LUISS

Dipartimento
di Impresa e Management

Cattedra di Macroeconomia

La moneta digitale e le sfide che Bitcoin sta lanciando alle banche centrali

Prof. Alessandro Pandimiglio
RELATORE

Giacomo Coppari 246971
CANDIDATO

Anno Accademico 2021/2022

Introduzione

Il 1° novembre 2008, un programmatore di computer noto con lo pseudonimo di Satoshi Nakamoto inviò una mail ad una mailing list di crittografia, annunciando che era riuscito a creare "un nuovo sistema di pagamento elettronico completamente *peer-to-peer,* che non aveva bisogno di fare affidamento su terzi per il proprio funzionamento". Egli, successivamente, copiò l'estratto di un documento dove veniva illustrato il design del sistema e lo affiancò ad un link per poterlo vedere anche sul web. In poche parole, Bitcoin ha offerto una rete di pagamento con la propria valuta nativa ed ha utilizzato un metodo sofisticato per i membri che permette di verificare tutte le transazioni senza doversi affidare a nessun'altro membro della rete. Tale criptovaluta è stata emessa ad un tasso di interesse predeterminato con l'obiettivo di premiare i membri che spendono la loro potenza informatica di elaborazione per verificare le transazioni, fornendo così una sorta di ricompensa per il loro lavoro. La cosa sorprendente di questa invenzione era che, contrariamente a molti altri tentativi di creazione di una valuta digitale, ha funzionato davvero. Sebbene fosse un design intelligente e ben fatto, non ci si sarebbe mai aspettato che un esperimento così bizzarro sarebbe mai interessato a gente estranea ai circoli dei fanatici di crittografia, ed infatti per mesi è stato così. Inizialmente, solamente qualche decina di utenti in tutto il mondo si univano alla rete, si dedicavano al *mining* e si inviavano reciprocamente tali monete, le quali iniziarono nel frattempo ad acquisire lo status di "oggetti da collezione", anche se in formato digitale. Il tutto cambiò quando nell'Ottobre del 2009, un exchange, ormai defunto, presente sul web conosciuto come "New Liberty Standard" convertì 5.050 bitcoins per $5.02, ad un prezzo di circa $1 per 1.006 bitcoins, registrando così il primo acquisto di un bitcoin con valuta legale. Il valore fu calcolato misurando il costo dell'elettricità necessaria per produrre un bitcoin. In termini economici, questo fatto è stato di gran lunga il più significativo nella vita di Bitcoin: la criptovaluta cessava ufficialmente di essere un gioco digitale utilizzato solamente da una ristretta comunità di programmatori, ed era diventato un vero e proprio bene di mercato, esprimibile per mezzo di un prezzo, indicando che qualcuno da una qualsiasi parte del mondo aveva rilasciato un giudizio positivo dello stesso. Il 22 maggio 2010, qualcun altro pagò 10.000 bitcoins per comprare due tranci di pizza per un valore totale di $25; era la prima volta che bitcoin fu usato come mezzo di scambio. La criptovaluta aveva avuto bisogno di sette mesi per poter passare dall'essere un bene di mercato ad essere un mezzo di scambio. Da allora, crebbero a ritmi elevati sia il numero di transazioni e di utenti che si univano alla rete di pagamento, sia la potenza elaborativa necessaria per produrre tale valuta digitale, mentre il suo valore è aumentato nel tempo fino ad arrivare a $7.000 per bitcoin verso fine novembre 2017. In altre parole, negli otto anni in cui è stato un bene di mercato, un bitcoin ha visto il suo valore apprezzarsi di circa il 793,513,944%, dal suo prezzo iniziale di $0,000994 al prezzo di $7.000 registrato nel Novembre 2017. Dopo quasi quattordici anni, è chiaro che tale invenzione non è più solamente un gioco online ma una tecnologia che ha superato il test di mercato

ed è utilizzato ai giorni nostri da molte persone per scopi reali, con il proprio tasso di cambio regolarmente riportato in TV, nei giornali e nei siti internet, insieme a quello delle principali valute nazionali. Bitcoin può essere meglio identificato come un software che permette di trasferire valore per mezzo di una valuta immune all'inflazione inattesa, e che non ha bisogno di fare affidamento su terzi. In altre parole, Bitcoin automatizza le funzioni di una banca centrale e le rende prevedibili e virtualmente immutabili programmandole in codice decentralizzato tra migliaia di utenti presenti nella rete, dei quali nessuno può modificarne il codice senza il consenso degli altri. Questo rende Bitcoin il primo esempio operativo dimostrabilmente affidabile di *digital hard money*. Mentre Bitcoin è una invenzione dell'era digitale, i problemi che si pone di risolvere, come fornire una forma di denaro che è direttamente sotto il controllo del suo proprietario e suscettibile di mantenere il suo valore nel lungo periodo, sono tanto antichi come la società umana stessa. Il valore di Bitcoin rimarrà probabilmente volatile per ancora molto tempo, e la stessa rete digitale potrebbe avere successo oppure fallire per qualsiasi ragione; inoltre, l'utilizzo del token richiede competenze tecniche e comporta rischi che lo rendono inadatto per molte persone. Solo dopo aver ottenuta una confermata comprensione ed aver effettuato una ricerca approfondita sugli aspetti operativi pratici della proprietà e dello *storing* di bitcoin, si potrebbe pensare di detenere valore per mezzo di questa criptovaluta. Nel primo capitolo di questo elaborato verranno presentate le principali caratteristiche della moneta, l'inflazione monetaria e il ruolo delle banche centrali all'interno del sistema monetario, con lo scopo di fare un'analisi approfondita del funzionamento e del controllo della maggior parte delle valute nazionali. Nel secondo capitolo verrà illustrato invece Bitcoin in senso stretto, trattando il suo funzionamento ed utilizzo all'interno della Blockchain. Verranno poi spiegati nel dettaglio il procedimento di conferma delle transazioni, il *mining*, la Blockchain e l'impatto ambientale di Bitcoin, nonché i suoi principali vantaggi. Saranno poi prese in considerazione ed allo stesso tempo sdoganate le principali perplessità riguardanti Bitcoin e le valute digitali in generale. Nel terzo ed ultimo capitolo verranno poi menzionate e analizzate le principali *alternative coins*, soffermando la trattazione su alcune di esse che in futuro potranno dare filo da torcere allo stesso Bitcoin.

