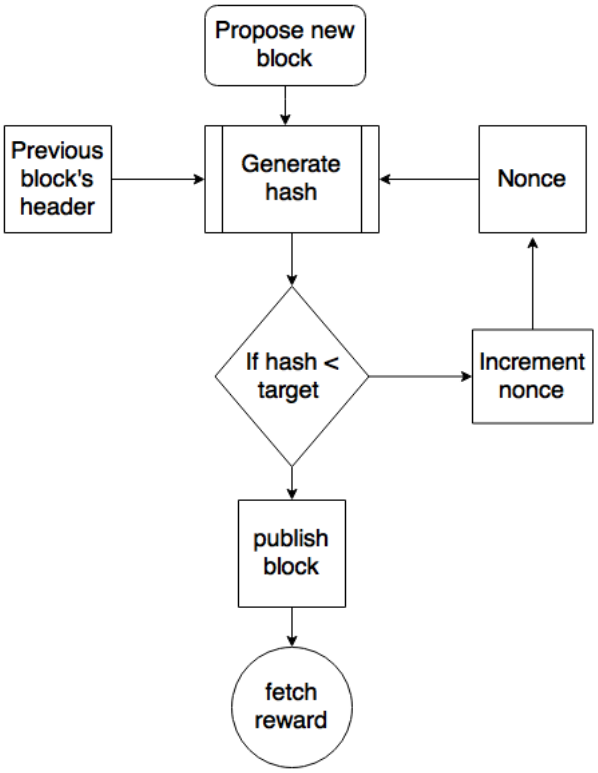

Figura 2.6 – Schematizzazione del processo di mining

La difficoltà del mining aumenta con il tempo e aumenta all'aumentare della complessità del network. L'andamento è mostrato nel grafico in Figura 2.7.

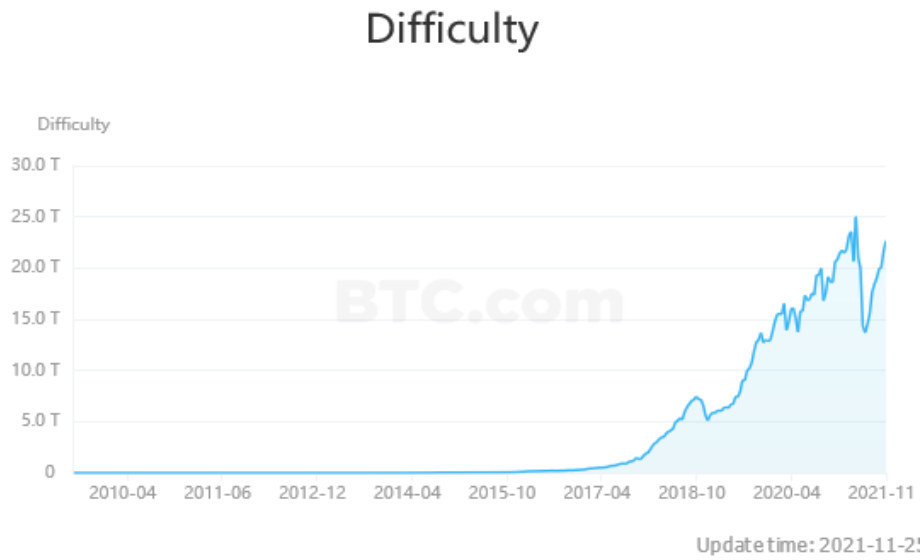

Figura 2.7 – Andamento della difficolta' del mining

La ragione per cui il processo di mining diviene sempre più complesso risiede nel fatto che nella catena del Bitcoin è necessario generare un blocco ogni 10 minuti circa. Questo vincolo ha come conseguenza il fatto che la difficoltà verrà aumentata se i blocchi verranno generati in meno di 10 minuti, mentre verrà diminuita se il tempo di creazione dei blocchi supererà i 10 minuti. La difficoltà viene aggiornata ogni 2016 blocchi (circa due settimane).

Un fattore strettamente correlato alla complessità della rete è il cosiddetto *hash rate*, ossia il tasso di calcolo degli hash al secondo. In altre parole, è la velocità con cui i miner riescono a calcolare gli hash per riuscire a generare un blocco. Il grafico mostrato nella Figura 2.8 mostra come attualmente l'hash rate sia approssimativamente 159 Exa hash/s, vale a dire che in 1 secondo, i miner sono in grado di generare più di $159 * 10^{18}$ hash.

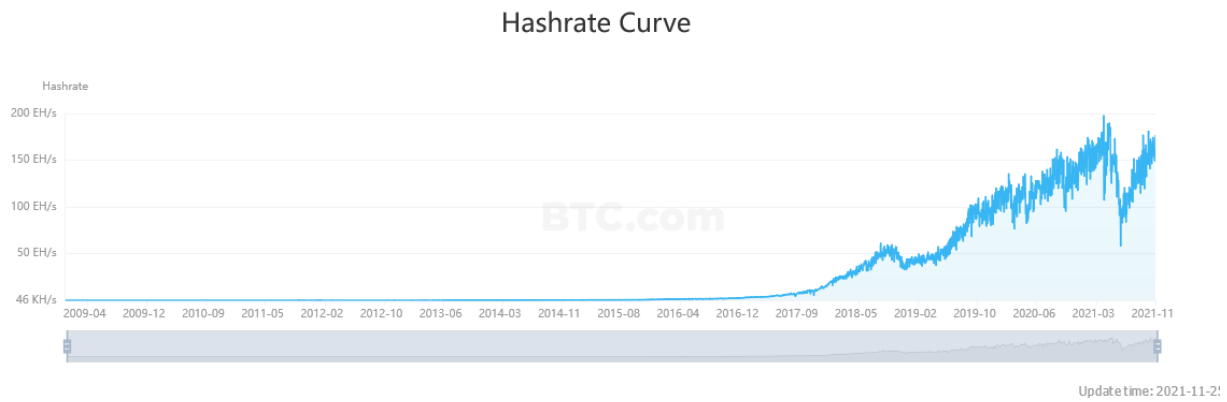

Figura 2.8 – Andamento dell'hash rate

2.3 Il Bitcoin e il problema dei Generali Bizantini

Il problema dei Generali Bizantini è un problema informatico che consiste nel trovare un accordo comunicando tramite messaggi tra le diverse componenti della rete che Bitcoin ha elegantemente risolto. Si tratta di un argomento di studio ben noto nel campo dei sistemi distribuiti ed è stato teorizzato nel 1982 dai matematici Leslie Lamport, Marshall Pease e Robert Shostak, i quali hanno creato la metafora dei generali (rif. [30]).
La blockchain di Bitcoin è stata creata con l'obiettivo di eliminare la fiducia verso terze parti durante una transazione. L'obiettivo è far sì che tutti siano d'accordo sull'ordine cronologico delle transazioni e quindi è fondamentale introdurre un algoritmo di consenso, che permetta ai vari attori della rete di mettersi d'accordo.

2.3.1 La Metafora

Diversi generali stanno per attaccare una città nemica durante un assedio. Si trovano in diverse aree strategiche e possono comunicare solo tramite messaggeri per coordinare l'attacco decisivo. Tuttavia, è altamente probabile, o addirittura certo, che tra questi messaggeri vi siano dei traditori che portano messaggi che contraddicono la strategia dell'esercito. Il problema, quindi, sta nella capacità di portare a termine l'attacco in modo efficace nonostante il rischio di tradimento. Questo è noto come consenso decentralizzato.
Nella migliore delle ipotesi, il messaggio che arriverà sarà coordinato: attacco o ritirata; oppure, come sembrerebbe più logico, il messaggio non sarà coordinato e quindi arriveranno entrambi gli ordini: attacco e ritirata. Questo concetto e' schematizzato nella Figura 2.9.

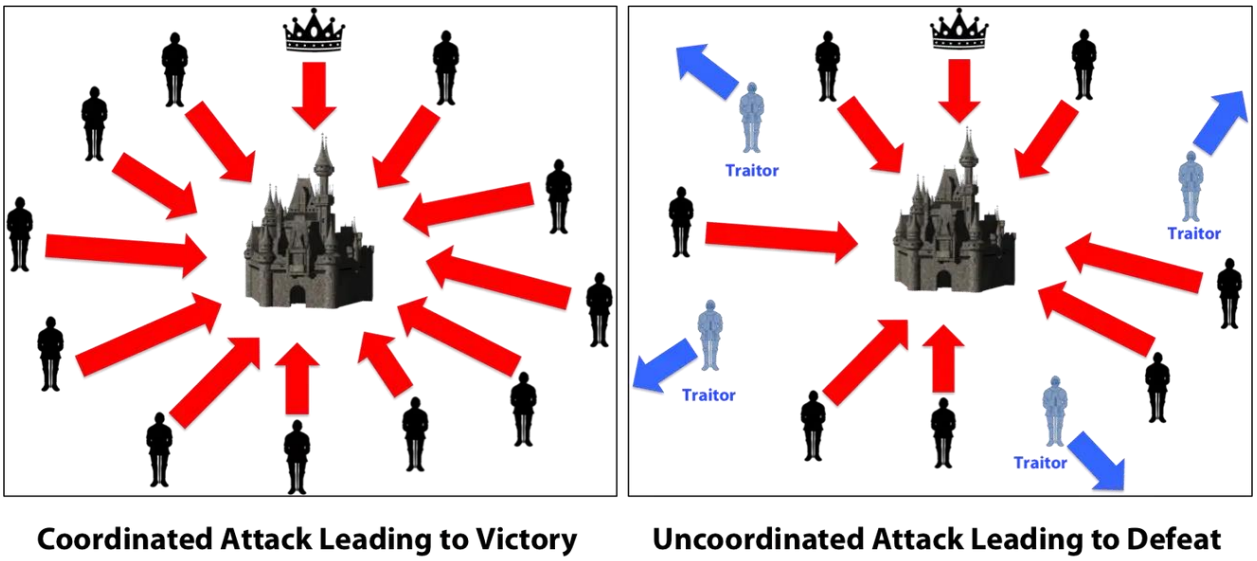

Figura 2.9 – Il problema dei Generali Bizantini

Il problema affrontato dai generali bizantini è lo stesso che condiziona i sistemi informatici distribuiti. Come raggiungere un consenso su una rete distribuita in cui alcuni nodi potrebbero essere mal funzionanti o volontariamente corrotti?

2.3.2 Il Problema dei Generali Bizantini nel caso di Bitcoin

Nel caso specifico di Bitcoin, il sistema deve essere in grado di mantenere la propria affidabilità nel caso in cui una minoranza di componenti invii informazioni errate o dannose per eludere il double-spending. Questo problema è molto difficile da risolvere. Tuttavia, Satoshi Nakamoto, con la blockchain di Bitcoin, ha offerto una soluzione pratica e funzionale combinando crittografia asimmetrica, sistemi peer-to-peer e Proof of Work, garantendo che tutti i partecipanti alla rete possano concordare e condividere in modo rapido e sicuro ogni messaggio trasmesso.

Nakamoto spiega come la catena Proof of Work offra una soluzione al problema dei Generali Bizantini e mostra come un certo numero di generali pronti ad attaccare debbano coordinarsi nel momento in cui viene lanciato l'attacco. Non è importante quale momento scegliere in particolare, ma è fondamentale che l'attacco avvenga in maniera sincronizzata.

Si è deciso che una volta stabilito l'orario dell'attacco da parte di uno dei generali, questo sarà considerato valido per tutti. Ma poiché la rete non è istantanea, è possibile che due generali annuncino contemporaneamente due tempi diversi per l'attacco con il risultato che alcuni riceveranno il primo annuncio e altri il secondo.
Questo conflitto viene risolto utilizzando la catena Proof of Work. Quando un generale riceve un messaggio deve risolvere un problema estremamente difficile. Il primo che lo risolve lo comunica agli altri partecipanti. Se qualcuno era al lavoro su un tempo di attacco diverso, dovrà sostituirlo con quello appena ricevuto, perché questa catena è la più lunga e quindi considerata valida.

2.3.3 Il Ruolo della Blockchain

La blockchain, quindi, garantisce che un insieme di nodi appartenenti alla stessa rete, lavorino insieme, gestendo la rete in modo sincrono ed efficace. La soluzione di Nakamoto è innovativa ma per esserlo richiede un certo consumo di energia e introduce un necessario ritardo tra la generazione di due blocchi, conseguenza quest'ultima di un sistema trustless funzionale e sicuro, a cui si sta rimediando sviluppando nuovi tipi di algoritmi di consenso.

2.4 Il Bitcoin e il Problema del Double-Spending

I documenti digitali possono essere copiati liberamente per cui il sistema deve impedire ai possessori di Bitcoin di trasferire il denaro digitale a due destinatari diversi. In questo senso, il Bitcoin è rivoluzionario perché risolve il problema del double-spending senza bisogno di un terzo intermediario.
In informatica, il problema del double-spending si riferisce al fatto che il denaro digitale potrebbe essere facilmente speso più di una volta. Si immagini la situazione in cui il denaro digitale è un semplice file informatico, proprio come un documento digitale. Anna potrebbe inviare $10 a Roberto inviandogli un file e può farlo facilmente con una e-mail. Tuttavia, l'invio di un file invia effettivamente una copia del file e non elimina il file originale dal computer. Quando Anna allega il file con il denaro in un'e-mail a Roberto, conserva ancora una copia del file anche dopo averlo inviato e quindi speso. Senza un

terzo intermediario di fiducia per garantire il contrario, Anna potrebbe facilmente inviare lo stesso denaro ad un'altra persona, per esempio Carlo.

Bitcoin risolve il problema del double-spending mantenendo un registro dei saldi. Invece di fare affidamento su un'unica terza parte fidata per gestire questo libro mastro, Bitcoin decentralizza questa responsabilità sull'intera rete. Infatti, la rete Bitcoin tiene costantemente traccia dei saldi in un registro pubblico chiamato blockchain.

La blockchain è un registro, pubblicamente accessibile, di tutte le transazioni mai elaborate, che consente a chiunque di utilizzare software Bitcoin per verificare la validità di una transazione. I trasferimenti di Bitcoin, o transazioni, vengono trasmessi all'intera rete e sono inclusi nella blockchain solo previo positiva verifica, in modo che i Bitcoin spesi non possano essere spesi di nuovo. Le nuove transazioni vengono verificate rispetto alla blockchain per assicurarsi che i Bitcoin non siano già stati spesi, risolvendo così il problema del double-spending.

Bitcoin utilizza ampiamente la crittografia a chiave pubblica per risolvere il problema del double-spending. Nella crittografia a chiave pubblica, ogni transazione ha una firma digitale e contiene un hash che consente un facile rilevamento della manomissione come evidenziato nelle Figura 2.10 e Figura 2.11.


```
{

"hash":"e9a66845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b8
0c1d",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":225,
  "in":[
    {
      "prev_out":{

"hash":"f4515fed3dc4a19b90a317b9840c243bac26114cf637522373a7d486b372
600b",
        "n":0
      },

"scriptSig":"3046022100bb1ad26df930a51cce110cf44f7a48c3c561fd977500b
1ae5d6b6fd13d0b3f4a022100c5b42951acedff14abba2736fd574bdb465f3e6f8da
12e2c5303954aca7f78f301
04a7135bfe824c97ecc01ec7d7e336185c81e2aa2c41ab175407c09484ce9694b449
53fcb751206564a9c24dd094d42fdbfdd5aad3e063ce6af4cfaaea4ea14fbb"
    }
  ],
  "out":[
    {
      "value":"0.01000000",
      "scriptPubKey":"OP_DUP                                OP_HASH160
39aa3d569e06a1d7926dc4be1193c99bf2eb9ee0 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```


Figura 2.10 – Esempio di transazione di Bitcoin

General information about this transaction		
Hash	e9a66845e05d5abc0ad04ec80f774a7e585c6e8db975962d069a522137b80c1d	The hash for this transaction
Block	100000 (2010-12-29 11:57:43)	Obtained from examining the block on the blockchain where this transaction was found
Version	1	Bitcoin software version
Size	225	The filesize in bytes of the transaction is recorded in the transaction data itself
Input from		
Previous output	f4515fed3dc4a19b90a317b9840c243bac26114cf637522373a7d486b372600b	The truncated hash of the previous transaction which provides the bitcoins to be sent for this transaction
Previous amount	0.01	The amount in the previous transaction which provides the bitcoins to be sent for this transaction
Public address	1JxDJCyWNakZ5kECKdCU9Zka6mh34mZ7B2	The public address of the sender, obtained from examining the blockchain
Signature	3046022100bb1ad26df930a51cce110cf44f7a48c3c561fd977500b1ae5d6b6fd13d0b3f4a022100c5b42951acedff14abba2736fd574bdb465f3e6f8da12e2c5303954aca7f78f30104a7135bfe824c97ecc01ec7d7e336185c81e2aa2c41ab175407c09484ce9694b44953fcb751206564a9c24dd094d42fdbfdd5aad3e063ce6af4cfaaea4ea14fbb	The digital signature of the transaction, signed by the sender
Output to		
Index	0	"0" indicates the first recipient in the transaction; here this transaction only has one recipient
Amount	0.01	Amount sent to this user in this transaction
Public address	16FuTPaeRSPVxxCnwQmdyx2PQWxX6HWzhQ	The public address of the recipient, obtained from the scriptPubKey
Bitcoin address (scriptPubKey)	39aa3d569e06a1d7926dc4be1193c99bf2eb9ee0	A hash160 of the public address
Conditions	OP_DUP OP_HASH160 OP_EQUALVERIFY OP_CHECKSIG	Conditions to be met together with the scriptPubKey for the output bitcoins to be redeemed by the recipient

Figura 2.11 – Informazione associata alla transazione di Bitcoin

CAPITOLO 3
L'ANALISI TECNICA DELLE CRIPTOVALUTE

Le criptovalute sono un nuovo tipo di strumento finanziario che ha ricevuto un grande interesse dai media e dagli investitori in tempi recenti. Come detto precedentemente, la prima criptovaluta di successo è stata il Bitcoin, il cui valore non è basato su alcun bene tangibile oppure sull'economia di un paese, ma viene stimato sulla base della sicurezza di un algoritmo che traccia tutte le transazioni. L'uso potenziale di Bitcoin come mezzo di scambio è attraente a causa dei suoi bassi costi di transazione, il suo design peer-to-peer, globale e senza governo. Tuttavia, gli utenti potrebbero essere preoccupati dalla mancanza di fiducia nel sistema così come l'odierno scarso utilizzo di Bitcoin per effettuare transazioni. Il Bitcoin è stato concepito come un nuovo tipo di valuta piuttosto che un bene di investimento. Tuttavia, la Figura 3.1 mostra che il prezzo di Bitcoin e di altre criptovalute è aumentato sostanzialmente dal 2010 denotando come questi nuovi strumenti sono utilizzati principalmente come investimento speculativo piuttosto che una valuta alternativa o un mezzo di scambio. La questione che le criptovalute possano ritenersi un investimento è tuttora aperta. Gran parte delle critiche rivolte al Bitcoin sono basate sulla sua mancanza di valore intrinseco. Tuttavia, la letteratura accademica che esamina la dinamica dei prezzi di Bitcoin e di altre criptovalute è in aumento, con una serie di articoli che studiano le bolle nei mercati delle criptovalute, l'efficienza dei mercati di Bitcoin, le sue proprietà di copertura e la scoperta del prezzo all'interno degli scambi. Tuttavia, la letteratura finanziaria a riguardo è limitata poiché si tratta di attività finanziarie piuttosto nuove.

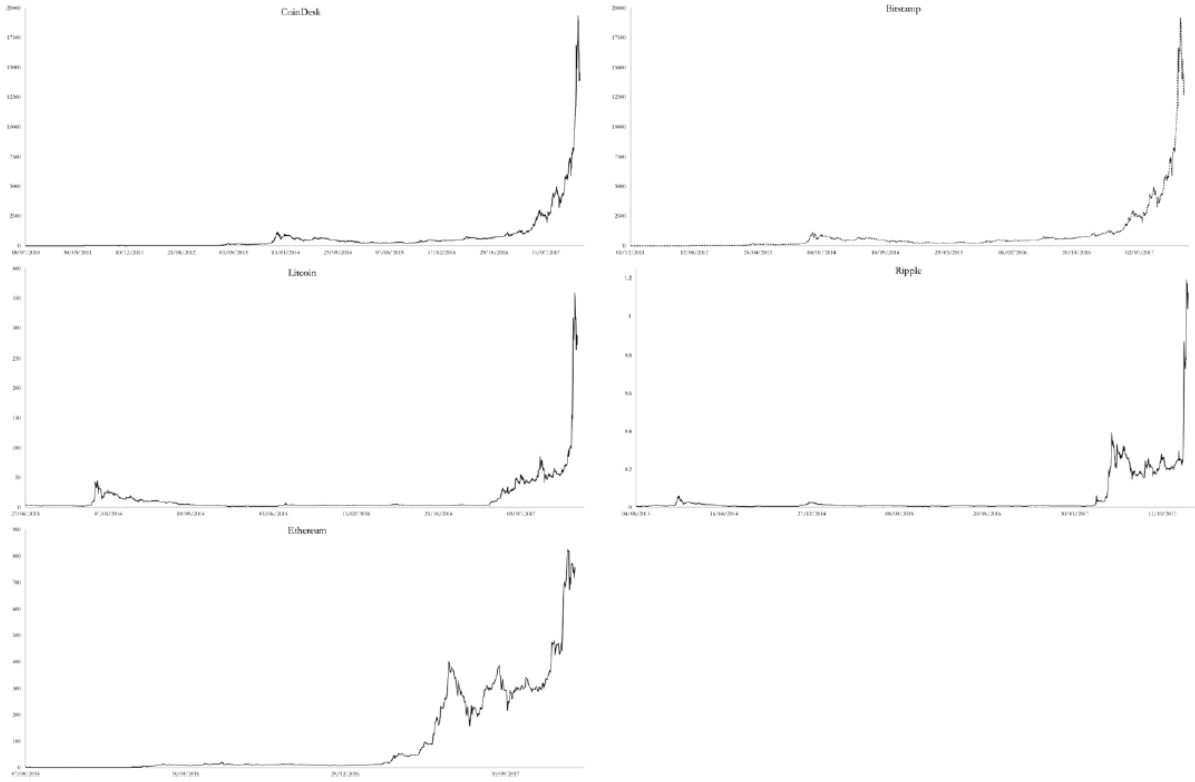

Figura 3.1 – Grafici che evidenziano l'aumento dei prezzi delle criptovalute prese in esame

Un'area che ha ricevuto una crescente attenzione nella letteratura sulle criptovalute è quella dei benefici di investire in questi asset. Kajtazi e Moro (rif. [15]) evidenziano gli effetti dell'aggiunta di Bitcoin a un portafoglio ottimale affidandosi all'approccio mean-CVaR per il portafoglio statunitense, europeo e cinese. Essi dimostrano che il Bitcoin migliora i rendimenti del portafoglio, soprattutto grazie all'aumento degli stessi piuttosto che da una minore volatilità, e che il Bitcoin ha un ruolo nella diversificazione del portafoglio. Recentemente, Platanakis e Urquhart (rif. [20]) esaminano il beneficio di includere il Bitcoin in otto popolari strategie di allocazione di asset in portafogli di azioni e obbligazioni. Essi trovano che l'inclusione della valuta digitale genera rendimenti corretti per il rischio (*risk-adjusted returns*) sostanzialmente più elevati, dove i risultati nei confronti di diverse stime, dell'incorporazione dei costi di transazione, dell'inclusione di un portafoglio di materie prime, di un indice alternativo per Bitcoin nonché di due ulteriori tecniche di ottimizzazione del portafoglio, sono robusti.

Si aggiunge alla letteratura uno studio del trading tecnico nei mercati delle criptovalute al fine di valutare se le regole del trading offrono potere predittivo e redditività in vari mercati di criptovalute. Il trading tecnico è di particolare interesse nei mercati delle

criptovalute per una serie di ragioni. L'approccio del trading ha un sostanziale successo documentato nei mercati delle valute convenzionali e, in una certa misura, in molti mercati di asset. Poiché i mercati delle criptovalute hanno avuto la tendenza a seguire forti pattern fin dal loro inizio, si ha qualche precedente che le regole tecniche di trading possano essere utili nei mercati delle criptovalute. Inoltre, la relativa mancanza di informazioni rilevanti per eseguire l'analisi fondamentale sulle criptovalute può elevare l'importanza relativa degli approcci tecnici. Questo perché le criptovalute non hanno fondamentali da esaminare e probabilmente non hanno valore intrinseco. Pertanto, gli investitori non possono studiare, per esempio, il bilancio o le previsioni dei dividendi per prevedere i prezzi futuri e, quindi, devono fare affidamento sul comportamento passato dei prezzi come segnale del comportamento futuro, che è il concetto fondamentale del trading tecnico.

L'unico articolo a disposizione che esamina il trading tecnico nei mercati delle criptovalute è a cura di Detzel e altri autori (rif. [12]), che mostrano che la regola della media mobile da 5 a 100 giorni, sia all'interno che all'esterno del campione, offre potere predittivo per gli investitori. Mostrano anche che le strategie di trading basate su queste regole generano alfa, utilità e indici di Sharpe sostanziali, riducendo significativamente la gravità dei *drawdown* (perdita) rispetto ad una posizione di *buy-and-hold* in Bitcoin. Tuttavia, questo documento esamina solo un tipo di regola di trading tecnico, mentre ci sono molti tipi diversi di regole con molte parametrizzazioni diverse. È stato dimostrato che gli investitori utilizzano una serie di diverse regole tecniche di trading e quindi, in questa sede, si approfondisce la letteratura studiando le più popolari. Inoltre, sebbene il mercato del Bitcoin sia il più grande, altri mercati di criptovalute hanno guadagnato un'attenzione che non dovrebbe essere ignorata poiché la crescita dell'interesse per le criptovalute diverse dal Bitcoin, è aumentata esponenzialmente negli ultimi anni.

In seguito, si studiano i dati giornalieri di quattro diverse criptovalute, ovvero Bitcoin, Litecoin, Ethereum e Ripple, per il periodo di dati più lungo disponibile per ogni singola criptovaluta. Si considera una gamma di cinque diverse classi di regole tecniche di trading, in cui si esaminano una serie di parametri diversi. Tuttavia, utilizzare poche regole può causare distorsioni nell'inferenza statistica dovuta al data mining. D'altra parte, usarne troppe può ridurre la potenza del test motivo per cui, si cerca un equilibrio e si seleziona una varietà abbastanza ampia di parametri ragionevoli all'interno delle

cinque famiglie di regole più popolari. Viene impiegata una gamma di metriche di performance per valutare i rendimenti del trading tecnico, compresa una serie di misure corrette per il rischio e i costi di *breakeven* (pareggio). Poiché si esaminano un certo numero di regole diverse, ci si trova di fronte alla reale possibilità di un *bias* (distorsione) da *data-snooping* (manipolazione artificiale dei dati o delle analisi per ottenere risultati significativi), dove il gran numero di ipotesi testate porta ad una probabilità piuttosto alta di rigettare l'ipotesi nulla di ogni regola di trading (commettendo un errore del I tipo). Per evitare questo problema, si calcolano prima i *p*-value individuali di ogni trading tecnico confrontando quello attuale con altri mille *p*-value stazionari "*bootstrapped*" (il bootstrap è una tecnica statistica di ricampionamento con reimmissione per approssimare la distribuzione campionaria di una statistica. Permette perciò di approssimare media e varianza di uno stimatore, costruire intervalli di confidenza e calcolare *p*-value di test quando, in particolare, non si conosce la distribuzione della statistica di interesse). Successivamente si utilizzano questi *p*-value individuali bootstrapped e si adottano una serie di approcci per testare ipotesi multiple, in particolare il *Family-Wise Error Rate* (FWER) e il *False Discovery Rate* (FDR). I risultati mostrano che le regole tecniche di trading offrono un potere predittivo nei mercati delle criptovalute, dove il rendimento medio annualizzato per ogni famiglia di regole tecniche è statisticamente significativo con un livello del 5% per ogni criptovaluta. Inoltre, i risultati sono robusti alle misure corrette per il rischio e i costi di transazione di breakeven della maggior parte delle regole esaminate sono sostanzialmente più alti di quelli riscontrati nei mercati delle criptovalute. Tenendo conto del data-snooping attraverso varie procedure di test di ipotesi multiple, gran parte delle regole di trading tecnico continua a registrare rendimenti significativi, indicando il potere predittivo e la redditività del trading tecnico nei mercati delle criptovalute. In quanto più rilevante, tuttavia, si dimostra come l'implementazione di regole di trading tecnico riduca significativamente i potenziali drawdown affrontati dalla strategia buy-and-hold e quindi protegga gli investitori dalle perdite associate ai mercati delle criptovalute. Infine, si evidenzia come il Bitcoin non offra alcun rendimento positivo nel periodo fuori campione, ma come le altre criptovalute offrano rendimenti positivi e indici di Sharpe e Sortino relativamente alti.

Il successo delle regole del trading tecnico nel generare profitti consistenti è stato sempre oggetto di dibattito nella letteratura accademica. È stato riscontrato che i professionisti

utilizzano ampiamente l'analisi tecnica, con Smith et al. (rif. [22]) che dimostrano che il 21,6% degli hedge fund utilizza l'analisi tecnica, mentre Menkhoff (rif. [18]) riferisce che l'analisi tecnica è diffusa nel mercato dei cambi. Tuttavia, la letteratura accademica ha esaminato dettagliatamente la performance dell'analisi tecnica poiché fornisce prove contro una delle teorie più rispettate in finanza, ossia l'ipotesi di un mercato efficiente. L'efficienza del mercato in forma debole afferma che tutte le informazioni di prezzo disponibili devono riflettersi nei prezzi dei titoli e quindi l'uso dell'analisi tecnica risulta superflua. Poiché il mercato dei cambi è quello in cui l'analisi tecnica è particolarmente utilizzata, gli studi sono stati abbondanti e hanno indicato a lungo opportunità di profitto. Questa letteratura mostra che semplici regole tecniche di trading sui tassi di cambio del dollaro hanno fornito 15 anni di rendimenti positivi, corretti per il rischio, durante gli anni '70 e '80 prima che questi rendimenti si estinguessero. In un'analisi completa, Hsu et al. (rif. [14]) effettuano uno studio su larga scala delle regole tecniche di trading nel mercato dei cambi per 45 anni in 30 mercati sviluppati e in via di sviluppo e trovano alcune prove di sostanziale prevedibilità ed eccesso di redditività in entrambi. Zarrabi et al. (rif. [25]) mostrano che dal 1994 al 2014, le regole tecniche di trading sono state redditizie in sei valute quotate in dollari statunitensi; tuttavia, la redditività non è stata costante.

Il mercato dei cambi non è l'unico mercato a riportare risultati significativi dall'impiego di regole tecniche di trading. Nei mercati azionari, Brock et al. (rif. [11]) mostrano che il trading tecnico fornisce una significativa prevedibilità su 90 anni per il *Dow Jones Industrial Average*, mentre Sullivan et al. (rif. [23]) e White (rif. [24]) mostrano che i risultati di Brock et al. non sono dovuti al data-snooping. Molti altri articoli hanno anche riportato risultati significativi per trading tecnico nei mercati azionari, come Shynkevich (rif. [26]), Han et al. (rif. [13]) e Neely et al. (rif. [19]). Ci sono anche prove di risultati significativi del trading tecnico nei mercati dei future delle materie prime, mercati spot delle materie prime, mercati obbligazionari e gli ETF sulle materie prime. Nonostante questi risultati, non c'è un chiaro consenso sulla prevedibilità delle regole di trading tecnico in letteratura, con molti articoli che indicano che le regole tecniche di trading non offrono alcun potere predittivo, specialmente se i costi di transazione vengono presi in considerazione.

In questo capitolo, si cerca di fornire uno studio su larga scala delle prestazioni del trading tecnico nelle criptovalute. Anche se la ricerca precedente si è concentrata su una vasta gamma di altre attività finanziarie, solo pochi articoli si concentrano sulle criptovalute ed in particolar modo sul Bitcoin, mentre in questa sede verranno prese in esame una serie di importanti valute digitali. Inoltre, verranno utilizzate una vasta gamma di regole di trading per fornire un'indagine approfondita delle prestazioni delle regole tecniche nei mercati delle criptovalute. Saranno presenti anche misure di performance corrette per il rischio e saranno calcolati i costi di transazione di breakeven. Successivamente, per evitare il problema dal data-snooping, verranno effettuati una serie di test di ipotesi multiple. Infine, verranno studiate le prestazioni nel campione e fuori dal campione di regole tecniche di trading nelle criptovalute per salvaguardarsi da qualsiasi problema di data mining. Il resto del capitolo è organizzato come segue: Il Paragrafo 3.1 discute il set di dati utilizzato in questo studio e fornisce statistiche descrittive, mentre il Paragrafo 3.2 descrive le varie regole tecniche di trading utilizzate. Il Paragrafo 3.3 delinea le varie metriche di performance considerate per valutare le prestazioni delle regole, mentre il Paragrafo 3.4 illustra le misure di data-snooping impiegate nell'analisi. Infine, il Paragrafo 3.5 riporta i risultati empirici.