Capitolo1: La moneta

1.1 Le caratteristiche fondamentali della moneta

Il modo più semplice per le persone di scambiare valore consiste nello scambiarsi reciprocamente beni dotati di valore intrinseco. Questo processo di scambio diretto prende il nome di "baratto", il

quale però può essere realmente esercitato solamente in piccole comunità dove vi è una netta scarsità di beni e servizi prodotti. In una ipotetica economia chiusa con una decina di individui isolata dal mondo esterno, non sarebbe conveniente promuovere la specializzazione e il commercio, e dunque sarebbe possibile per gli individui impegnarsi ciascuno nel produrre degli elementi essenziali basilari per la sopravvivenza, e successivamente scambiarseli direttamente tra di loro. Il baratto è sempre esistito nella società umana ed è tutt'oggi praticato in diverse parti del mondo, ma è altamente impraticabile e rimane in uso solo in circostanze eccezionali, di solito coinvolgendo individui con una certa familiarità gli uni con gli altri. In un'economia più sofisticata e più ampia, la convenienza per gli individui si sposta nello specializzarsi nella produzione di più beni, per poi scambiarli successivamente con molte altre persone con le quali non hanno un rapporto personale, estranei con i quali sarebbe impraticabile mantenere un conteggio continuo dei beni, servizi e favori.

Più grande è il mercato, maggiori sono le opportunità di specializzazione e di scambio, ma aumenta allo stesso modo il problema della *doppia coincidenza dei bisogni*: ciò che si vuole acquistare potrebbe essere prodotto da qualcuno che non necessita ciò che si ha da offrire.[1] Tale problema è più profondo di quello che si pensa perché presenta tre diverse sfaccettature.

Innanzitutto, vi è la mancanza della doppia coincidenza di valore: quello che si vuole acquistare potrebbe non essere uguale in valore a quello che si possiede e si intende scambiare, e dividere uno di tali beni in parti più piccole potrebbe avere scarsi risvolti pratici. In secondo luogo, vi è la mancanza della doppia coincidenza dei tempi: ciò che si vuole vendere potrebbe essere deperibile mentre quello che si vuole comprare potrebbe essere al contrario più durevole e prezioso, il che rende difficile accumulare una certa quantità del primo al fine di poterla scambiare per il secondo.[2] Infine, vi è la mancanza della doppia coincidenza dei luoghi: si potrebbe voler vendere una casa per poterne acquistare un'altra in un luogo diverso, e la maggior parte delle case non sono trasportabili.[3]

Questi tre problemi rendono i meccanismi di scambio diretto altamente impraticabili e fanno crescere nelle persone il bisogno alla messa a punto di un sistema di scambi alternativo ai fini del soddisfacimento dei loro bisogni di carattere economico.

L'unico modo per aggirare questo problema è attraverso la messa a punto di meccanismi di scambio indiretto: si cerca di trovare il bene desiderato da un determinato individuo, e successivamente si cerca qualcuno che possegga tale bene e che abbia intenzione di scambiarlo con noi per quello che abbiamo da offrire. Tale bene intermediario prende il nome di "mezzo di scambio", e, mentre qualsiasi bene inizialmente potrebbe svolgere tale funzione, man mano che la portata e le dimensioni

[1] N. Gregory Mankiw, Mark P. Taylor (2019). Macroeconomia
[2] "Economia monetaria e moneta"; estratto di un PDF messo a disposizione dall'Università di Macerata
[3] Saifedean Ammous (2018). The Bitcoin Standard

dell'economia crescono diventa impossibile per le persone mettersi costantemente alla ricerca dei beni che le loro controparti stanno cercando, effettuando così molteplici transazioni allo scopo di effettuare l'unica transazione di loro interesse. Una soluzione molto più efficiente è stata poi adottata nel corso degli anni: la messa a punto di un bene globalmente accettato come *mezzo di scambio* che prende il nome di "moneta". A tal proposito, è bene fare una distinzione tra il termine "denaro" e "moneta", in quanto con il primo si intende identificare l'ammontare di circolante collettivamente accettato nelle transazioni di mercato, mentre con il secondo si fa riferimento al circolante direttamente emesso dallo Stato o dagli enti pubblici, il quale può rientrare nella categoria del denaro solamente nel caso in cui venga riconosciuto e accettato come mezzo di scambio.[4] Essere un mezzo di scambio è la funzione per eccellenza che definisce la moneta. In altre parole, essa rappresenta un bene che viene acquistato per non essere consumato e per non essere impiegato nella produzione di altri beni, ma principalmente per essere scambiato con gli altri beni.

La commerciabilità di un bene si misura con riferimento alla sua capacità di mantenere il suo valore nel tempo, permettendo al possessore di immagazzinare ricchezza in esso, la quale rappresenta la seconda funzione della moneta: *riserva di valore*. Affinché un bene mantenga il proprio potere di acquisto nel tempo, esso deve essere immune alla putrefazione, alla corrosione e agli altri tipi di deterioramento.[5] L'integrità fisica nel tempo, tuttavia, è una condizione necessaria ma non sufficiente per il mantenimento del potere di acquisto, in quanto può accadere che un bene perda il suo valore significativamente anche se la sua condizione fisica rimane invariata.

Affinché un determinato bene mantenga il suo valore è anche necessario che l'offerta di mercato del bene stesso non aumenti drasticamente durante il periodo in cui il detentore lo possiede.[6]

Inoltre, la collettiva accettazione di un mezzo di scambio consente che tutti i prezzi vengano espressi nei suoi termini, il che gli consente di svolgere la terza funzione della moneta: l'*unità di conto*. In un'economia senza mezzo di scambio riconosciuto, ogni bene dovrà essere prezzato sulla base dei prezzi di tutti gli altri beni, portando così alla presenza di una molteplicità di prezzi che renderebbero i calcoli economici estremamente difficili. In un'economia con un mezzo di scambio riconosciuto, invece, i prezzi di tutte le merci sono espressi in termini della stessa unità di conto. In queste società la moneta serve come un metro con cui misurare il valore interpersonale, premia i produttori nella misura in cui contribuiscono a creare valore per gli altri e indica ai consumatori quanto devono pagare per ottenere i beni desiderati. Solo con un mezzo di scambio uniforme che

[4] "Moneta", da Wikipedia, l'enciclopedia libera
[5] "Riserva di valore" da Wikipedia, l'enciclopedia libera
[6] Saifedean Ammous (2018). The Bitcoin Standard

agisce come unità di conto vengono resi possibili i complessi calcoli economici, e con essi nascono la possibilità di specializzarsi in compiti complessi, l'accumulazione di capitale e i mercati globali.[7]

Il funzionamento di un'economia di mercato dipende dai prezzi, i quali per essere precisi devono dipendere da un mezzo di scambio comune che rifletta l'effettiva scarsità di beni diversi. Avere un unico mezzo di scambio permette alle dimensioni dell'economia di crescere tanto quanto cresceranno il numero di individui disposti ad utilizzare quel mezzo di scambio. Maggiori sono le dimensioni dell'economia, maggiori saranno le opportunità di guadagno dallo scambio e di specializzazione.[8]

In una piccola e primitiva economia, la struttura di produzione del pesce era caratterizzata da individui che si recavano alla riva per pescare il pesce a mani nude, e l'intero processo richiedeva all'incirca poche ore per essere terminato. Con la crescita dell'economia, vennero utilizzati beni strumentali e strumenti più sofisticati, e la produzione di tali strumenti allungò notevolmente la durata del processo produttivo, aumentando allo stesso tempo la sua produttività. Nel mondo moderno, i pesci vengono catturati con barche altamente sofisticate che impiegano anni per essere costruite e che hanno una vita utile che può durare decenni. Queste barche possono navigare per mari che barche più piccole non possono raggiungere, e dunque pescare esemplari di pesci che altrimenti non sarebbero disponibili.

Tali barche possono inoltre sfidare il maltempo e continuare la pesca anche in condizioni poco favorevoli, a differenza di tutte le altre a minor intensità di capitale, le quali, al verificarsi di tali eventi, sarebbero costrette a ritornare in porto.

Poiché l'accumulazione di capitale ha allungato il processo produttivo, quest'ultimo ha visto aumentare la produttività per unità di lavoro ed inoltre è stata resa possibile la produzione di determinati prodotti che non furono mai possibili per l'economia primitiva, la quale si serviva degli strumenti base e non vi era alcuna accumulazione di capitale. Niente di tutto questo sarebbe stato possibile senza la moneta a svolgere i ruoli di mezzo di scambio per consentire la specializzazione, riserva di valore per creare orientamento al futuro e per incentivare gli individui a indirizzare le risorse in loro possesso all'investimento anziché al consumo, ed unità di conto per consentire il calcolo economico di utili e perdite.[9]

La storia dell'evoluzione della moneta ha visto vari beni giocare il ruolo di quest'ultima, con vari gradi di solidità e resistenza, in base alle disponibilità tecnologiche di ogni epoca. Dalle conchiglie al sale, al bestiame, all'argento, all'oro, alla moneta governativa sostenuta dall'oro fino ad arrivare all'uso quasi universale della moneta a corso legale fornita dal governo. Ogni passo del progresso