3.1 Origine dei Dati

Nell'analisi vengono utilizzati i prezzi giornalieri del Bitcoin provenienti da due fornitori diversi per scopi di robustezza, vale a dire CoinDesk e Bitstamp. Il primo mostra una media dei prezzi del Bitcoin sulle principali piattaforme di scambio che soddisfano i criteri specificati da CoinDesk stesso. Questi criteri includono che lo scambio debba servire una clientela internazionale, debba fornire uno spread per una vendita e un acquisto immediato, mentre anche la dimensione minima di scambio deve essere inferiore a $1500. Inoltre, il volume di scambio giornaliero deve soddisfare i livelli minimi come determinato da CoinDesk, mentre lo scambio deve rappresentare almeno il 5% del volume totale di 30 giorni cumulativo per tutte gli scambi inclusi nel prezzo di CoinDesk. Viene considerato anche un prezzo attuale di scambio del Bitcoin, vale a dire Bitstamp, una delle prime piattaforme di scambio del Bitcoin, con sede nel Regno Unito. Per le altre piu' grandi criptovalute sul mercato quali Litecoin, Ethereum e Ripple, si

ottengono dati giornalieri da CoinMarketCap. Si prende in considerazione ogni criptovaluta per il massimo periodo possibile per garantire che i risultati forniscano un quadro completo delle prestazioni dell'analisi tecnica di queste criptovalute. In particolare, si studia il prezzo del Bitcoin da CoinDesk dal 18 luglio 2010, Bitstamp dal 1 dicembre 2012, Litecoin dal 28 aprile 2013, Ripple dal 4 agosto 2013 ed Ethereum dal 7 agosto 2015. L'osservazione dei prezzi termina il 31 dicembre 2017 per tutte le criptovalute. Gli scambi avvengono 24 ore al giorno, 7 giorni su 7 in tutti i mercati e quindi sono incluse tutte le osservazioni durante il giorno, compresi i fine settimana, le vacanze e si ottiene, quindi, una serie temporale completa. La Figura 3.1, nell'introduzione del capitolo, rappresenta il grafico della serie temporale di ogni criptovaluta nel tempo per i periodi di campionamento scelti in questo studio e ciascuno mostra il drammatico aumento del prezzo di ogni criptovaluta e quindi anche la grande volatilità. Si considerano rendimenti tali che:

$$r_t = \frac{P_t - P_{t-1}}{P_{t-1}} \qquad (1)$$

dove P_t è il prezzo della criptovaluta al tempo t e P_{t-1} è il prezzo della criptovaluta al tempo $t-1$. LaTabella 3.1 riporta le statistiche descrittive dei rendimenti delle varie criptovalute dove si evince che queste hanno un rendimento medio positivo, con Ethereum avente il maggiore e Litecoin il minore, e dove Ethereum ha un rendimento medio doppio rispetto a quello di Bitstamp e Litecoin. Ripple è la criptovaluta più volatile mentre Bitstamp è la meno volatile. I valori massimi e minimi per ogni criptovaluta documentano i rendimenti estremi che si possono trovare con queste criptovalute. Tutte le criptovalute mostrano un eccesso di curtosi (allontanamento dalla normalità distributiva) che indica la natura leptocurtica di questi rendimenti. Litecoin e Ripple hanno la maggior inclinazione positiva e la maggiore curtosi in eccesso tra tutte le criptovalute. La Tabella 3.1, quindi, riflette la natura dei mercati delle criptovalute e come questi siano abbastanza diversi dalle attività finanziarie tradizionali.

Tabella 3.1 – Statistiche descrittive dei rendimenti di Bitstamp, CoinDesk, Ethereum, Ripple e Litecoin

Cryptocurrency	Mean	SD	Max	Min	Skewness	Kurtosis	Obs
CoinDesk	0.0061	0.0592	0.5289	−0.3883	0.8328	12.1985	2735
Bitstamp	0.0049	0.0481	0.4014	−0.4852	0.0693	14.2082	2217
Litecoin	0.0049	0.0769	1.2910	−0.4019	5.0661	67.6347	1710
Ripple	0.0070	0.0927	1.7937	−0.4600	6.3377	97.9744	1624
Ethereum	0.0098	0.0799	0.5070	−0.7292	0.2199	13.1442	877

3.2 Regole di Trading basate sull'Analisi Tecnica

L'analisi tecnica può essere suddivisa in due categorie distinte, quali la forma qualitativa e la forma quantitativa. La forma qualitativa è quella in cui vengono analizzati i grafici e si cerca di identificare dei pattern nei dati, mentre la forma quantitativa è l'analisi dei grafici passati attraverso l'utilizzo delle serie temporali per costruire segnali di trading. La differenza principale tra le due forme è che, data una certa regola di trading, l'analisi tecnica quantitativa è completamente oggettiva e ogni individuo dovrebbe giungere alla stessa conclusione, mentre l'analisi tecnica qualitativa è soggettiva e gli individui possono giungere a conclusioni diverse dallo stesso grafico. Nel prosieguo dell'analisi verranno studiate cinque classi di regole di trading comunemente usate dai trader ed esaminate in letteratura. La prima classe è la media mobile (la più utilizzata) che tenta di ripetere le tendenze e identificare le rotture imminenti esaminando le medie mobili, ed è molto simile all'effetto momentum della serie temporale. La seconda classe di regole prese in esame sono regole di "filtro" che tentano di seguire le tendenze comprando (o vendendo) ogni volta che il prezzo è incrementato (o diminuito) di una data percentuale. La terza classe è costituita dalle regole di supporto-resistenza che creano dei limiti di supporto o resistenza intorno al prezzo che, se violati, indicano un ulteriore movimento nella stessa direzione. La quarta classe è quella degli oscillatori, che tentano di identificare gli asset *overbought* (termine usato per indicare il caso in cui una security è scambiata ad un prezzo superiore del suo fair value) e quindi anticipare l'imminente correzione del mercato. L'ultima classe di regole studiate sono le regole di *breakout* che

identificano livelli di supporto e resistenza variabili nel tempo che, una volta violati, indicano ulteriori movimenti nella stessa direzione.
La scelta dei parametri da impiegare in queste regole è piuttosto importante poiché parametri diversi possono generare rendimenti abbastanza contrastanti. Pertanto, si esamina una serie di diverse varianti di ogni classe, ottenendo così un numero molto elevato di regole.

3.3 Indici di Performance

Il rendimento della *j*-esima regola di trading in ogni mercato di criptovalute è definita da:

$$R_{j,t} = S_{j,t-1} * r_t \qquad (2)$$

Dove $S_{j,t-1}$ indica la posizione guidata dalla *j*-esima regola tecnica ed è determinata tracciando lo storico dei prezzi dallo spot rate di chiusura del periodo $t-1$. $S_{j,t-1}$ assume valore pari ad 1 nel caso in cui si è in posizione lunga, -1 se si è in posizione corta oppure 0 se si è neutrali.
Qualsiasi analisi delle strategie di trading deve considerare i costi di transazione, poiché se i rendimenti di una strategia di trading non sono positivi dopo aver tenuto conto di tali costi, la strategia, per un investitore, diventa inutile. Questo è particolarmente importante perché molti articoli hanno esaminato che le regole tecniche di trading sono redditizie per gli investitori, ma una volta che vengono aggiunti i costi di transazione, molte regole non lo sono più. Tuttavia, i costi di transazione effettivi possono essere molto diversi sulle diverse borse, e dal momento in cui vengono studiate quattro diverse criptovalute, i costi di transazione sui mercati possono variare. Pertanto, si riportano i costi di transazione di breakeven al fine di determinare l'entità dei suddetti che renderebbero i rendimenti tecnici di trading pari a zero.
Il primo indicatore di performance presentato è il rendimento medio giornaliero della *j*-esima regola tecnica di trading definito come:

$$\bar{R}_j = \frac{1}{n}\sum_{t=1}^{T} R_{j,t} \qquad (3)$$

dove $\bar{R}_j$ è il rendimento medio. Questa è la misura di performance più semplice e quantifica il rendimento medio di ogni operazione di ogni regola di trading tecnico. Tuttavia, un limite di questa misura è che non tiene conto della rischiosità della regola di trading in termini di volatilità dei rendimenti. Perciò è utile introdurre anche l'indice di Sharpe che rappresenta la metrica standard di performance nell'industria finanziaria e misura le unità di eccesso di rendimento medio per unità di rischio come misura della deviazione standard dei rendimenti in eccesso. L'indice di Sharpe della *j*-esima regola tecnica di trading è definita come:

$$SR_j = \frac{\bar{R}_j - r_f}{\sigma_j} \qquad (4)$$

dove r_f è il tasso risk-free giornaliero e σ_j è la deviazione standard dell'eccesso dei rendimenti generati dalla j-esima regola tecnica. Tuttavia, una limitazione dell'indice di Sharpe è che include sia la volatilità al ribasso che quella al rialzo, con la stessa ponderazione. Gli investitori possono essere interessati solo al rischio di ribasso, dato che il rialzo fornisce loro maggiori rendimenti. Di conseguenza, si calcola anche l'indice di Sortino della *j*-esima regola tecnica definito come:

$$SO_j = \frac{\bar{R}_j - r_f}{\sigma_{n,j}} \qquad (5)$$

dove $\sigma_{n,j}$ è la deviazione standard dell'eccesso negativo dei rendimenti generati dalla j-esima regola tecnica. L'ultima metrica di performance è l'indice di Calmar, un indicatore importante per le banche d'investimento e per l'industria degli hedge fund. Quest'indice calcola il rendimento medio annuale di un investimento per unità di massimo drawdown ed è particolarmente utile per i professionisti che impiegano strategie basate sul

momentum che possono subire notevoli perdite. L'indice di Calmar della j-esima regola tecnica definito come:

$$CR_j = \frac{\bar{R}_j}{MDD_j} \tag{6}$$

dove MDD_j è il massimo drawdown dell'eccesso dei rendimenti generato dalla j-esima regola tecnica.

3.4 Data-Snooping

La distorsione da snooping dei dati è un problema reale ogni volta che viene implementata una strategia di trading, poiché esaminare solo l'eccesso di rendimento medio tra le regole non è sufficiente. La ricerca tra una serie di regole di trading concorrenti implica l'aumento del numero di ipotesi testate, dato che le regole meno performanti vengono ignorate. Il problema del test di ipotesi multiple deriva dal fatto che, aumentando il numero di ipotesi testate, aumenta anche la probabilità di un evento raro e quindi la probabilità di rifiutare erroneamente l'ipotesi nulla di ogni regola di trading (commettendo un errore del I tipo). Come soluzione, vengono adottati due approcci per affrontare il test di ipotesi multiple, vale a dire il *Family-Wise Error Rate* (FWER) ed il *False Discovery Rate* (FDR).

3.4.1 Family-Wise Error Rate (FWER)

Il test di ipotesi multiple più rigoroso consiste nel cercare di evitare qualsiasi falso rifiuto. Questo si traduce con il controllo del FWER, definito come la probabilità di rifiutare anche una sola delle ipotesi nulle vere e, quindi, misura la probabilità di scoprirne anche sola una falsa. Si analizzano nei seguenti sottoparagrafi i due test FWER principali.

3.4.1.1 Il Metodo Bonferroni

Il metodo Bonferroni è una procedura a passo singolo poiché tutti i p-value sono confrontati con un singolo valore critico. Questo p-value critico è α/M, dove α è il valore

critico scelto e M è il numero di regole esaminate. Per un gran numero di regole, questo aggiustamento porta ad un *p*-value estremamente piccolo che lo rende molto conservativo e porta ad una perdita di potenza del metodo. La mancanza di potenza è dovuta al fatto che tratta implicitamente tutte le statistiche di test come indipendenti e quindi ignora la correlazione incrociata che è destinata ad essere presente nelle regole tecniche di trading impiegate in questo studio.

3.4.1.2 Il Metodo Holm

Il metodo Holm è un aggiustamento graduale che rifiuta l'ipotesi nulla se $p_i \leq \alpha/(M - i + 1)$ per $i = 1, \ldots$ Rispetto al metodo Bonferroni, il metodo Holm diventa meno rigoroso per *p*-value grandi. Quindi, questo metodo tipicamente rifiuta più ipotesi ed è più potente del metodo Bonferroni. Tuttavia, esso non tiene conto della struttura di dipendenza dei singoli *p*-value ed è molto conservativo.

3.4.2 False Discovery Rate (FDR)

Piuttosto che controllare il numero di volte in cui viene rifiutata un'ipotesi vera, conviene controllare la proporzione di falsi rifiuti della *False Discovery Proportion* (FDP). Il FDR misura e controlla tutte le FDP attese in tutti i casi in cui un test di ipotesi multiple controlli il FDR al livello δ se $FDR \equiv E(FDP) \leq \delta$, dove il livello δ è definito dall'utente.

3.4.2.1 Il Metodo BH

Uno dei primi metodi di controllo FDR è da attribuire a Benjamini e Hochberg (rif. [9]) ed è una procedura graduale che, data l'assunzione che tutti i singoli *p*-value siano ordinati dal più piccolo al più grande, è definito come:

$$j^* = max\left\{ j : p \leq \frac{j * \delta}{M} \right\} \qquad (7)$$

dove vengono rigettate tutte le ipotesi $H1, H2, \ldots, Hj$. Questo è un metodo step-up che inizia con l'esame dell'ipotesi meno significativa e passa a statistiche di test più significative.

3.4.2.2 Il Metodo BY

Sebbene il metodo BH misuri il FDR se i *p*-value sono indipendenti, il metodo BY, ideato da Benjamini and Yekutieli (rif. [10]), dimostra che può essere ottenuto un controllo più generale dello stesso sotto una condizione di dipendenza arbitraria dei *p*-value sostituendo la definizione di j^* con:

$$j^* = max\left\{ j: p \leq \frac{j * \delta}{M * C_M} \right\} \qquad (8)$$

dove $C_M = \sum_{i=1}^{M} {}^{1}/_{i} \approx log(M) + 0{,}5$. Ad ogni modo, questo metodo è meno potente del BH ed è molto conservativo.

Sono utilizzate queste quattro procedure di test di ipotesi multiple sui singoli *p*-value di ogni regola di trading. Per acquisire i singoli *p*-value si segue la procedura di ricampionamento e successivamente si utilizza il metodo bootstrap stazionario per ricampionare i rendimenti di ogni strategia, dove la corrispondente statistica di test per ogni serie di rendimenti del bootstrap è calcolata confrontando il *p*-value originale con i *p*-value bootstrap.

3.5 Risultati Empirici

3.5.1 Risultati Iniziali

La Tabella 3.2 riporta il riepilogo delle prestazioni delle regole tecniche di trading su tutte le criptovalute. Viene presentato il risultato medio per tutte le parametrizzazioni di ogni regola dove si mostra che, in media, tutte e cinque le classi di regole tecniche di trading generano rendimenti annualizzati significativi per tutte le criptovalute studiate. Per ogni criptovaluta e regola tecnica di trading, il rendimento medio di un segnale di acquisto è positivo e statisticamente significativo, mentre il rendimento medio da un

segnale di vendita è per lo più negativo, il che indica che i rendimenti positivi del trading tecnico nelle criptovalute provengono dai segnali di acquisto piuttosto che dai segnali di vendita. Tra tutte le criptovalute, la regola del filtro e il breakout hanno dato i risultati migliori, generando rendimenti annualizzati più alti, pari al 16,45% per Ripple. I risultati riportati nella Tabella 3.2 mostrano solo i rendimenti, ma la rischiosità degli stessi contiene molte informazioni per gli investitori. Pertanto, si riportano una serie di metriche che tengono conto del rischio nella Tabella 3.3, dove si osserva che tutte sono maggiori di zero, indicando che il trading tecnico nelle criptovalute supera il tasso risk-free. Troviamo che l'indice di Sortino è molto più alto di quelli di Sharpe e Sharpe corretto, il che indica che il rischio dovuto a movimenti al ribasso dei rendimenti è molto limitato. Questo è supportato, inoltre, dall'indice di Calmar che, in ogni caso, è abbastanza grande. Pertanto, i risultati mostrano che, in media, tutte le classi di regole di trading tecnico generano rendimenti significativi che forniscono metriche corrette per il rischio.