[7] Palermo, L. "Sulla teoria e sulla funzione della moneta nel XIV secolo" – OpenEdition journals
[8] Ibidem
[9] Saifedean Ammous (2018). The Bitcoin Standard

tecnologico ci ha permesso di utilizzare una nuova forma di moneta con vantaggi aggiuntivi ma, allo stesso tempo, portatrice di nuove insidie.[10]

1.1.1 Hard Money and Easy Money

Con il termine *hard money* ci si riferisce genericamente ad una qualsiasi moneta che sia costituita o direttamente sostenuta da un metallo prezioso come l'oro o l'argento, mentre con il termine *easy money* si intendono tutte le monete che non presentano tale caratteristica.[11] Le monete "forti" mantengono un valore di mercato stabile rispetto ai beni e ai servizi reali ed un forte tasso di cambio rispetto alle altre valute. Grazie al loro valore intrinseco e alla loro stabilità nei mercati dei beni e nei mercati finanziari, questa tipologia di moneta rispetta tutte le caratteristiche fondamentali sopra descritte: unità di conto, riserva di valore e mezzo di scambio; a differenza delle monete "deboli" che, invece, hanno un valore più volatile. In sostanza, l'uso di una moneta forte comporta costi di transazione e rischi inferiori rispetto all'utilizzo di una moneta debole.[12]

Possiamo capire la potenza di una moneta attraverso la comprensione di due diverse quantità relative alla fornitura di un bene: lo *stock*, che si riferisce alla sua fornitura esistente formata da tutto ciò che è stato prodotto in passato al netto di tutto ciò che invece è stato consumato o distrutto; e il flusso, che rappresenta la produzione extra che verrà prodotta nel periodo successivo. Il rapporto tra stock e flusso è un indicatore affidabile della potenza di un bene come la moneta, e di quanto esso sia in grado di svolgere tale ruolo. Qualora il rapporto stock/flow dovesse risultare basso, ciò significherebbe che l'offerta del bene in questione può essere aumentata smisuratamente nel momento in cui gli individui cominciano ad utilizzarlo come riserva di valore.

Un bene del genere non sarebbe in grado di mantenere il proprio valore dal momento in cui viene utilizzato come riserva di valore. Maggiore risulterà tale rapporto, maggiore sarà anche la probabilità che il bene in questione mantenga inalterato nel tempo il proprio valore e il proprio potere di acquisto.[13] Se gli individui scegliessero una moneta forte con un rapporto stock/flow elevato come riserva di valore, il loro acquisto per conservarla aumenterebbe la domanda della stessa, provocando un aumento del suo prezzo che incoraggerebbe i suoi produttori a produrne di più. Ma poiché il flusso è relativamente basso se comparato con l'offerta esistente, persino un aumento vertiginoso della produzione sarebbe improbabile che provochi una significativa diminuzione del valore. D'altro canto, se gli individui decidessero di conservare la propria ricchezza in denaro debole, con un

[10] Ibidem
[11] Corporate Finance Institute, "Hard Money – Overview, Pros and Cons"
[12] Hayes, Adam "Hard Money" - Investopedia
[13] Antal Fekete (1997). Whither Gold?

basso rapporto stock-to-flow, sarebbe futile per i produttori di questo bene crearne grandissime quantità in quanto causerebbero una diminuzione del suo valore, diminuendone il prezzo, che a sua volta causerebbe l'erosione della ricchezza dei risparmiatori e la distruzione del potere di acquisto dello stesso bene.[14]

Questa situazione prende il nome di "trappola della moneta debole": qualsiasi cosa se usata come riserva di valore avrà la sua offerta aumentata, e tutto ciò la cui offerta può essere facilmente aumentata distruggerà la ricchezza di coloro che l'hanno usata come riserva di valore.[15] Il corollario di questa trappola è che tutto ciò che viene usato come moneta avrà un meccanismo naturale o artificiale che restringe il nuovo flusso del bene nel mercato, mantenendone il valore nel tempo. Ne consegue, quindi, che affinché qualcosa possa assumere un ruolo monetario, è necessario che sia costoso da produrre, altrimenti la tentazione di "fare soldi su ciò che costa poco" distruggerà la ricchezza dei risparmiatori e con essa l'incentivo a risparmiare in tale mezzo di scambio. Qualora uno sviluppo naturale, tecnologico o politico dovesse portare ad un rapido aumento dell'offerta di un bene monetario, quest'ultimo perderebbe il suo status monetario e sarebbe sostituito da altri mezzi di scambio più affidabili con un rapporto stock-to-flow più elevato. Le conchiglie venivano usate come moneta quando erano difficili da trovare, mentre le sigarette sfuse vengono utilizzate tutt'ora come moneta nelle carceri in quanto difficili da procurare e da produrre, e con le valute nazionali, più basso è il tasso di aumento dell'offerta, più probabilmente la valuta verrà detenuta dai singoli e manterrà il suo valore nel tempo.

Quando la tecnologia moderna semplificò l'importazione e la raccolta delle conchiglie, le società che le utilizzavano sono passate al metallo o al cartamoneta, e quando il governo aumenta l'offerta di queste, i cittadini cominciano a detenere valute straniere, oro o altri strumenti monetari più affidabili.

Purtroppo, il Novecento ci ha fornito un gran numero di tragici esempi, in particolare riguardanti i paesi in via di sviluppo. I sistemi monetari che sono sopravvissuti più a lungo sono quelli che presentavano meccanismi di gran lunga più affidabili per limitare la crescita della loro offerta; in altre parole, si basavano su monete forti. Mentre gli individui sono generalmente liberi di utilizzare qualsiasi cosa vogliano come mezzo di scambio, la realtà è che nel tempo, quelli che usano una moneta forte trarranno maggiori benefici in quanto l'inevitabile aumento dell'offerta di tale mezzo di scambio risulterà in una diminuzione insignificante del valore dello stesso. Quelli che scelgono una moneta debole, invece, vedranno quest'ultima perdere di valore al crescere graduale della sua offerta, che porterà inoltre una riduzione del suo valore di mercato. Sia attraverso il calcolo razionale

[14] Carlo Clerici. "Il concetto di scarsità nella determinazione del valore di Bitcoin". In particolare, viene affermato che Saifedean Ammous è stato il primo a parlare di scarsità in termini di rapporto *stock-to-flow*
[15] Parrado C. "Easy Money Trap", CreateGlobalFuture.com

prospettico, sia grazie alle dure lezioni retrospettive della realtà, la maggior parte della ricchezza e della quantità di moneta sarà concentrata su chi sceglie la moneta più forte e più commerciabile.

Ma la potenza e la vendibilità delle merci stesse rappresentano un qualcosa che non è statico nel tempo. Poiché le capacità tecnologiche delle diverse società ed epoche che si sono susseguite nel corso del tempo sono man mano cambiate, lo stesso si può dire della "potenza"[16] delle varie tipologie di moneta, e con essa la loro commerciabilità.[17] In realtà, la scelta su cosa rende alcune forme di moneta migliori delle altre è sempre stata determinata dalle realtà tecnologiche delle diverse società, che modellano la vendibilità di beni diversi.

Quindi, gli economisti austriaci sono raramente dogmatici o oggettivisti nella loro definizione di moneta solida, definendola non come un bene o una merce specifica, ma come quella particolare moneta che risulti liberamente preferita sul mercato dagli individui che la utilizzano come mezzo di scambio, e non dalle autorità coercitive che impongono una tale decisione; e il cui valore è determinato attraverso le interazioni e gli scambi sul mercato, e non attraverso un'imposizione governativa.[18] La concorrenza monetaria all'interno del mercato libero è incredibilmente efficace nel produrre moneta solida, in quanto permette ai detentori della stessa di poter mantenere una notevole ricchezza nel corso del tempo. Tutte le implicazioni individuali e sociali della moneta forte e di quella debole sono molto più profonde della mera perdita o guadagno finanziario.

Gli individui che decideranno di detenere la propria ricchezza sotto forma di una buona riserva di valore saranno in grado di pianificare il futuro in modo più efficiente rispetto a coloro che possiedono una scarsa riserva di valore.

La solidità dei mezzi monetari, in termini di capacità di detenere valore nel tempo, è un fattore determinante di quanto gli individui valorizzino il presente anziché il futuro, ossia la loro preferenza temporale. Al di là del rapporto stock-to-flow, un altro aspetto importante della commerciabilità di un mezzo monetario è rappresentato dalla sua accettabilità da parte degli altri individui. Più persone accettano un mezzo monetario, più esso diventa liquido e più è probabile che venga venduto e comprato senza troppe perdite. In contesti sociali con molte interazioni *peer-to-peer*, come dimostrano i protocolli di elaborazione, è naturale che emergano alcuni standard per dominare lo scambio, perché i guadagni derivanti dall'adesione ad una rete crescono in modo esponenziale al crescere delle dimensioni della rete stessa.[19] Allo stesso modo, Facebook e una manciata di altri social

[16] Con il termine "potenza" riferito ad una moneta, si richiama il concetto di *hard money* sopra menzionato e descritto
[17] Saifedean Ammous (2018). The Bitcoin Standard
[18] Joseph Salerno (Ludwig von Mises Institute, 2010). Money: Sound and Unsound
[19] Bob Mason, "Come funziona il mining di Criptovalute? Cosa è l'Hashrate?"

media occupano una posizione dominante sul mercato, mentre centinaia di altre piattaforme anche similari che sono state promosse e successivamente create non hanno avuto la stessa fortuna.

1.2 L'inflazione monetaria

Nelle moderne economie di mercato, i prezzi dei beni e dei servizi vengono espressi per mezzo di un valore che può subire variazioni in un qualsiasi momento. Si ha inflazione quando si registra un aumento prolungato del livello medio dei prezzi, che provoca a sua volta una diminuzione del valore della moneta.[20] Nel linguaggio economico, inoltre, si è soliti effettuare una distinzione tra tasso di interesse nominale e tasso di interesse reale: il primo fa riferimento al tasso corrisposto dalla banca, mentre il secondo si riferisce all'incremento del potere di acquisto. Tali tassi possono essere messi in relazione tra di loro mediante una semplice scrittura che prende il nome di "equazione di Fisher"[21]:

$$i = r + \pi$$

Dove "i" rappresenta il tasso di interesse nominale, "r" indica il tasso di interesse reale, mentre "π" si riferisce al tasso di inflazione.