Tuttavia, è possibile che non tutte le diverse parametrizzazioni delle regole di trading tecnico generino rendimenti positivi e significativi. Pertanto, per ogni regola, si riporta la percentuale di segnali di acquisto, di vendita e complessivi che producono rendimenti positivi e significativi i cui risultati sono presentati nella Tabella 3.4. Oltre il 95% delle regole tecniche di trading genera rendimenti positivi in acquisto in CoinDesk e Bitstamp, mentre oltre il 90% delle regole genera rendimenti positivi in acquisto in Litecoin e Ripple. La stragrande maggioranza delle regole genera rendimenti di acquisto significativi in tutte le classi di regole tecniche e in tutte le criptovalute. La percentuale di ritorni di vendita che generano rendimenti positivi è leggermente più bassa, variando tra solo l'1,97% per la regola oscillator in CoinDesk, al 52,47% per la regola della media mobile in Litecoin. Questo suggerisce che solo alcune delle parametrizzazioni di ogni regola generano rendimenti positivi da un segnale di vendita. Inoltre, si trova che solo una percentuale molto piccola di segnali di vendita genera rendimenti significativi, con 15 delle 20 classi di regole di trading tecnico su tutte le criptovalute non aventi regole che generano un rendimento di vendita significativo dopo i segnali di vendita. Le due colonne finali riportano le statistiche per i rendimenti complessivi e mostrano che la grande maggioranza delle regole genera rendimenti positivi e oltre il 50% di esse genera rendimenti significativi con un livello del 5%, con eccezione della regola supporto-

resistenza per Litecoin, Ripple ed Ethereum. Quindi, i risultati della Tabella 3.4 mostrano che, sebbene non tutte le regole tecniche di trading generino rendimenti significativi, molte di esse generano comunque rendimenti importanti per gli investitori.

Dal momento in cui alcune delle regole di trading danno buoni risultati e altre meno, la Tabella 3.5 riporta le regole con le migliori e le peggiori prestazioni in termini di rendimento annualizzato, indici di Sharpe e Sortino. Chiaramente, le regole con le peggiori prestazioni generano rendimenti annualizzati che vanno dal 2,68% al -3,90%, con indici di Sharpe e Sortino negativi. Tuttavia, le regole più performanti riportate nelle ultime tre colonne mostrano rendimenti sostanziali per gli investitori. Per esempio, il rendimento annualizzato più alto di CoinDesk è del 13,42%, mentre il più alto per Ethereum è del 22,15%. Gli indici annualizzati di Sharpe e Sortino sono anche abbastanza grandi, indicando i benefici corretti per il rischio del trading tecnico nelle criptovalute. Pertanto, se gli investitori possono scegliere le migliori regole in termini di performance, allora sono presenti opportunità di guadagno nell'applicazione di regole di trading tecnico ai mercati delle criptovalute.

Tabella 3.2 - Perfomance delle regole tecniche di trading sul periodo di riferimento per ogni criptovaluta

Technical trading rule	No.Buys	No.Sells	Ave Buy Return (%)	Ave Sell Return (%)	Ave Return (%)	Ann.Return (%)
Panel A: CoinDesk						
Moving average rule	1114.80	546.59	0.42***	−0.02	0.40***	7.72***
Filter rule	2235.67	104.60	0.55***	−0.01	0.54***	10.24***
Support-resistance rule	333.03	85.09	0.19***	−0.02	0.17***	3.33***
Oscillator rule	858.04	265.08	0.41***	−0.02	0.38***	7.34***
Channel breakout rule	2075.14	135.36	0.54***	−0.01	0.53***	10.11***
Panel B: Bitstamp						
Moving average rule	899.11	432.58	0.33***	−0.03	0.30***	5.82***
Filter rule	1788.75	80.65	0.43***	−0.01	0.42***	7.97***
Support-resistance rule	282.81	62.76	0.16***	−0.02	0.14***	2.63***
Oscillator rule	623.26	161.15	0.29***	−0.03	0.27***	5.07***
Channel breakout rule	1642.09	109.92	0.42***	−0.01	0.41***	7.89***
Panel C: Litecoin						
Moving average rule	478.50	530.66	0.36***	0.00	0.35***	6.74***
Filter rule	1291.54	109.95	0.48***	0.00	0.48***	9.18***
Support-resistance rule	123.48	71.52	0.12***	−0.02	0.10***	1.96***
Oscillator rule	300.87	257.41	0.31***	0.00	0.31***	5.85***
Channel breakout rule	1162.34	153.71	0.47***	0.01	0.48***	9.21***
Panel D: Ripple						
Moving average rule	425.25	576.14	0.48***	−0.01	0.47***	8.89***
Filter rule	1191.46	139.85	0.64***	0.00	0.64***	12.30***
Support-resistance rule	135.52	105.24	0.26***	−0.02	0.25***	4.73***
Oscillator rule	282.21	271.30	0.42***	0.00	0.42***	7.94***
Channel breakout rule	1090.53	184.69	0.63***	0.01	0.64***	12.21***
Panel E: Ethereum						
Moving average rule	369.60	153.57	0.65***	−0.06	0.59***	11.32***
Filter rule	697.17	33.02	0.88***	−0.02	0.86***	16.45***
Support-resistance rule	104.46	33.71	0.24***	−0.03	0.20***	3.85***
Oscillator rule	261.87	91.31	0.52***	−0.03	0.49***	9.40***
Channel breakout rule	663.41	42.50	0.85***	−0.02	0.84***	15.99***

Tabella 3.3 - Performance corrette per il rischio delle regole tecniche di trading sul periodo di riferimento per ogni criptovaluta

Technical trading rule	Sharpe	Ann. Sharpe	Adj. Sharpe	Sortino	Ann. Sortino	Calmar
Panel A: CoinDesk						
Moving average rule	0.0039	0.0751	0.0763	0.1378	2.6324	2.9415
Filter rule	0.0053	0.1009	0.1022	0.1626	3.1060	3.7812
Support-resistance rule	0.0015	0.0286	0.0291	0.0867	1.6559	1.2753
Oscillator rule	0.0037	0.0713	0.0725	0.1487	2.8409	2.8481
Channel breakout rule	0.0052	0.0995	0.1008	0.1619	3.0927	3.9109
Panel B: Bitstamp						
Moving average rule	0.0029	0.0553	0.0553	0.1162	2.2206	1.9806
Filter rule	0.0041	0.0778	0.0774	0.1435	2.7411	2.8246
Support-resistance rule	0.0010	0.0189	0.0257	0.0883	1.6875	0.9897
Oscillator rule	0.0025	0.0480	0.0479	0.1297	2.4775	1.9336
Channel breakout rule	0.0040	0.0769	0.0765	0.1433	2.7373	2.9659
Panel C: Litecoin						
Moving average rule	0.0034	0.0657	0.0691	0.1041	1.9891	1.3079
Filter rule	0.0047	0.0906	0.0960	0.1359	2.5957	1.8565
Support-resistance rule	0.0007	0.0132	0.0139	0.0495	0.9461	0.4557
Oscillator rule	0.0030	0.0573	0.0606	0.1137	2.1719	1.4240
Channel breakout rule	0.0048	0.0908	0.0963	0.1370	2.6170	2.0260
Panel D: Ripple						
Moving average rule	0.0046	0.0876	0.0935	0.1271	2.4276	2.2358
Filter rule	0.0064	0.1220	0.1304	0.1648	3.1491	3.1258
Support-resistance rule	0.0023	0.0447	0.0484	0.0948	1.8116	1.4682
Oscillator rule	0.0041	0.0778	0.0831	0.1318	2.5189	2.0657
Channel breakout rule	0.0063	0.1211	0.1293	0.1638	3.1286	3.2246
Panel E: Ethereum						
Moving average rule	0.0058	0.1115	0.1134	0.1676	3.2017	8.2456
Filter rule	0.0085	0.1633	0.1673	0.2346	4.4822	16.2931
Support-resistance rule	0.0018	0.0351	0.0358	0.0796	1.5214	1.9094
Oscillator rule	0.0048	0.0919	0.0935	0.1601	3.0591	6.0633
Channel breakout rule	0.0083	0.1586	0.1624	0.2279	4.3532	15.9528

Tabella 3.4 - Percentuale di successo delle regole tecniche di trading per ogni criptovaluta, di cui si riporta la percentuale di successo delle regole con rendimenti di acquisto (e vendita) positivi e la percentuale di quelle statisticamente significative con un livello di significatività del 5%

Technical trading rule	% + Buy Ret.	% Sig. Buy Ret.	% + Sell Ret.	% Sig. Sell Ret.	% + Ret.	% Sig. Ret.
Panel A: CoinDesk						
Moving average rule	96.71	88.69	27.53	0.01	96.61	87.40
Filter rule	100.00	99.68	18.20	0.00	100.00	98.84
Support-resistance rule	95.03	66.56	7.62	0.00	92.49	58.10
Oscillator rule	99.63	96.05	1.97	0.00	99.63	95.44
Channel breakout rule	100.00	98.66	29.33	0.00	99.74	97.26
Panel B: Bitstamp						
Moving average rule	96.70	88.69	27.52	0.01	96.61	87.40
Filter rule	100.00	99.15	21.69	0.11	99.68	98.31
Support-resistance rule	97.04	71.96	4.87	0.00	95.45	62.12
Oscillator rule	99.75	96.17	1.98	0.00	99.75	95.56
Channel breakout rule	100.00	98.66	29.33	0.00	99.74	97.26
Panel C: Litecoin						
Moving average rule	95.60	78.20	52.47	0.09	96.15	69.30
Filter rule	99.79	97.46	51.96	0.00	99.47	92.80
Support-resistance rule	90.79	32.17	14.71	0.00	83.28	20.95
Oscillator rule	95.19	79.26	45.19	0.00	95.19	74.07
Channel breakout rule	99.45	94.84	70.54	0.04	98.72	90.50
Panel D: Ripple						
Moving average rule	96.92	84.44	38.73	0.31	96.45	79.26
Filter rule	100.00	99.79	37.46	0.32	100.00	99.68
Support-resistance Rule	94.29	46.56	15.24	0.00	92.38	39.89
Oscillator rule	99.14	80.39	33.17	0.00	99.14	76.33
Channel breakout rule	100.00	99.55	52.40	0.70	100.00	98.60
Panel E: Ethereum						
Moving average rule	96.09	85.17	16.37	0.01	94.73	80.92
Filter rule	100.00	98.84	20.74	0.00	100.00	97.35
Support-resistance rule	87.63	39.01	14.16	0.00	86.89	28.22
Oscillator rule	98.40	80.02	14.06	0.00	98.40	75.96
Channel breakout Rule	99.77	96.77	25.56	0.08	99.66	94.88

Tabella 3.5 - Performance delle migliori e delle peggiori regole tecniche di trading per ogni classe di regole esaminata

Technical trading rule	Low. Ret. (%)	Low. Sharpe	Low. Sortino	High. Ret. (%)	High. Sharpe	High. Sortino
Panel A: CoinDesk						
Moving average rule	−1.56	−0.1876	−0.9431	12.89	0.1275	3.5891
Filter rule	0.14	−0.0022	−0.0686	12.71	0.1256	4.4093
Support-resistance rule	−0.82	−0.0310	−0.6051	11.50	0.1135	4.4346
Oscillator rule	−0.11	−0.0062	−0.0829	11.68	0.1154	4.4654
Channel breakout rule	−0.98	−0.0006	−0.0228	13.42	0.1328	4.0655
Panel B: Bitstamp						
Moving average rule	−2.12	−0.1754	−1.3216	9.49	0.0932	5.5326
Filter rule	−1.66	−0.0204	−0.9523	10.71	0.1054	3.6829
Support-resistance rule	−1.40	−0.1754	−0.9331	8.76	0.0858	4.1687
Oscillator rule	0.36	−0.0038	−0.3844	8.75	0.0856	4.1410
Channel breakout rule	−1.71	−0.0209	−0.9789	10.88	0.1071	3.7081
Panel C: Litecoin						
Moving average rule	−3.07	−0.0718	−1.4312	12.09	0.1199	4.9047
Filter rule	−1.00	−0.0118	−0.5276	12.73	0.1263	3.6305
Support-resistance rule	−2.99	−0.0765	−1.0944	11.39	0.1128	3.4859
Oscillator rule	−1.14	−0.0251	−0.6743	10.46	0.1035	3.9360
Channel breakout rule	−1.95	−0.0321	−1.0591	12.59	0.1249	3.6916
Panel D: Ripple						
Moving average rule	−3.77	−0.0626	−0.8037	20.51	0.2043	5.4383
Filter rule	2.68	0.0239	0.9338	18.75	0.1866	4.7530
Support-resistance rule	−0.72	−0.0192	−0.6126	17.43	0.1734	4.7239
Oscillator rule	−0.63	−0.0144	−0.7068	17.95	0.1787	4.5778
Channel breakout rule	1.57	0.0119	0.5512	17.21	0.1712	4.8170
Panel E: Ethereum						
Moving average rule	−3.90	−0.0414	−1.4669	21.49	0.2138	6.5969
Filter rule	0.67	−0.0108	−0.4907	22.15	0.2203	5.9422
Support-resistance rule	−1.42	−0.0195	−1.1403	18.72	0.1861	4.9685
Oscillator rule	−1.45	−0.0227	−1.0047	20.47	0.2035	5.3837
Channel breakout rule	−0.67	−0.0108	−0.4907	21.76	0.2164	5.8498

3.5.2 Costi di Transazione

Fino a questo punto, l'analisi ha assunto costi di transazione nulli, ma nella realtà questi possono essere significativi, anche quando si scambiano criptovalute. Infatti, una regola tecnica di trading può prevedere i movimenti di una criptovaluta, vale a dire capire se possa generare rendimenti significativi, ma questa potrebbe non essere redditizia una volta che i rendimenti in eccesso sono corretti per i costi di transazione. Tali costi nelle criptovalute differiscono a seconda della criptovaluta scambiata e dal tipo di scambio. Lintilhac e Tourin (rif. [16]) mostrano che la tassa di transazione per numero di Bitcoin è di 0,0025 dollari, mentre lo spread bid-ask è di 0,005 come frazione del prezzo in dollari. Tuttavia, è difficile stimare con precisione i costi di transazione di CoinDesk poiché è una media dei principali scambi globali di Bitcoin, mentre i costi di transazione

delle altre criptovalute possono variare notevolmente nel tempo. Pertanto, per evitare qualsiasi distorsione nei risultati, si riportano nella Tabella 3.6 i costi medi di transazione di breakeven in punti base, insieme al numero di transazioni richieste. Il numero di transazioni è piuttosto costante all'interno di ogni criptovaluta, anche se la regola del filtro genera il maggior numero di transazioni tra le criptovalute. I costi di transazione di breakeven variano da 7,88 punti base per la regola supporto-resistenza in Litecoin a 147,56 punti base per la regola del filtro in Ethereum. Se ci si concentra su CoinDesk e Bitstamp, i costi di transazione di breakeven sono rispettivamente 66,41 e 57,51 punti base. Lintilhac e Tourin riportano che i costi di transazione per Bitcoin è di circa 50 punti base e quindi, anche nella Tabella 3.6, si riporta la percentuale di regole tecniche di trading che offrono costi di transazione di breakeven superiori a 50 punti base. Ogni classe di regole tecniche di trading per ogni criptovaluta genera una percentuale sostanziale di regole maggiori di 50 punti base, con l'eccezione della regola di supporto-resistenza. Per esempio, il 36,06% delle regole dell'oscillatore genera costi di transazione di breakeven superiori a 50 punti base per CoinDesk, mentre il 47,35% delle regole di breakout genera regole con costi di transazione di breakeven superiori a 50 punti base per Ethereum. Pochissime regole di supporto-resistenza generano costi di transazione di pareggio superiori a 50 punti base, indicando che questa famiglia di regole tecniche di trading non ha molto successo per tutte e quattro le criptovalute. Tuttavia, un'ampia percentuale di regole di trading tecnico genera costi di transazione di breakeven maggiori di 50 punti base, indicando che le prestazioni delle regole di trading tecnico nelle criptovalute non vengono eliminate dai costi di transazione appropriati.

Tabella 3.6 - Numero di nuovi scambi generati dalle regole tecniche di trading per ogni criptovaluta, il punto di breakeven espresso in basis point e la percentuale di regole aventi punto di breakeven al di sopra di 50 basis point

Technical trading rule	No. trades	Breakeven TCs	% > 50 basis points
Panel A: CoinDesk			
Moving average rule	182.98	54.86	32.04
Filter rule	294.22	66.41	32.38
Support-resistance rule	223.65	11.42	0.00
Oscillator rule	210.89	44.60	36.06
Channel breakout Rule	274.25	61.00	30.18
Panel B: Bitstamp			
Moving average rule	152.65	50.40	22.79
Filter rule	238.43	57.51	28.15
Support-resistance rule	184.06	11.89	0.95
Oscillator rule	172.04	38.74	25.15
Channel breakout rule	217.57	54.12	27.38
Panel C: Litecoin			
Moving average rule	137.39	35.44	25.81
Filter rule	237.13	30.66	19.68
Support-resistance rule	121.38	7.88	0.21
Oscillator rule	134.73	38.42	24.44
Channel breakout rule	214.77	30.42	17.97
Panel D: Ripple			
Moving average rule	128.55	36.01	26.25
Filter rule	242.44	33.59	19.15
Support-resistance rule	135.45	16.16	3.49
Oscillator rule	127.45	52.14	34.04
Channel breakout rule	219.22	33.06	18.37
Panel E: Ethereum			
Moving average rule	68.39	78.60	38.72
Filter rule	99.83	147.56	49.52
Support-resistance rule	76.66	9.89	0.11
Oscillator rule	69.12	50.05	36.74
Channel breakout Rule	93.53	144.03	47.35

3.5.3 Confronto con la strategia buy-and-hold

Come mostrato nella Figura 3.1, le criptovalute hanno seguito una tendenza al rialzo nel tempo, specialmente in periodi recenti. Pertanto, una strategia buy-and-hold può aver avuto un discreto successo nello stesso periodo preso come campione. Quindi si riportano, nella Tabella 3.7, il rendimento annualizzato, l'indice di Sharpe e di Sortino annualizzati e l'indice di Calmar per le strategie buy-and-hold per ogni criptovaluta. Tra parentesi, si riporta anche la percentuale di regole tecniche di trading che generano

rendimenti corretti per il rischio superiori alla strategia buy-and-hold. Per ogni criptovaluta, si nota che solo una piccola percentuale di regole genera rendimenti annualizzati maggiori della strategia buy-and-hold. Tuttavia, una volta esaminate le metriche corrette per il rischio, si trova che un numero sostanzialmente maggiore di regole di trading tecnico offre rendimenti superiori alla strategia buy-and-hold specialmente per gli indici annualizzati di Sortino e Calmar, i quali catturano entrambi il rischio di ribasso. Questo indica che l'impiego di regole tecniche di trading evita grandi, gravi e lunghi drawdown associati alle criptovalute e offre agli investitori rendimenti più uniformi rispetto a quelli che si sarebbero potuti ottenere con la semplice strategia buy-and-hold. Pertanto, si dimostra che, nel caso in cui gli investitori volessero limitare la loro esposizione al rischio della volatilità delle criptovalute, potrebbero impiegare regole tecniche di trading per appianare i loro rendimenti futuri.