In accordo con tale equazione, se la banca centrale decidesse di aumentare l'offerta di moneta, ciò provocherebbe un aumento del tasso di interesse nominale che causerebbe a sua volta un aumento del tasso di inflazione. L'inflazione, infatti, genere una discrepanza tra rendimenti nominali e rendimenti reali, ed allo stesso tempo comporta determinati costi, che si differenziano a seconda del fatto che l'inflazione fosse attesa oppure no.[22]

I costi dell'inflazione attesa sono essenzialmente di tre tipi: i *costi di listino,* in quanto le imprese dovranno adeguare i loro listini dei prezzi a causa del cambiamento del livello dei prezzi; il *costo delle suole,* che si riferisce al tempo perso dagli individui per recarsi in banca più volte per effettuare prelievi di contanti; i *costi scaturenti dalla normativa tributaria*: dato che le imposte sul reddito delle persone fisiche sono progressive e procedono per scaglioni, è possibile che l'inflazione determini un "salto" del reddito nominale ad uno scaglione superiore senza che vi sia un contestuale aumento del reddito reale.[23]

L'inflazione inattesa, invece, produce costi ed effetti ben più gravi in quanto ridistribuisce arbitrariamente la ricchezza tra gli individui. Tali costi sono diversi a seconda del fatto che l'inflazione inattesa venga sottostimata o sovrastimata. Nel primo caso, il rendimento ex post delle

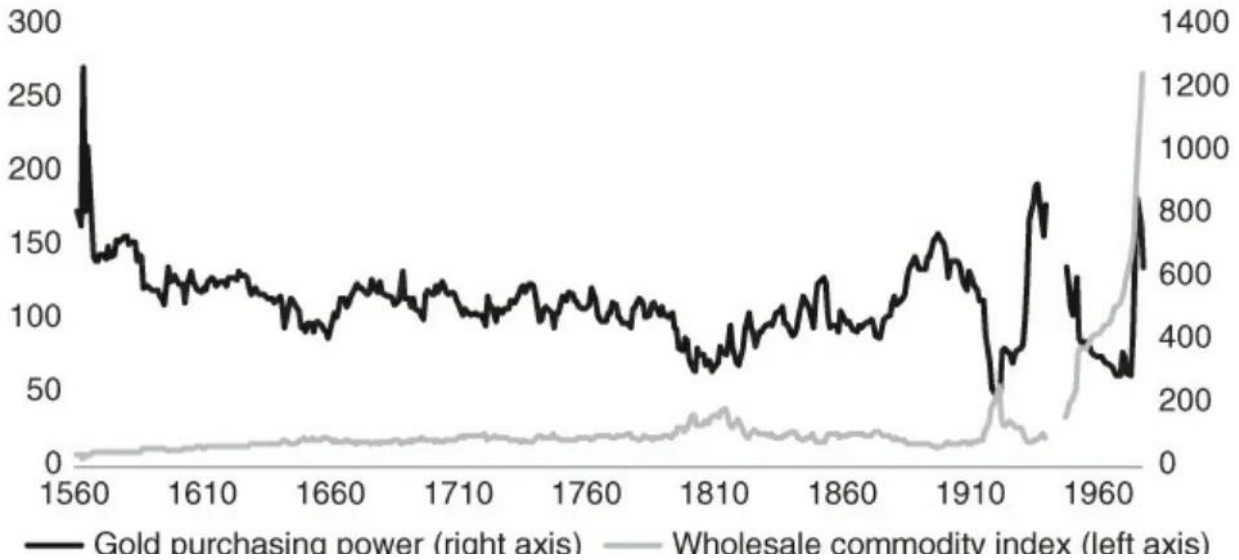
[20] "Cos'è l'inflazione?", Banca Centrale Europea
[21] "Equazione di Fisher", Irving Fisher
[22] Mankiw N. G., Taylor M. P. (2019). Macroeconomia
[23] Ibidem

obbligazioni risulterà minore del rendimento ex ante, comportando un vantaggio inaspettato per i debitori, i quali dovranno ripagare un debito con una moneta presentante un valore minore di quello atteso. Nel secondo caso, gli effetti saranno specularmente opposti a quelli appena citati, in quanto il vantaggio inaspettato si verificherà a favore dei creditori. L'inflazione inattesa danneggia anche coloro che percepiscono un reddito fisso, come i pensionati, il quale viene spesso stabilito in termini nominali.[24]