Tabella 3.7 - Presentazione del rendimento, dell'indice di Sharpe, di Sortino e di Calmar annualizzati per la strategia buy-and-hold in ogni criptovaluta.

	Ann.Return	Ann.Sharpe	Ann.Sortino	Calmar
CoinDesk	0.1167 (6.12%)	0.1153 (6.12%)	3.1996 (32.83%)	4.22019 (28.58%)
Bitstamp	0.0942 (4.96%)	0.0925 (4.86%)	3.0163 (32.14%)	3.4522 (32.72%)
Litecoin	0.0928 (11.49%)	0.0918 (41.30%)	2.4167 (51.26%)	1.3750 (57.64%)
Ripple	0.1339 (15.69%)	0.1330 (15.69%)	3.1768 (27.99%)	2.7796 (36.73%)
Ethereum	0.1875 (9.01%)	0.1864 (8.98%)	3.9645 (49.71%)	11.0426 (42.17%)

3.5.4 Correzione MHT

Finora, si è dimostrato che le regole tecniche di trading offrono potere predittivo agli investitori nei cinque mercati di criptovalute. Tuttavia, come menzionato in precedenza, è presente un problema con il data mining in cui la ricerca tra una serie di regole in competizione è probabile che si traduca in almeno un paio di regole che generano risultati significativi. In questa sede, si esaminano moltissime regole e quindi la probabilità di rifiutare erroneamente l'ipotesi nulla è piuttosto alta. Per aggirare questo problema, si adottano una serie di procedure diverse in cui prima si calcola il *p*-value individuale di ogni regola, il che implica l'impiego del bootstrap stazionario per ricampionare i rendimenti di ogni strategia e i singoli *p*-value sono generati confrontando l'originale con

quelli di bootstrap. La Tabella 3.8 presenta la percentuale di rendimenti dei singoli *p*-value bootstrap significativi con un livello del 5% dopo le correzioni tramite Bonferroni, Holm, BH, BY e nessuna correzione. La correzione Bonferroni è la più restrittiva di tutte le procedure di test di ipotesi multiple, dove per ogni criptovaluta, suggerisce che il minor numero di regole genera rendimenti significativi. Tuttavia, si può notare che per ogni criptovaluta, una grande proporzione di regole è significativa anche dopo aver tenuto conto del test di ipotesi multiple. Per esempio, il 33,61% delle regole sono ancora statisticamente significative dopo le correzioni Bonferroni e Hold per CoinDesk, indicando che oltre un terzo delle regole genera rendimenti significativi. Sebbene questo sia un forte calo rispetto al numero di regole significative riportate nella Tabella 3.4, è chiaramente evidenziato che le regole tecniche sono redditizie nei mercati delle criptovalute.

Tabella 3.8 - Percentuale di regole significative con un livello del 5% dopo test effettuati su numerose ipotesi multiple

	Bonferroni (%)	Holm (%)	BH (%)	BY (%)	None (%)
CoinDesk	33.61	33.61	50.41	33.61	57.65
Bitstamp	27.11	27.13	46.28	28.56	58.64
Litecoin	23.26	23.26	31.84	23.26	53.23
Ripple	20.35	20.35	27.96	20.35	27.96
Ethereum	23.37	23.37	32.68	23.37	32.68

3.5.5 Performance Fuori Campione

Un'altra soluzione per affrontare il problema del data-snooping è quella di impiegare un'analisi out-of-sample per esaminare se le migliori regole tecniche di trading dalla stima effettuata in-sample si comportano bene al di fuori del campione. Tuttavia, uno dei problemi che sorge quando si esamina una performance fuori campione di qualsiasi strategia di investimento è la scelta dei periodi di in-sample e out-of-sample. Questo è particolarmente importante per le regole di trading tecnico, poiché c'è una tendenza in letteratura a considerare la performance delle regole decrescente nel tempo. Inoltre, McLean e Pontiff (rif. [17]) mostrano che la performance delle variabili di prevedibilità diminuiscono sostanzialmente dopo la pubblicazione nella letteratura accademica. In

aggiunta, una stima fuori campione è molto importante per quanto riguarda le criptovalute. La loro volatilità è stata estremamente elevata, il che ha scoraggiato un certo numero di istituzioni e investitori dall'includerle nei loro portafogli. Inoltre, c'è stata un'enorme impennata nel prezzo delle criptovalute nella seconda metà del 2017, soprattutto per il Bitcoin, dove il prezzo ha raggiunto in tempi rapidi i 20.000 dollari. Nell'analisi inclusa in questo capitolo si utilizzano dati fino al 31 Dicembre 2017, ma da allora c'è stato un enorme calo del valore delle criptovalute, con il prezzo che si aggirava intorno ai 6500 dollari all'inizio di Luglio 2018. Quindi, è possibile offrire un'analisi out-of-sample pura per determinare se l'analisi tecnica delle criptovalute offra un potere predittivo e sia capace di esaminare quale sia stata la loro performance durante il mercato delle criptovalute della prima metà del 2018.

Si fornisce uno spunto della performance che gli investitori avrebbero potuto ottenere in un periodo fuori campione e durante la flessione dei mercati delle criptovalute. In particolare, si esamina la performance delle regole più performanti fino al 31 Dicembre 2017 e successivamente il loro rendimento durante i primi 6 mesi del 2018, i cui risultati sono riportati nella Tabella 3.9. La regola di breakout produce le regole più performanti (tutte molto simili in termini di parametri) sia per i prezzi del Bitcoin che di Litecoin per il periodo in-sample, mentre le regole della media mobile sono le regole di trading tecnico più performanti nel campione per Ripple e Ethereum. Nei periodi fuori campione, si trovano rendimenti annualizzati negativi, indici di Sharpe e Sortino per entrambi i prezzi di Bitcoin. Tuttavia, le altre tre criptovalute mostrano rendimenti out-of-sample positivi, così come indici di Sharpe e Sortino. Questo indica che il Bitcoin potrebbe non essere redditizio per il trading utilizzando l'analisi tecnica in un contesto fuori campione, mentre le altre criptovalute studiate generano ancora rendimenti sostanziali e indici di Sharpe e Sortino elevati nel periodo fuori campione.

Il Bitcoin può essere la criptovaluta meno redditizia nel periodo fuori campione. Quest'ultima fu la prima criptovaluta creata, nonché la più liquida e quindi con maggiore forza attrattiva per gli investitori. Il numero relativamente grande di investitori che sono attratti dal Bitcoin significa che le strategie di trading redditizie possono essere più difficili da trovare man mano che il mercato diventa più efficiente. Questo si riflette anche nella letteratura accademica dove Corbet et al. (rif. [27]) mostrano che la maggior parte degli articoli accademici sulle criptovalute si concentra esclusivamente sul Bitcoin.

Inoltre, le altre criptovalute analizzate sono meno liquide e quindi hanno attirato con minor forza l'attenzione da parte degli investitori, suggerendo che potrebbero offrire maggiori opportunità di profitto rispetto al Bitcoin.

Tabella 3.9 - Presentazioni dei risultati out-of-sample per la miglior regola nel periodo di riferimento

	Best rule	Ann.Return	Ann.Sharpe	Ann.Sortino
CoinDesk	CB2: 25/0.05/0.025/5	− 0.0010	− 0.0502	− 0.3470
Bitstamp	CB2: 25/0.05/0.025/3	− 0.0091	− 0.0641	− 0.0553
Litecoin	CB2: 25/0.05/0.025/5	0.0775	1.3553	2.1900
Ripple	MA1: 2/0.001/1	0.0546	0.7380	1.2162
Ethereum	MA4: 2/25/0/1/5	0.0631	1.1900	1.8500

CAPITOLO 4
LE VALUTE DIGITALI DELLE BANCHE CENTRALI

I recenti avanzamenti tecnologici nelle tecniche crittografiche hanno contribuito all'espansione delle valute digitali. Le prime criptovalute furono pensate e create da enti privati, come ad esempio Bitcoin, Ethereum e Libra, ma nel corso della loro diffusione fino ad oggi, è lecito pensare di esplorare la possibilità che anche le Banche Centrali possano emettere le proprie valute digitali, propriamente chiamate "Valute Digitali della Banca Centrale" (*Central Bank Digital Currencies*, CBDC).

L'introduzione di una CBDC potrebbe rappresentare un'importante innovazione nella storia del denaro e delle banche. In aggiunta al ruolo chiave nella possibile eliminazione del contante fisico, una CBDC potrebbe permettere alla banca centrale di impegnarsi nell'intermediazione su larga scala entrando in competizione con gli intermediari finanziari privati per i depositi. In altre parole, emettere una CBDC equivale a dare agli individui la possibilità di tenere un conto bancario direttamente con la banca centrale.

Potrebbe, quindi, determinarsi un frangente nel quale i cambiamenti della tecnologia sarebbero in grado di giustificare una modifica fondamentale nell'architettura di un sistema finanziario, ossia una banca centrale "aperta a tutti". Le innovazioni tecnologiche potrebbero rimodellare il modo in cui viene inteso il ruolo del governo nella creazione di istituzioni monetarie e finanziarie.

Queste considerazioni sono già rilevanti per la politica monetaria. Nel Giugno 2018, gli elettori svizzeri hanno respinto l'iniziativa sul denaro sovrano (*Vollgeld*) che avrebbe dato alla banca centrale un monopolio sull'emissione di depositi, un'idea motivata in parte dalla possibilità di una CBDC svizzero. Nonostante l'iniziativa sia stata una sonora

sconfitta alle urne, progetti simili saranno destinati ad essere ampiamente discussi nei prossimi anni. Quali effetti avrà l'introduzione di una CBDC e l'apertura delle strutture della banca centrale sull'intermediazione finanziaria? Una CBDC comprometterà il ruolo del sistema finanziario nell'allocare fondi a progetti produttivi? O è possibile riorganizzare il sistema finanziario in modo tale che una CBDC permetta ancora il corretto flusso di fondi tra risparmiatori e investitori? Una CBDC farà scomparire le corse alle banche e stabilizzerà il sistema finanziario? In questo capitolo, si discuteranno le implicazioni di una CBDC sull'intermediazione finanziaria, coadiuvata dalla presenza di una banca centrale. Durante la trattazione, si porrà particolare enfasi sul ruolo delle banche nella trasformazione delle scadenze: le banche finanziano progetti a lungo termine con depositi. Capire come una CBDC interagirà con la trasformazione delle scadenze è una considerazione di primo ordine che non è stata esaminata a fondo dalla letteratura, spesso più interessata a questioni come le conseguenze di una CBDC sui tassi di interesse o l'evasione fiscale. Inoltre, si analizzerà come le "corse agli sportelli" (*bank-runs)* potrebbero cambiare con l'introduzione di una CBDC e di confrontare i risultati ottenuti con i precedenti presenti in letteratura.

Più concretamente, si prende in esame una situazione in cui la CBDC prende la forma di conti di deposito a vista presso la banca centrale. Analogamente ad una banca commerciale, la banca centrale detiene attività per finanziare queste passività, ma in contrasto con la prima, si assume che questa non possa investire in progetti a lungo termine. Tale fattore potrebbe essere dovuto al fatto che la banca centrale non ha una buona capacità di selezionare, monitorare e fornire liquidità per progetti produttivi. Tuttavia, è in grado, invece, di fare affidamento sulle banche d'investimento per impegnarsi in prestiti all'ingrosso. Il risultato è un principio di equivalenza che mostra che l'insieme delle allocazioni ottenute con l'intermediazione finanziaria privata può essere ottenuta anche con l'utilizzo di una CBDC, a condizione che la concorrenza con le imprese commerciali sia in grado di fornire la migliore allocazione *ex-ante*.

Questo risultato di equivalenza potrebbe giustificare il punto di vista dei sostenitori della CBDC: la quantità socialmente ottimale di trasformazione delle scadenze può ancora essere prodotta in un'economia in cui la banca centrale è aperta a tutti. Tuttavia, è importante fare una riflessione su questo esito: se la concorrenza delle banche commerciali è ostacolata (per esempio, attraverso qualche sovvenzionamento fiscale dei

depositi della banca), la banca centrale deve fare attenzione nelle sue scelte per evitare di creare il panico con la trasformazione delle scadenze.

Mentre la banca centrale è in grado di offrire il contratto di deposito socialmente ottimale, proprio come una banca commerciale, si dimostra che la rigidità del contratto della banca centrale con le banche d'investimento porta ad allocazioni diverse durante il panico bancario. Il prestito alla banca d'investimento non è richiamabile e questo implica che l'investimento indiretto della banca centrale nell'attività lunga è protetto dalla liquidazione anticipata da quest'ultimo, scoraggiando completamente le corse alla banca centrale o rendendole meno probabili delle corse al settore bancario commerciale. Gli individui, che verranno denominati depositanti nel proseguo del capitolo, interiorizzano questa caratteristica e depositano esclusivamente presso la banca centrale. Questo ha come conseguenza il fatto che la banca centrale diventa il fornitore monopolistico di depositi. Tale potere monopolistico può mettere in pericolo l'offerta della migliore quantità di trasformazione delle scadenze nell'economia, permettendo alla banca stessa di deviare dall'offerta del contratto di deposito socialmente ottimale.

4.1 Il Contesto Storico

Storicamente, molte banche centrali hanno concesso depositi ed esteso prestiti alle imprese e ai cittadini. Il più delle volte, queste attività erano considerate più importanti della corretta conduzione della politica monetaria, in termini di operazioni quotidiane e in termini di priorità del top management. Infatti, molti governi vedevano l'impatto positivo sulla crescita economica delle attività commerciali di una banca come motivazione per la creazione di tali istituzioni.

Il caso più famoso di una banca centrale impegnata in attività commerciali è la Banca d'Inghilterra. A questa istituzione, fondata nel 1694 come una società a responsabilità limitata, venne conferito il "*diritto di massimizzare i suoi profitti intraprendendo un'attività bancaria generale, compresa l'emissione di cartamoneta, l'accettazione di depositi, la concessione di prestiti ipotecari e trattando cambiali, nonché oro e argento*" (rif. [28]). La Banca d'Inghilterra ha perseguito vigorosamente tale obiettivo per oltre due secoli, invadendo il giro di affari delle altre banche commerciali attraverso la concorrenza diretta e lo sforzo di lobbying con il Parlamento a Westminster per ottenere

ulteriori privilegi legali per proteggere le sue attività private contro i potenziali concorrenti.

Negli Stati Uniti, sia la Prima che la Seconda Banca del Paese hanno partecipato attivamente ai mercati del prestito e del credito. Infatti, la guerra bancaria tra Andrew Jackson e Nicholas Biddle era legata direttamente alle operazioni della Seconda Banca degli Stati Uniti con le imprese e i commercianti.

A volte, le attività commerciali delle banche centrali erano così grandi da diventare gli attori dominanti nei mercati del prestito e del credito. Per esempio, nel 1900, la Banca di Spagna, con 58 filiali che coprivano tutte le principali città della nazione, deteneva il 68% delle attività totali e il 73% di tutti i depositi a vista nel settore finanziario spagnolo. Nella Figura 4.1 vengono tracciate le attività e le passività della Banca di Spagna dal 1874 al 1914. Il grafico superiore mostra come, all'inizio del 20° secolo, il portafoglio privato dei prestiti della banca era più grande del portafoglio pubblico di buoni del tesoro. Si può anche apprezzare, nel grafico inferiore, la grande dimensione dei conti correnti (i depositi a vista) sul lato delle passività della banca.

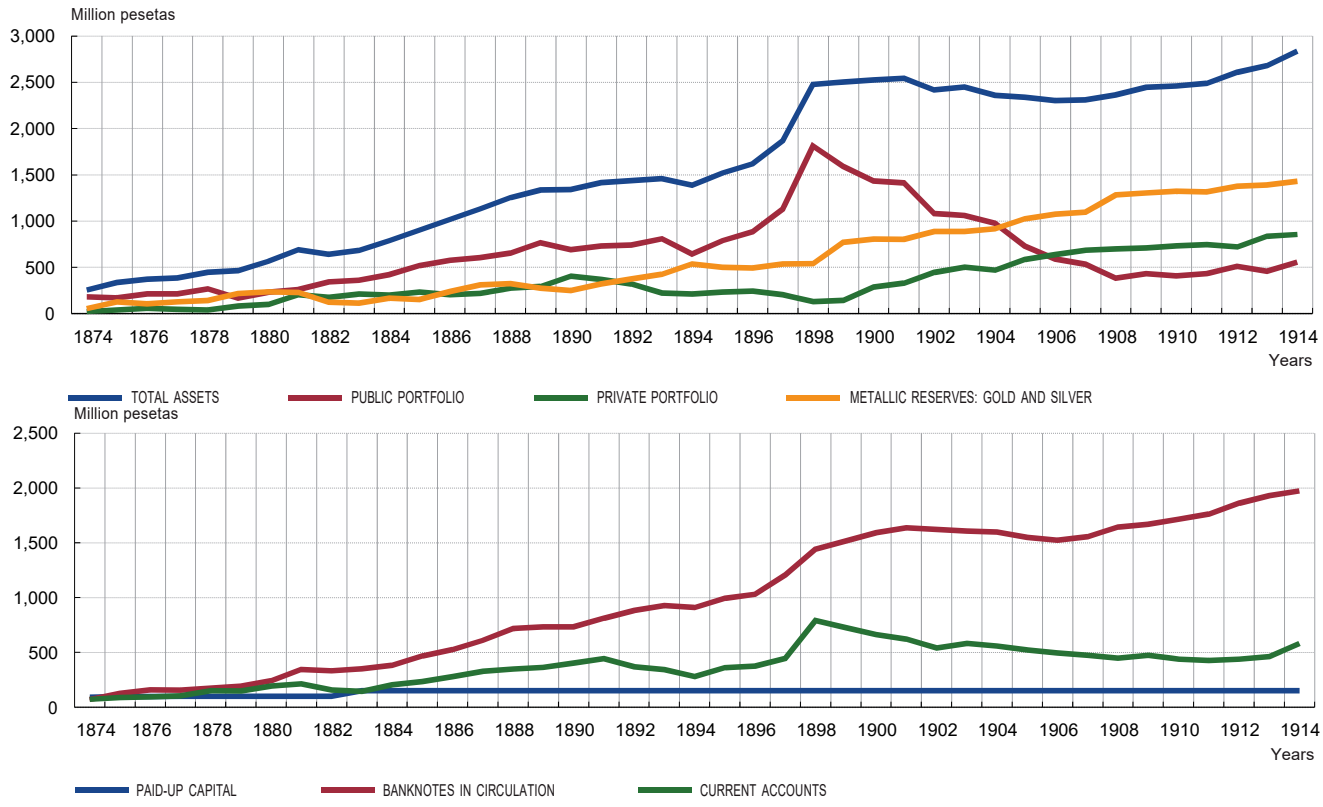

Figura 4.1 – Attività e passività della Banca di Spagna dal 1874 al 1914