L'iperinflazione, a sua volta, produce costi ben più gravi per l'intera economia: il costo delle suole diventa intollerabile e i costi di listino diventano elevatissimi. Oltre a ciò, i prezzi relativi cessano di riflettere l'effettiva scarsità dei beni e, per quanto riguarda il sistema tributario, anche un brevissimo ritardo nel pagamento riduce drasticamente la portata del gettito fiscale. Con il tempo, la moneta perderà sempre più valore e, nei casi più estremi, verrà abbandonata comportando un ritorno al baratto. I fenomeni di iperinflazione sono dovuti ad un'eccessiva crescita dell'offerta di moneta: nel momento in cui lo Stato non dispone di entrate sufficienti per coprire la spesa pubblica, comincia a stampare moneta facendo lievitare i prezzi, e portando così a fenomeni di questo genere.[25]

Roy Jastram ha effettuato uno studio sistematico del potere d'acquisto dell'oro, basandosi sul più ampio set di dati disponibili.[26] Osservando alcuni dati inglesi prodottisi a partire dal 1560 fino ad arrivare al 1976 con lo scopo di analizzare le variazioni del potere d'acquisto dell'oro, Jastram notò un calo generale durante i primi 140 anni, per poi stabilizzarsi nel periodo che va dal 1700 al 1914, quando la Gran Bretagna uscì dal gold standard. Per più di due secoli durante i quali la Gran Bretagna ha usato principalmente l'oro come moneta, il suo potere d'acquisto è rimasto relativamente costante, così come il prezzo delle materie prime all'ingrosso (vedi immagine[27])

[24] Ibidem
[25] Ibidem
[26] Roy Jastram (2009). The Golden Constant: The English and American Experience
[27] Roy Jastram (2009). The Golden Constant: The English and American Experience



Per quanto riguarda l'iperinflazione invece, l'esempio di gran lunga più significativo è quello riguardante il *pengö* ungherese. L'Ungheria, infatti, uscì in modo disastroso dalla Seconda Guerra Mondiale, con il 40% delle proprie infrastrutture e del proprio capitale completamente distrutti. Inoltre, durante la guerra, il debito pubblico era cresciuto esponenzialmente per supportare lo sforzo bellico e l'alleanza con i tedeschi. Nel dopoguerra furono imposte da parte dei sovietici ingenti riparazioni di guerra, le quali variavano tra il 25% e il 50% del PIL. Inoltre, i sovietici diedero indicazione di ricorrere al signoraggio in maniera massiccia per poter pagare la spesa pubblica. I dirigenti provarono ad avvisare i sovietici circa i possibili danni che una decisione del genere avrebbe potuto portare, ma questi ultimi continuarono nella propria strada, forse con l'obiettivo collaterale di distruggere proprio una classe sociale vista come base del capitalismo.[28]

Fu così che si arrivò a registrare il tasso di inflazione più elevato mai registrato nella storia. La moneta perse di valore e i prezzi cominciarono a salire in modo esponenziale, impiegando all'incirca 15 ore per raddoppiare, in confronto ai 3,7 giorni necessari per il raddoppio del valore del *papiermark* durante l'iperinflazione tedesca, avvenuta subito dopo la Prima Guerra Mondiale.[29] La salita fuori controllo dei prezzi obbligò, a sua volta, l'emissione di tagli di banconote sempre più elevati, raggiungendo il massimo con la stampa di un biglietto da 1.000.000.000.000.000.000.000 (10^{21}) *pengö*.

[28] Fabio Lugano (2013). "Iperinflazione: casi storici e loro cause, e perché non dovremmo averne paura"
[29] "Iperinflazione" da Wikipedia, l'enciclopedia libera

Tale episodio di iperinflazione poteva essere risolto solamente tramite l'emissione di una nuova valuta, e quindi il 1° agosto 1946 venne emesso il *fiorino* ungherese con un tasso di cambio pari a $4x10^{29}$ *pengö*.[30]

1.2.1 Il caso della crescita monetaria nell'isola di Yap

Di tutti i sistemi monetari che si sono susseguiti nel corso della storia, quello che presenta maggiori analogie con il funzionamento di Bitcoin è l'antico sistema basato sulle pietre Rai caratteristico dell'isola di Yap, oggi parte degli Stati Federali della Micronesia.[31]

Le pietre Rai, utilizzate come moneta, erano di varie dimensioni, ed apparivano come grandi dischi circolari con un foro nel mezzo che potevano arrivare a pesare fino a quattro tonnellate. Non erano pietre native dell'isola di Yap, la quale non possedeva calcare, ma venivano importate dalle vicine Palau e Guam. La bellezza e la rarità di queste pietre le rendevano desiderate e venerate a Yap, ma procurarsele era molto difficile in quanto comportava un laborioso processo di estrazione e spedizione per mezzo di zattere e canoe.[32] Alcune di queste rocce richiedevano per il loro trasporto la presenza di centinaia di persone, e, una volta giunte sull'isola di Yap, venivano collocate in un posto di rilievo dove chiunque poteva vederle. Il proprietario di una pietra poteva usarla come mezzo di pagamento senza la necessità di doverla spostare: in pratica, tutto ciò che doveva fare si esauriva nella comunicazione al popolo che la pietra in questione era stata trasferita ad un altro soggetto, appunto il destinatario del pagamento.[33] L'intera città avrebbe così riconosciuto il trasferimento di proprietà e il destinatario poteva così utilizzarla per effettuare un dato pagamento in un qualsiasi momento. In effetti, non c'era modo di rubare la pietra in quanto la sua proprietà era nota a tutti.