Uno sviluppo correlato fu l'esistenza di sistemi di risparmio postale. Il primo di questi sistemi fu la Post Office Savings Bank (POSB) nel Regno Unito, fondata nel 1861. Negli Stati Uniti, un tale sistema è stato operativo dal 1911 al 1967, raggiungendo alla fine della Seconda Guerra Mondiale circa il 10% delle attività del settore bancario commerciale. Questi sistemi di risparmio postale sfruttavano la rete già esistente di uffici postali per offrire conti di deposito sostenuti dal governo e altri servizi finanziari come trasferimenti di denaro immediati ed economici ai cittadini. Pensando ad un bilancio consolidato del settore pubblico, i depositi presso un sistema di risparmio postale possono essere considerati del tutto equivalenti ai depositi presso una banca centrale: sono depositi in due agenzie diverse dello stesso settore pubblico. I vincoli politico-economici, tuttavia, possono far sì che tale equivalenza venga meno nella pratica (per esempio, se un governo tratta i profitti e le perdite di un sistema di risparmio postale in modo diverso dai profitti e dalle perdite di una banca centrale).

La netta distinzione tra una banca centrale che opera solo con istituzioni e le banche commerciali che trattano con i membri del pubblico in generale è, in misura non trascurabile, uno sviluppo successivo alla Seconda Guerra Mondiale. Questa mossa fu indotta, tra le altre ragioni, dal desiderio dei governi di controllare direttamente le politiche monetarie discrezionali una volta che il loro standard scomparve.

Queste nuove condizioni economiche portarono alla nazionalizzazione di molte banche centrali, come la Banca d'Inghilterra nel 1946 e la Banca di Spagna nel 1962, indipendentemente dall'inclinazione politica dei governi (di sinistra nel Regno Unito nel 1946, di destra autoritaria in Spagna nel 1962). Ma, anche oggi, si possono scambiare azioni di molte banche centrali in borsa, inclusa la Banca Nazionale Svizzera (vedi Figura 4.2 per il prezzo giornaliero di questo titolo dal 2001) e la Banca del Giappone. Sebbene queste azioni hanno severe limitazioni dei diritti di voto, il loro commercio attivo è la prova che le banche centrali erano impegnate in un insieme di attività molto diverse dalla pura conduzione della politica monetaria convenzionale.

Figura 4.2 – Prezzo delle azioni giornaliero della Banca Nazionale Svizzera

L'arrivo del denaro digitale ha riaperto il dibattito sul ruolo delle banche centrali. In primo luogo, le CBDC sono divenute una possibilità concreta. In aggiunta, internet permette ad una banca centrale di saltare la costruzione di una vasta rete di filiali, direttamente o in cooperazione con le banche commerciali esistenti.

4.2 Il Modello Bancario

Per affrontare le tematiche esposte in questo capitolo si prenderà come riferimento il modello bancario canonico di Diamond e Dybvig (rif. [8]). Tale modello è particolarmente adatto poiché pone la massima importanza al ruolo delle banche come fornitori di servizi di trasformazione delle scadenze. In questo modo, è possibile utilizzarlo per chiarire come la presenza di una CBDC, e la successiva apertura dei depositi della banca centrale al pubblico, influisca su tale intermediazione finanziaria e sulle corse alle banche che potrebbero interromperla.

Tuttavia, il modello si discosterà dalla sua versione standard, ed in particolar modo su due punti. La prima novità è l'introduzione di una distinzione tra banche commerciali e banche d'investimento. Successivamente si introdurrà una banca centrale controllata dal governo.

La distinzione tra i due tipi di banche risulterà conveniente per chiarire al meglio i risultati. Inoltre, trattare separatamente ogni tipo di banca porta alla possibilità di estendere il modello verso casistiche in cui ci sono differenze di regolamentazione tra banche commerciali e di investimento.

L'introduzione della banca centrale, invece, è necessaria poiché viene discusso l'impatto di una CBDC, la quale viene appunto emessa da una banca centrale. Tuttavia si deve fare un'ulteriore considerazione. Uno degli obiettivi primari dell'analisi è verificare che l'implementazione di un'allocazione efficiente può essere realizzata attraverso un accordo in cui un'istituzione controllata dal governo compete con le banche private per i depositi. Tali discussioni potrebbero essere separate da qualsiasi altra considerazione riguardante il denaro digitale, anche se questo rende la discussione più rilevante superando i precedenti ostacoli logistici che l'apertura al pubblico dei bilanci delle banche centrali potrebbe portare. Il potenziale risultato di equivalenza che potrebbe emergere dalla discussione può essere visto come un importante esercizio di implementazione per le discussioni riguardanti il ruolo delle banche centrali nella fornitura di conti di deposito al pubblico in generale.

Si introdurranno, quindi, i blocchi principali del modello. Sono presenti tre periodi indicizzati da $t = 0,1,2$. In ogni periodo, un solo bene può essere usato per il consumo e per l'investimento. L'economia è popolata da consumatori, da banche commerciali e di investimento, e da una banca centrale. È importante, ora, descrivere ogni tipo di operatore economico. I sottoparagrafi 4.2.1 e 4.2.2 riportano la trattazione del modello in modo del tutto analogo all'originale, tranne che per l'introduzione delle banche di investimento nella sottosezione 4.2.2.

4.2.1 I Consumatori

Sono presenti *N* consumatori identici, ognuno dei quali è dotato di un'unità del bene nel periodo 0. La funzione di utilità del singolo consumatore è data da:

$$U(c_1, c_2) = \begin{cases} u(c_1) \ \ con\ probabilità\ \lambda \\ u(c_2) \ \ con\ probabilità\ 1-\lambda \end{cases}$$

dove c_1 indica il consumo nel periodo 1 e c_2 indica il consumo nel periodo 2. In altre parole, un operatore è impaziente se valuta il consumo nel periodo 1 con probabilità λ; allo stesso modo, un operatore è paziente se valuta il consumo nel periodo 2 con probabilità $1 - \lambda$. La funzione di utilità u è strettamente crescente, concava e derivabile in ogni punto.

Questa impostazione ha un'interpretazione in cui gli operatori sono soggetti *ex-ante* a shock idiosincratici di consumo in $t = 1$. Ogni consumatore scopre se è paziente o impaziente nel periodo 1, guadagnando, rispetto alle banche, un'informazione aggiuntiva privata. Questa asimmetria informativa impedisce alle banche di discriminare tra i consumatori.

Infine, il consumatore ha accesso a una tecnologia di stoccaggio che trasporta un'unità del bene dal periodo 0 in un'unità del bene nel periodo 1 e, analogamente, un'unità del bene dal periodo 1 in un'unità del bene nel periodo 2. Questa tecnologia permette al consumatore paziente di ritirare il suo deposito dalla banca nel periodo 1 anche se preferisce consumare nel periodo 2. Questa caratteristica diventerà rilevante quando si parlerà di corse allo sportello.

4.2.2 Le Banche

È presente un gran numero di banche che effettuano investimenti per conto dei consumatori. Le banche hanno accesso a due tipi di tecnologie di investimento: una a breve e una a lungo termine. La tecnologia a breve termine (o attività breve) è una tecnologia a rendimento costante che prende una unità del bene alla data $t = 0{,}1$ e la converte in un'unità del bene alla data $t + 1$. Si può pensare a questa tecnologia come ad un magazzino, come il caveau nel seminterrato di una banca.

La tecnologia a lungo termine (o bene lungo) è una tecnologia priva di rischio a rendimento costante che prende un'unità del bene nel periodo 0 e la trasforma in $R > 1$ unità di bene nel periodo 2. Se la tecnologia a lungo termine viene liquidata prematuramente nel periodo 1, allora questa paga κ unità di bene per ogni unità investita. Si può pensare a questa tecnologia come ad un progetto produttivo che richiede un po' di tempo per dare i suoi frutti e che è soggetto a un costo di liquidazione anticipata.

Sono presenti due tipi di banche: le banche commerciali e le banche d'investimento. Entrambi i tipi si trovano sempre in un luogo centrale. Di seguito, i termini “banchiere" e "banca" sono utilizzati in modo interscambiabile. Le banche commerciali (chiamate anche al dettaglio) offrono contratti di deposito a vista ai consumatori e usano il procedimento per investire in attività brevi e lunghe.

In confronto, le banche d'investimento, pur avendo accesso alla tecnologia di deposito e alle attività lunghe, offrono solo contratti che contribuiscono a profitti non negativi nel periodo 2. In altre parole, le banche d'investimento non forniscono liquidità offrendo depositi a vista ai consumatori. Il cash flow futuro che le banche d'investimento offrono a un partner contrattuale (come la banca centrale) è già determinato in $t = 0$, e il partner contrattuale non può richiedere pagamenti in $t = 1$, come nel caso dei depositi a vista delle banche commerciali. Di conseguenza, poiché il rendimento delle attività lunghe è preponderante rispetto ai rendimenti delle attività corte, i banchieri d'investimento scelgono solo di operare la tecnologia a lungo termine e di massimizzare i profitti del periodo 2.

Nella trattazione si considerano non solo le istituzioni finanziarie, ma anche le banche industriali (storicamente comuni in Europa continentale, Giappone e Corea del Sud) e qualsiasi altro veicolo di investimento, come i fondi pensione, i cui obiettivi sono incentrati sui rendimenti a lungo termine.

4.2.2.1 Il Deposito Bancario

Una banca commerciale offre un contratto di deposito $(\hat{c}_1, \hat{c}_2)$ ai consumatori. Se il consumatore accetta di firmare il contratto, allora è tenuto a depositare un'unità del bene presso la banca nel periodo 0. La banca investe una parte y del bene nella tecnologia a breve termine, e la parte rimanente $1 - y$ è investita nella tecnologia a lungo termine.

La banca promette di pagare $\hat{c}_1$ unità del bene su richiesta del consumatore nel periodo 1 oppure promette il più basso tra l'importo $\hat{c}_2$ e le risorse disponibili per il banchiere, le quali sono equamente divise tra tutti i depositanti rimanenti nel periodo 2. Il banchiere è impegnato a pagare $\hat{c}_1$ unità ai consumatori che arrivano nel periodo 1 utilizzando i rendimenti degli investimenti a breve termine o liquidando i progetti a lungo termine fino all'esaurimento delle risorse. Tutte le risorse rimaste nel periodo 1 sono investite nella

tecnologia di investimento a breve termine. Il banchiere consuma le risorse rimaste nel periodo 2.

Si assume che il consumo del banchiere non possa essere negativo e che i banchieri massimizzino il loro consumo del periodo 2 secondo la loro scelta del contratto di deposito. Infine, si assume anche che i banchieri siano in concorrenza alla Bertrand quando offrono contratti di deposito ai consumatori e, di conseguenza, realizzino profitti nulli.

Si noti che la conclusione del modello, prima dell'introduzione di una banca centrale, avrebbe avuto come risultato la stessa allocazione dell'impostazione standard di Diamond e Dybvig. All'equilibrio, i banchieri non consumerebbero nulla e l'utilità attesa dei consumatori è massimizzata, soggetta ai vincoli di fattibilità derivanti dal problema precedente. Come risultato, l'allocazione di equilibrio sarebbe la soluzione di first-best (anche se soggetta a possibili corse). Ci si riferisce al contratto associato all'allocazione di first-best come (c_1^*, c_2^*).

4.2.3 La Banca Centrale

La banca centrale nel modello proposto è un'istituzione controllata dal governo che ha accesso alla tecnologia di investimento a breve termine, ma non ha alcun accesso all'attività lunga. Tuttavia, la banca centrale può stipulare contratti con le banche d'investimento. Inoltre, questa non può contare su fonti di tassazione indipendenti.

4.2.3.1 Le Proprietà della Banca Centrale

La breve introduzione di cui sopra necessita di una spiegazione più dettagliata. Innanzitutto, come già si è affermato, la banca centrale è un'istituzione controllata dal governo. Questa definizione è importante perché evidenzia chi controlla effettivamente la banca e non chi la possiede. Molte banche centrali hanno strutture di proprietà complesse che sono il prodotto di ricorsi storici e accordi politico-economici (si pensi, ad esempio, alla struttura del Federal Reserve System negli Stati Uniti). Tuttavia, nella pratica, tutte le banche centrali nelle economie avanzate si comportano in modo simile, indipendentemente dalla loro proprietà, a causa delle regole di governance che sono state fissate che le pongono in gran parte sotto il controllo del settore pubblico. Questo è vero

anche se le banche centrali possono godere di indipendenza operativa nel perseguimento di obiettivi come la stabilità dei prezzi stabiliti dal ramo legislativo.

Successivamente, è permesso alla banca centrale di avere accesso alle attività a breve termine. Tutte le banche centrali hanno accesso alle tecnologie di stoccaggio: una semplice visita al caveau dell'oro della Federal Reserve Bank di New York dimostra questo punto. Ampliare tali strutture potrebbe essere costoso, ma, certamente, rientra nelle capacità degli stati moderni.

Inoltre, non è permesso alla banca centrale di avere accesso ad attività a lungo termine. Questa ipotesi rende l'idea di come le banche private abbiano un vantaggio comparativo nel monitorare i prestiti per estrarre il loro pieno rendimento (o il loro valore). È ragionevole assumere che una banca centrale non abbia accesso alle stesse opportunità di investimento delle banche private, in quanto queste ultime hanno sviluppato nel corso di decenni un'esperienza nello screening, nel monitoraggio e nel finanziamento di progetti produttivi. L'ipotesi rende anche l'economia della trattazione più interessante: la banca centrale non può essere un semplice clone di una banca commerciale su grande scala.

Infine, la banca centrale non è sostenuta fiscalmente, sia direttamente che indirettamente attraverso fonti indipendenti di tassazione. In altre parole, la banca centrale ha accesso solo ai beni forniti dai consumatori nel periodo 0 o ai proventi degli investimenti nella tecnologia a breve termine oppure presso le banche di investimento. Al contrario, le banche commerciali non sono tassate da alcun prelievo speciale che potrebbe rendere i loro depositi poco attraenti (un'assicurazione dei depositi equa non viola questa condizione, dal momento che il valore atteso dei depositi non varia).

Quest’ultima ipotesi sarà fondamentale per il prosieguo dell’analisi e, tuttavia, allo stesso tempo, la più fragile. Qualora una banca centrale avesse sostegno fiscale, avrebbe un vantaggio rispetto alle banche commerciali che renderebbe il resto dell'analisi alquanto banale. Allo stesso tempo, le considerazioni politico-economiche sono probabilmente di primo ordine nell'effettiva gestione di una banca centrale aperta a tutti. Molti gruppi politici faranno pressione sulla banca per cambiare le sue politiche di prestito e di assunzione di prestiti in modo da raggiungere i risultati preferiti dal gruppo, anche se questa azione richiede l'appoggio dello Stato. Allo stesso modo, le considerazioni sulla struttura proprietaria delle banche centrali e sul pagamento dei dividendi, di cui si è

discusso sopra, e che sono per lo più irrilevanti al momento, potrebbero tuttavia riemergere.

4.2.3.2 I Depositi nella Banca Centrale

La banca centrale può offrire lo stesso tipo di contratto di deposito (d_1, d_2) sopra descritto ai consumatori e, in questo senso, compete per i depositi con le banche commerciali. In particolare, in cambio di un'unità del bene alla data 0, la banca centrale permette ai depositanti di ritirare d_1 unità nel periodo 1 oppure d_2 unità nel periodo 2.

Dalla precedente discussione è chiaro che la banca centrale è in una posizione svantaggiata per competere con le banche commerciali. Mancando l'accesso alle opportunità di investimento a lungo termine, una banca centrale potrebbe sembrare meno capace di impegnarsi nella trasformazione della liquidità. Si mostrerà che, nonostante questo svantaggio, la banca centrale può ancora competere nel mercato dei depositi al dettaglio stipulando contratti con le banche d'investimento per accedere alla tecnologia a lungo termine. In questo passaggio l'assunzione che una banca centrale non debba essere soggetta a frizioni nel mercato dei depositi all'ingrosso (come la mancanza di informazioni o di competenze per operare in esso) è implicita. Dal momento in cui le banche centrali già partecipano a questo mercato, questa ipotesi è empiricamente plausibile.

Nel periodo 0, tutti i banchieri e la banca centrale giocano un gioco simultaneo, denominato gioco dei depositi a vista, in quanto offrono contratti di deposito sia al dettaglio che all'ingrosso. Dopo aver osservato i contratti pubblicati da tutti i banchieri e dalla banca centrale, i consumatori prendono le loro decisioni riguardo depositare o meno. La banca centrale deposita quindi una parte $1 - x$ di ogni unità depositata con le banche d'investimento, investendo il resto *x* nella tecnologia a breve termine.

Sia ℓ_2 il contratto tra la banca centrale e la banca d'investimento di riferimento. Vale a dire che ℓ_2 descrive le passività reali della banca d'investimento per unità di beni ricevuti dalla banca centrale nel periodo 0. La banca d'investimento privata si impegna a investire tutti i fondi ricevuti dalla banca centrale nell'attività lunga.

Nel periodo 2, la banca d'investimento riceve i proventi dell'investimento nella tecnologia a lungo termine ed effettua, nel secondo periodo, il pagamento ℓ_2 alla banca

centrale per unità depositata da quest'ultima nel periodo 0. Le banche d'investimento offrono contratti ℓ_2 alla banca centrale se questi risultano in profitti non negativi, cioè se

$$\ell_2 \leq R \tag{1}$$

Sia f la frazione di consumatori che depositano presso la banca centrale nel periodo 0. Poiché ogni consumatore deposita un'unità, la banca centrale riceve f unità da tutti i depositanti. Sia α la frazione dei depositanti che decide di prelevare nel periodo 1. I vincoli di bilancio per la banca centrale nei periodi 1 e 2 sono:

$$\alpha d_1 \leq x \tag{2}$$

e

$$(1-\alpha)d_2 \leq \ell_2(1-x) + x - \alpha d_1, \tag{3}$$

rispettivamente.

Si noti che nella descrizione del comportamento della banca centrale, non si sta assumendo una particolare funzione obiettivo (come la massimizzazione del profitto o del benessere sociale) oltre al requisito che la banca centrale soddisfi i suoi vincoli di bilancio. Nella tradizione della finanza pubblica, si descriverà, di seguito, un equilibrio indicizzato dalla scelta del contratto di deposito da parte della banca centrale (indipendentemente da come è determinato) e sarà caratterizzato per una classe di contratti rilevanti.

4.2.4 Il Problema del Consumatore

Viene posta ora l'attenzione sul problema del consumatore. Un consumatore individuale deve decidere se depositare presso la banca centrale, consumando $c_1 = d_1$ al momento del prelievo nel periodo 1, oppure $c_2 = d_2$ nel periodo 2 oppure, in alternativa, consumare con una banca commerciale $c_1 = \hat{c}_1$ al momento del prelievo nel periodo 1 oppure $c_2 = \hat{c}_2$ nel periodo 2. I consumatori scelgono il contratto che fornisce la più alta utilità attesa *ex-ante*. Se entrambi i contratti offrono la stessa utilità, allora una frazione

f sceglierà la banca centrale, e la rimanente sceglierà le banche commerciali. In questo caso, la frazione f è indeterminata.

Per completare la descrizione del comportamento dei consumatori nel periodo 0, è necessario specificare le decisioni di deposito nel periodo iniziale e le strategie di prelievo nel periodo intermedio. Sia h_i la decisione di deposito del consumatore i, dove $h_i = 0$ rappresenta il deposito presso una banca commerciale e $h_i = 1$ rappresenta il deposito presso la banca centrale. Sia h la scelta di deposito nel periodo iniziale.

Una strategia di prelievo per il consumatore i è una variabile σ_i che indica il periodo in cui il consumatore ritira dal sistema bancario. Un consumatore precoce ritira sempre nel periodo intermedio con probabilità uno. Un consumatore ritardatario può scegliere di ritirarsi in anticipo, a seconda delle sue convinzioni sulle azioni degli altri consumatori pazienti. Sia σ il profilo delle strategie di prelievo, e sia σ_{-i} il profilo delle strategie per tutti gli investitori tranne i. Nel periodo 1, il consumatore i seleziona la migliore risposta σ_i nel gioco del prelievo data la sua aspettativa sulle strategie degli altri operatori σ_{-i}.

4.3 L'Equilibrio

Si è ora in grado di definire formalmente un equilibrio per l'economia con una banca centrale. In particolare, viene posta l'attenzione verso gli equilibri simmetrici, dove tutte le banche d'investimento e tutte le banche commerciali usano lo stesso contratto.

Un equilibrio è definito come l'insieme di un contratto ℓ_2 tra la banca centrale e la banca d'investimento di riferimento, di un contratto di deposito a vista $(\hat{c}_1, \hat{c}_2)$ per la banca commerciale di riferimento, di un contratto di deposito a vista (d_1, d_2) per la banca centrale, di decisioni di deposito h nel periodo iniziale, di un profilo strategico σ per il gioco di prelievo nel periodo intermedio, di una frazione α di depositanti che si ritirano nel periodo 1, e infine di una frazione f di consumatori che depositano presso la banca centrale, tale che:

1) Nel periodo 0, dati i contratti $(\hat{c}_1, \hat{c}_2)$ e (d_1, d_2) ogni consumatore i, in modo ottimale, deposita un'unità del bene presso un istituto finanziario selezionando il contratto che gli offre la più alta utilità attesa. La strategia σ è un equilibrio di Nash del gioco del prelievo nel periodo 1.

2) Ogni banca commerciale sceglie il contratto $(\hat{c}_1, \hat{c}_2)$ che massimizza i profitti nel periodo 2, noti (d_1, d_2) .
3) Ogni banca d'investimento offre il contratto ℓ_2, purché soddisfi la condizione (1).
4) I vincoli di budget (2) e (3) mantengono l'uguaglianza per la banca centrale, dato il profilo strategico σ.
5) I prelievi nel periodo 1 soddisfano la relazione $\alpha = 1 - \int_{\{i\in[0,1]:\sigma_i=2} di$
6) La frazione di depositi iniziale f nella banca centrale soddisfa la relazione $f = \int h_i di$

L'economia precedentemente descritta rappresenta un accordo con una banca centrale che non agisce necessariamente come un operatore economico guidato dal proprio interesse. Nell'analisi, la banca centrale compete con le banche private per i depositi dei consumatori e può accedere alla tecnologia a lungo termine contrattando con le banche d'investimento. L'esistenza di un'entità non finalizzata alla massimizzazione nella competizione per i contratti di deposito a vista potrebbe portare le banche private a comportarsi in modo diverso da quello che ci si aspetterebbe da loro con la concorrenza standard di Bertrand. In particolare, la condizione per cui $0 < f < 1$ può verificarsi solo se i consumatori sono indifferenti nel depositare presso la banca centrale o presso una banca commerciale.

Tuttavia, è possibile dimostrare che la banca centrale è in grado di replicare il contratto socialmente ottimale investendo in modo corrispondente nel settore bancario d'investimento. La replicazione del contratto ottimale è possibile per la banca ponendo $x = y^*$, $d_1 = c_1^*$, $d_2 = R(1 - y^*)/1 - \lambda$. Per poter offrire tale contratto, è necessario porre $l_2 = R$, implicando quindi profitti nulli per le banche d'investimento. Le condizioni di uguaglianza sono fattibili in seguito alle condizioni (1), (2), (3) e ponendo $\alpha = \lambda$. Inoltre, il contratto socialmente ottimo è offerto dalle banche commerciali, dalla banca centrale oppure da entrambe. Se entrambe possiedono clienti allora entrambe le banche offrono il contratto ottimale. È bene notare che, qualora fossero solo le banche commerciali ad offrire il contratto ottimale, esse assorbirebbero l'intero mercato dei depositi e quindi $f = 0$. Viceversa, se solo la banca centrale offrisse il contratto ottimale, allora $f = 1$. Se, tuttavia, entrambi i tipi di banche offrissero il contratto ottimale, allora per indifferenza, ogni f è un equilibrio.

Le considerazioni fatte in precedenza mostrano che, poiché una banca centrale è in grado di replicare il contratto socialmente ottimale affidandosi al settore bancario d'investimento, la presenza di una CBDC (o, più in generale, di una banca centrale aperta a tutti) può ancora fornire la stessa trasformazione delle scadenze che le banche commerciali offrono in sua assenza. Inoltre, se il contratto socialmente ottimale è raggiungibile se tutti i depositanti si comportano a seconda della loro tipologia (vale a dire che i consumatori ritirano se e solo se impazienti), allora il contratto socialmente ottimale è effettivamente raggiunto. Questo risultato vale indipendentemente dal fatto che il contratto sia offerto dalla banca commerciale o dalla banca centrale.

Questo risultato di equivalenza conferma alcune delle affermazioni dei sostenitori di una CBDC: in equilibrio, otteniamo ancora l'ammontare socialmente ottimale della trasformazione delle scadenze. Tuttavia, come si è discusso nell'introduzione, questo risultato di equivalenza ha una controparte negativa. Se le condizioni sopra descritte sono infrante, per esempio, perché la banca centrale riceve il sostegno del fisco, le forze competitive che creano la giusta quantità di trasformazione delle scadenze scompaiono e la banca centrale deve procedere con cautela nel decidere come evitare di creare livelli subottimali di trasformazione. Mentre la banca centrale può farlo, nulla nel modello assicura un tale risultato. In particolare è presente il rischio che, in assenza delle forze di bilanciamento della concorrenza, i meccanismi politico-economici possano portare la banca centrale a risultati chiaramente subottimali.

4.4 Il Panico Bancario

Nella sezione precedente è stato raggiunto un risultato di equivalenza fondamentale tra i contratti di deposito delle banche commerciali e delle banche centrali. Tuttavia, i pagamenti descritti nel contratto di deposito diventano fattibili solo se i depositanti si comportano a seconda della loro tipologia. Ma cosa succede se essi non lo fanno?

Il contratto offerto dalla banca centrale non è identico per funzionalità al contratto offerto dalle banche commerciali. Il primo è più rigido, poiché la banca centrale non può richiamare il suo prestito dalla banca d'investimento per liquidarlo anticipatamente. In altre parole, la banca centrale è costretta a operare per raggiungere i rendimenti dell'attività corta e non di più.

In confronto, la banca commerciale ha un controllo diretto sul suo investimento: può servire i depositanti nel periodo intermedio liquidando non solo l'attività corta, ma anche l'attività lunga. Quindi, una volta che i panici bancari sono permessi, in cui i depositanti si comportano come se fossero impazienti e prelevano presto per assicurarsi i loro depositi, la rigidità del contratto della banca centrale ha implicazioni per gli incentivi dei depositanti e i risultati dell'equilibrio.

4.4.1 Il Panico nella Banca Commerciale

Con riferimento al modello di Diamond e Dybvig, si discuterà ora come le banche commerciali siano inclini a competere come se non ci fossero altri operatori economici. Si consideri un individuo che ha depositato presso la banca commerciale. Dalle precedenti considerazioni, è noto che questa banca deve offrire il contratto socialmente efficiente (c_1^*, c_2^*). Si suppone che, in $t = 1$, l'individuo scopra di essere paziente. Poiché la sua tipologia non è osservabile, può comunque agire come se fosse impaziente e decidere di prelevare.

Deciderebbe per tale azione solo se una quantità $\alpha = \lambda$ di depositanti effettuasse un prelievo, quando i payoff sono esattamente come nel suo contratto. Se invece anche i depositanti pazienti prelevassero, vale a dire $\lambda < \alpha \leq 1$, i payoff del rinnovo e del prelievo si discosterebbero dai payoff promessi nel contratto. Questo accade perché la banca commerciale si è impegnata a pagare la cedola a breve termine c_1^* ad ogni depositante che richiede indietro il suo deposito in $t = 1$. Per finanziare i prelievi al di sopra di λ, la banca commerciale ha bisogno di liquidare l'attività a lungo termine, il che riduce i pagamenti verso quei depositanti che hanno deciso di non prelevare.

In una banca commerciale si può verificare panico bancario se la banca è costretta a liquidare i suoi investimenti a lungo e breve termine per soddisfare i prelievi a breve termine. Formalmente, se $\alpha c_1^* > y^* + (1 - y^*)\kappa$, o equivalentemente se

{Panico nella Banca Commerciale} $\{(\alpha - \lambda)c_1^* > (1 - y^*)\kappa\}$ (4)

Nel caso di panico bancario, i depositanti che non hanno prelevato non ricevono nulla, mentre i depositanti che prelevano ricevono il payoff c_1^* solo con una certa probabilità a

causa del razionamento. L'interpretazione è che $\alpha = \lambda$ depositanti si recano presso la banca commerciale per ricevere indietro il loro deposito. Come spiegato sopra, la banca lavora per i depositanti utilizzando attività a breve termine e liquidando attività a lungo termine. Qualora non ci fossero abbastanza attività a lungo termine da liquidare, la banca commerciale sceglierebbe un sottoinsieme casuale di operatori $\frac{y^*+(1-y^*)\kappa}{\alpha c_1^*}$ nella coda a cui è in debito per il pagamento c_1^*. A condizione che non vi sia panico, i payoff dei depositanti sono come nel contratto originale. La matrice di payoff, come mostrato nella Tabella 4.1, è quindi:

Tabella 4.1 – Matrice di payoff

Evento/Azione	Prelievo	Non prelievo
No panico	$u(c_1^*)$	$u\left(\frac{R[(1-y^*)-(\alpha-\lambda)c_1^*/\kappa]}{1-\alpha}\right)$
Panico	$\frac{y^*+(1-y^*)\kappa}{\alpha c_1^*} * u(c_1^*)$	0

In questo modo, si trova una classica complementarità strategica nelle azioni: condizionato da un panico bancario, il payoff del prelievo è maggiore del payoff del non prelievo e, come conseguenza, il prelievo dei depositi è ottimale. Viceversa, se solo pochi consumatori prelevano, allora $\alpha = \lambda$, e quindi il payoff del non prelievo è maggiore, da cui $c_1^* < c_2^*$; così, per un depositante paziente è ottimale non prelevare il suo deposito. Si può riassumere questa idea nella proposizione seguente:
Il gioco del prelievo dei depositanti delle banche commerciali ha due equilibri puri. Un primo equilibrio si trova nel momento in cui tutti i depositanti pazienti decidono di non prelevare il loro deposito, quindi $\alpha = \lambda$, e il contratto socialmente ottimale viene così raggiunto. Ma è presente anche un equilibrio di panico bancario, in cui tutti i depositanti pazienti vanno in panico e prelevano, da cui $\alpha = 1$. In quest'ultimo caso, il contratto socialmente ottimale non viene raggiunto.

4.4.2 Il Panico nella Banca Centrale

Le corse alle banche centrali sono, al contrario, un'entità molto diversa. Durante un panico bancario, la banca centrale non può richiamare il prestito alla banca

d'investimento e può, quindi, servire solo prelievi fino ai rendimenti derivanti dall'attività allo scoperto. In altre parole, il contratto offerto dalla banca centrale non è un contratto di deposito a vista in quanto presenta un fattore di rigidità.

Questo vincolo ha due conseguenze. In primo luogo, i payoff in caso di una corsa alla banca centrale sono diversi da quelli di una corsa alla banca commerciale. Nell'ottimo sociale, la banca centrale investe $y = \lambda c_1^*$ nell'attività breve e il restante $1 - y^*$ nel prestito alla banca d'investimento. Così, la banca centrale non può servire più di una misura y^* di prelievi di denaro, mentre la banca commerciale può servire fino alla misura $y^* + (1 - y^*)\kappa$ finanziata attraverso la liquidazione anticipata dell'attività lunga.

In secondo luogo, il fattore che fa scattare la corsa alla banca centrale differisce dall'evento scatenante di una corsa a una banca commerciale. Una corsa alla banca centrale si verifica se $\alpha c_1^* > y^*$ o, equivalentemente, se:

$$\{\text{Panico nella Banca Centrale}\} \qquad \{\alpha > \lambda\} \tag{5}$$

In caso di panico, la banca centrale può assegnare solo beni reali pari a y^* ad α operatori. Come nel caso della banca commerciale, si assume che i depositanti si rechino presso la banca e ricevano il credito originale di c_1^* unità se e solo se sono sufficientemente in anticipo nella coda, vale a dire con probabilità $\frac{\lambda}{\alpha}$. Poiché la banca centrale non può liquidare l'investimento nel lungo, come vengono gestiti i depositanti rimanenti che non sono stati finora serviti? Ci sono due modi in cui la banca centrale può procedere.

Il primo rimedio che la banca centrale ha a disposizione consiste nel "punire" i depositanti che contribuiscono al panico. Più concretamente, la banca centrale non pagherà più di un ammontare pari a λ a coloro che cercano di prelevare, e tutti i profitti guadagnati in $t = 2$ andranno esclusivamente a coloro che prorogano la decisione. Sotto questo regime, la struttura payoff risultante dissuade un panico dal verificarsi. Per i depositanti pazienti, il non prelievo del deposito è la scelta migliore, e, in equilibrio, solo i depositanti impazienti prelevano. Formalmente, abbiamo la seguente proposizione: Se la banca centrale punisce i depositanti che contribuiscono al panico, allora il gioco del prelievo dei depositanti della banca centrale ha un unico equilibrio. Tutti i depositanti pazienti non prelevano, e solo i depositanti impazienti prelevano. Le corse alla banca

centrale non si verificano ed il contratto socialmente ottimale è sempre raggiunto quando viene offerto.

L'alternativa alla punizione è considerare i depositanti che contribuiscono al panico come se avessero deciso di non prelevare il loro deposito. Ne consegue che il gioco ha un equilibrio unico: tutti gli individui pazienti non prelevano i depositi e solo gli impazienti prelevano. Il panico non avviene e il contratto socialmente ottimo è sempre raggiunto quando offerto.

4.4.3 Il Monopolio dei Depositi

Dalla trattazione e dalle varie considerazioni analizzate finora si arriva alla conclusione che qualora la banca centrale offrisse il contratto socialmente ottimo, allora, indipendentemente dal fatto che punisca i depositanti per aver contribuito ad un panico, attirerà tutti i depositi sul mercato lontano dal settore bancario commerciale.

L'intuizione deriva dal fatto che se il settore bancario commerciale offre il contratto socialmente ottimo per competere con la banca centrale, la banca commerciale non può impedire che si raggiunga l'equilibrio di panico bancario. Allo stesso modo, la banca commerciale non può garantire l'allocazione secondo il contratto ottimale, al contrario della banca centrale.

Tuttavia, poiché i depositanti sanno che il contratto della banca centrale è a prova di panico, questa gode di una sorta di potere di mercato. Qualora decidesse di sfruttare tale potere di mercato, potrebbe offrire un contratto di deposito diverso da quello socialmente ottimale, e ottenere comunque il monopolio di tutti i depositi. Quando la banca centrale si comporta in questo modo, l'economia non raggiunge la quantità migliore di trasformazione delle scadenze. La resistenza delle banche centrali al panico è un'arma a doppio taglio: evita il caos finanziario, ma distrugge le forze competitive che disciplinano le banche centrali che sono aperte a tutti.

Conclusioni

Dall'analisi effettuata e dalle tematiche affrontate in questo lavoro di Tesi, si possono trarre alcune conclusioni in merito a cosa siano effettivamente le criptovalute e come si inseriscono nella concorrenza alle valute tradizionali.

Come punto di partenza, facendo riferimento alla digitalizzazione come forma di cambiamento della moneta in generale e non legata solamente al campo delle criptovalute, si può concludere che la rivoluzione digitale in corso e l'ascesa delle grandi imprese tecnologiche presentano la possibilità di un allontanamento radicale dal modello tradizionale di scambio monetario. La struttura e la tecnologia che sta alla base delle reti digitali possono portare ad una disaggregazione dei ruoli della moneta, creando una concorrenza più feroce tra le valute specializzate. L'associazione delle valute digitali con grandi ecosistemi di piattaforme, d'altra parte, può portare ad una riorganizzazione del denaro in cui i servizi di pagamento sono confezionati con una serie di servizi di dati, incoraggiando la differenziazione ma scoraggiando l'interoperabilità tra le piattaforme. La convertibilità tra strumenti monetari e l'interoperabilità tra piattaforme saranno cruciali per abbassare le barriere al commercio e promuovere la concorrenza. Le valute digitali possono anche causare uno sconvolgimento del sistema monetario internazionale: i paesi che sono socialmente o digitalmente integrati con i territori confinanti potrebbero dover far fronte alla dollarizzazione digitale, e la prevalenza di piattaforme di importanza sistemica potrebbe portare all'emergere di aree di valuta digitale che trascendono i confini nazionali. L'ascesa delle valute digitali avrà implicazioni per il trattamento del denaro privato, la regolamentazione della proprietà dei dati e l'indipendenza delle banche centrali.

Proseguendo nella trattazione, si è passati ad un'analisi più approfondita e dettagliata e ci si è chiesto se le criptovalute potessero essere considerate una forma d'investimento. Nel Capitolo 3 si è affrontato l'argomento utilizzando l'analisi tecnica, la quale ha una lunga e ricca storia nella letteratura accademica, con molti articoli che riportano una redditività significativa nei mercati dei cambi, nei mercati azionari, nelle obbligazioni e

nelle materie prime. Sebbene la redditività riportata del trading tecnico sia diminuita nel tempo, è presente ancora una forte evidenza di come gli investitori prestano attenzione alle regole del trading tecnico e le implementano come parte delle loro strategie di investimento. Si è fornito uno studio sul beneficio dell'impiego di una vasta gamma di regole tecniche di trading nei mercati delle criptovalute. Pertanto, è stata effettuata un'indagine su larga scala della redditività delle stesse regole su cinque delle criptovalute più liquide e redditizie impiegando un gran numero di tecniche di trading. Inoltre, sono stati effettuati anche una serie di test di ipotesi multiple per salvaguardarsi dalla distorsione dei dati.

Sono state utilizzate cinque famiglie di regole tecniche di trading in tutti i mercati delle criptovalute e si è evidenziato come queste abbiano un forte potere predittivo. I rendimenti medi annualizzati per ogni famiglia di regole in ogni mercato sono tutti statisticamente significativi con un livello del 5%, indicando la solidità dei risultati. Si sono riportati anche i costi di transazione di breakeven che, generalmente, mostrano un valore superiore rispetto a quello comunemente visto nelle criptovalute, indicando che i profitti generati dal trading tecnico non vengono eliminati dall'inclusione dei costi di transazione. Inoltre, si è mostrato che anche l'impiego di regole di trading tecnico nelle criptovalute genera misure corrette per il rischio molto più favorevoli rispetto alla semplice strategia buy-and-hold, e può proteggere gli investitori da gravi perdite associate alle valute digitali. Infine, si sono implementate quattro correzioni popolari di test d'ipotesi multiple per proteggersi contro le distorsioni da data-snooping e si è notato che una grande proporzione di regole sono ancora statisticamente significative. Infine, si è dimostrato che le regole tecniche di trading non possono generare rendimenti positivi nel periodo fuori campione per il Bitcoin, ma possono farlo per altre criptovalute. Pertanto, i risultati dimostrano che le regole tecniche di trading hanno un significativo potere predittivo nei mercati delle criptovalute anche dopo aver considerato i test di ipotesi multiple, ma il Bitcoin non offre alcuna prevedibilità nel periodo fuori campione. Infine, affinché la trattazione risultasse completa, nel Capitolo 4 sono state discusse e affrontate le implicazioni di una valuta digitale emessa dalla banca centrale (CBDC), concentrandosi sulla sua potenziale concorrenza con il ruolo tradizionale di trasformazione delle scadenze delle banche commerciali, come nel modello di Diamond e Dybvig. La banca centrale non può investire direttamente in progetti a lungo termine,

ma deve invece fare affidamento sulla conoscenza esperta delle banche d'investimento. Si è derivato un risultato di equivalenza che mostra che l'insieme di allocazioni ottenute con l'intermediazione finanziaria privata saranno ottenute anche con una CBDC, a condizione che la concorrenza con le banche commerciali sia consentita e che i depositanti non si facciano prendere dal panico.

Tuttavia, il risultato di equivalenza ha un importante risvolto da tenere in considerazione. Se la concorrenza delle banche commerciali è ostacolata, la banca centrale deve fare attenzione nelle sue scelte per evitare di creare scompiglio con trasformazione delle scadenze. Inoltre, è stato evidenziato come la rigidità del contratto della banca centrale con le banche d'investimento scoraggi la possibilità di determinare caos. All'equilibrio, i depositanti internalizzano questa caratteristica e depositano esclusivamente presso la banca centrale in modo tale che questa si candidi come un monopolista dei depositi, attirando gli stessi dal settore bancario commerciale. Ma questo potere monopolistico elimina le forze che inducono la banca centrale a fornire la quantità socialmente ottimale di trasformazione delle scadenze.

Bibliografia e sitografia

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Available at https://bitcoin.org/bitcoin.pdf , 2008

[2] Markus K. Brunnermeier, H. James, J.P. Landau, "The Digitalization of Money", Working Paper 26300, National Bureau of Economic Research, USA, 2019

[3] Imran Bashir, "Mastering Blockchain, Distributed ledger technology, decentralization, and smart contracts explained", 2nd Edition, Packt Publishing, 2018

[4] David Lee Kuo Chuen, "Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data", Elsevier Inc., USA, 2015

[5] C. Manasse, G. Baldantoni, "Protocollo E-Cash e RSA", Università degli Studi di Perugia, Facoltà di Scienze Matematiche, Fisiche e Naturali, 2012

[6] J. Fernandez-Villaverde, D. Sanches, L. Schilling, H. Uhlig, "Central Bank Digital Currency: Central Banking for All?", Working Paper 26753, National Bureau of Economic Research, USA, 2020

[7] R. Hudson, A. Urquhart, "Technical trading and cryptocurrencies", Annals of Operations Research, vol. 297, pp. 191-220. ISSN 0254-5330 doi: 10.1007/s10479-019-03357-1, USA, 2021

[8] D. W. Diamond, P. H. Dybvig, "Bank runs, deposit insurance, and liquidity", Journal of Political Economy, vol. 91, pp. 401-419, USA, 1983

[9] Y. Benjamini, Y. Hochberg, "Controlling the false discovery rate: A practical and powerful approach to multiple testing", Journal of the Royal Statistical Society, Series B, vol. 57, pp. 289-300, USA, 1995

[10] Y. Benjamini, D. Yekutieli, "The control of the false discovery rate in multiple testing under dependency", Annals of Statistics, vol. 29, pp. 1165-1188, USA, 2001

[11] W. Brock, J. Lakonishok, B. LeBaron, "Simple technical trading rules and the stochastic properties of stock returns", Journal of Finance, vol. 47, pp. 1731-1764, USA, 1992

[12] A. L. Detzel, H. Liu, J. Strauss, G. Zhou, Y. Zhu, "Bitcoin: Learning, predictability and profitability via technical analysis". Available at SSRN: https://ssrn.com/abstract=3115846, USA, 2018

[13] Y. Han, T. Hu, K. Yang, "Are there exploitable trends in commodity futures prices?", Journal of Banking and Finance, vol. 70, pp. 214-234, USA, 2016

[14] P. H. Hsu, M. P. Taylor, Z. Wang, "Technical trading: Is it still beating the foreign exchange market?", Journal of International Economics, vol. 102, pp. 188-208, USA, 2016

[15] A. Kajtazi, A. Moro, "The role of bitcoin in well diversified portfolios: A comparative global study", International Review of Financial, vol. 61, pp. 143-157, USA, 2019

[16] P. S. Lintilhac, A. Tourin, “Model-based pairs trading in the bitcoin markets”, Quantitative Finance, vol. 17, pp. 703-716, USA, 2017
[17] R. D. McLean, J. Pontiff, “Does academic research destroy stock return predictability?”, Journal of Finance, vol. 71, pp. 5-32, USA, 2016
[18] L. Menkhoff, “The obstinate passion of foreign exchange professionals: Technical analysis”, European Journal of Finance, vol. 145, pp. 936-972, 2007
[19] C. J. Neely, P. Weller, R. Dittmar, “Is technical analysis in the foreign exchange market profitable? A genetic programming approach”, Journal of Financial and Quantitative Analysis, vol. 32, pp. 405-426, 1997
[20] E. Platanakis, A. Urquhart, “Should investors include bitcoin in their portfolios? A portfolio theory approach”. Available at SSRN: https://ssrn.com/abstract=3215321, USA, 2019
[21] I. Psaradellis, J. Laws, A. A. Pantelous, G. Sermpinis, “Performance of technical trading rules: evidence from the crude oil market”, European Journal of Finance, vol. 25, pp. 1793-1815, 2019
[22] D. M. Smith, N. Wang, Y. Wang, E. J. Zychowicz, “Sentiment and the effectiveness of technical analysis: Evidence from the hedge fund industry”, Journal of Financial and Quantitative Analysis, vol. 51, pp. 1991–2013, 2016
[23] R. Sullivan, A. Timmermann, H. White, “Data-snooping, technical trading rule performance, and the bootstrap”, Journal of Finance, vol. 354, pp. 1647–1691, USA, 1999
[24] H. White, “A reality check for data snooping”, Econometrica, vol. 65, pp. 1097–1126, 2000
[25] N. Zarrabi, S. Snaith, J. Coakley, “FX technical trading rules can be profitable sometimes!”, International Review of Financial Analysis, Elsevier, vol. 49, pp. 113-127, 2017
[26] A. Shynkevich, “Performance of technical analysis in growth and small cap segments of the us equity market”, Journal of Banking and Finance, vol. 36, pp. 193–208, 2012
[27] S. Corbet, B. Lucey, A. Urquhart, L. Yarovaya, “Cryptocurrencies as a financial asset: A systematic analysis”, International Review of Financial Analysis, vol. 62, pp. 182–199, 2019
[28] D. Kynaston, “Till Time’s Last Sand: A History of the Bank of England, 1694-2013”, Bloomsbury Publishing, 2017
[29] https://www.bancaditalia.it/
[30] https://en.cryptonomist.ch/2019/08/04/byzantine-generals-bitcoin-solution/
[31] https://www.coindesk.com/
[32] https://www.bitstamp.net/

Ringraziamenti

In primis, desidero ringraziare i miei relatori, la Prof.ssa Laura Rondi e il Prof. Franco Varetto, per avermi dato la possibilità di affrontare un argomento estremamente attuale e per me di grandissimo interesse.

Un grazie di cuore ai miei genitori che cinque anni or sono mi hanno aiutato ad iniziare questo percorso di vita e mi hanno sempre sostenuto dandomi la forza e le motivazioni necessarie, specialmente nei momenti più difficili quando pensavo di non farcela. Non posso inoltre non ringraziare i miei nonni per tutta la saggezza e gli insegnamenti che mi hanno sempre trasmesso con grande amore nel corso degli anni.

Ringrazio poi tutte le persone con cui in questi anni ho condiviso momenti belli e anche delusioni. In particolare, voglio ringraziare Mattia, che conosco ormai da più di dieci anni e con cui ho condiviso i migliori (ed anche i peggiori) momenti della mia vita e che, dopo tutto questo tempo, rappresenta la prima persona alla quale mi rivolgo quando ho bisogno di aiuto.

Voglio ringraziare Matteo, conosciuto durante il mio percorso universitario con cui ho condiviso due anni di studi durante i quali è diventato un amico sempre pronto ad ascoltarmi e ad aiutarmi quando ne ho avuto bisogno.

Voglio infine ringraziare Federico, mio coinquilino da ormai più di tre anni, per aver sempre sopportato i miei sfoghi quando le cose andavano male, ma soprattutto per aver condiviso insieme a me tutte le gioie di questa bellissima esperienza.