Per secoli, e forse anche per millenni, questo sistema monetario ha funzionato perfettamente all'interno dell'isola di Yap. Anche se tali pietre non si muovevano mai, potevano comunque essere utilizzate come mezzo di pagamento in una qualsiasi parte dell'isola. Le diverse dimensioni di una pietra hanno fornito un certo grado di vendibilità trasversale, così come la possibilità di pagare con frazioni di una sola pietra. Il potere d'acquisto delle pietre nel tempo è stato assicurato per secoli dalla difficoltà e dal costo elevato di acquisirne di nuove, in quanto non era possibile l'estrazione delle stesse sull'isola di Yap, ma era necessario che venissero spedite da Palau. Il costo molto elevato di procurare nuove pietre ha fatto sì che la fornitura esistente fosse sempre molto più elevata di qualunque nuova offerta che potesse essere prodotta in un dato periodo di tempo, rendendo prudente

[30] "Pengö ungherese" da Wikipedia, l'enciclopedia libera
[31] Marco Geremicca (2018), "I Rai di Yap e la blockchain del 1830", articolo pubblicato su LinkedIn
[32] "Rai (Moneta)" da Wikipedia, l'enciclopedia libera
[33] "Le isole", Banca d'Italia

l'accettazione delle stesse come mezzo di pagamento. In altre parole, le pietre Rai presentavano un rapporto stock-to-flow particolarmente elevato, comportando il fatto che fosse oneroso per chiunque gonfiare la scorta esistente di pietre.[34]

O, almeno, fu così fino al 1871, quando un capitano irlandese-americano di nome David O'Keefe fece naufragio sulle rive di Yap e venne rianimato dagli stessi abitanti. O'Keefe vide un'opportunità di profitto nel procurarsi noci di cocco per poi rivenderle ai produttori isolani di olio di cocco; tuttavia, non aveva mezzi per invogliare la gente del posto a lavorare per lui, in quanto erano già molto contenti delle loro vite, nel loro paradiso tropicale, e non avevano alcun interesse verso qualunque forma straniera di moneta che O'Keefe potesse offrire loro. Ma quest'ultimo non accettò un "no" come risposta e navigò così fino ad Hong Kong per procurarsi una barca di notevoli dimensioni ed una grossa quantità di esplosivi.

Si diresse poi a Palau, dove utilizzò gli esplosivi per estrarre diverse pietre Rai, ed infine salpò per Yap per presentare le pietre alla gente del posto come pagamento per le noci di cocco.[35] Contrariamente a quello che O'Keefe si aspettava, gli abitanti del villaggio non furono entusiasti di ricevere le sue pietre e il capo del villaggio proibì ai suoi concittadini di prestare il loro lavoro per ottenerle, decretando che le pietre di O'Keefe non fossero di valore, in quanto procurate troppo facilmente. Solo le pietre estratte tradizionalmente, con il sudore e il sangue degli abitanti di Yap potevano essere accettate come mezzo di pagamento. Altri sull'isola non furono d'accordo con la decisione del capo, e fornirono ad O'Keefe le noci di cocco di cui aveva bisogno. Ciò provocò un conflitto sull'isola che portò alla fine dell'utilizzo delle pietre Rai come moneta.[36] Oggi, le pietre svolgono un ruolo solamente culturale sull'isola, mentre viene utilizzato il dollaro statunitense come mezzo monetario ufficiale.[37]

Anche se la storia di O'Keefe è altamente simbolica, egli fu solamente il precursore dell'inevitabile fino dell'utilizzo delle pietre Rai come moneta, dato che nel corso degli anni la moderna civiltà industriale avrebbe portato alle medesime conseguenze, rendendo molto meno costosa la produzione di tali pietre rispetto a come era in passato. Ci sarebbero, al giorno d'oggi, molti "O'Keefe", locali o stranieri, in grado di fornire a Yap un flusso sempre più grande di nuove pietre. Con lo sviluppo delle tecnologie moderne, il rapporto stock-to-flow delle pietre Rai è diminuito drasticamente: divenne possibile produrne sempre di più ogni anno, e ciò causò una progressiva svalutazione della scorta di pietre già presente sull'isola. Diventò, dunque, sempre più imprudente per chiunque usare tali pietre come riserva di valore, in quanto perdevano sempre di più la loro vendibilità e, con essa, la loro

[34] Saifedean Ammous (2018), The Bitcoin Standard
[35] Ibidem
[36] Ibidem
[37] Mankiw N.G., Taylor M.P., (2019), Macroeconomia

funzione di mezzo di scambio. I dettagli possono differire, ma la dinamica sottostante della diminuzione del rapporto stock-to-flow è la stessa che si è presentata per ogni forma di moneta che nel tempo ha perso il proprio ruolo di mezzo monetario.[38]

1.2.2 Il caso delle aggry beads africane

Una storia simile a quella sopra descritta è successa in riferimento alle "*aggry beads*" africane, le quali vennero usate come mezzo di scambio per secoli nell'Africa Occidentale. La storia di queste perline non è completamente chiara: vi sono alcuni che affermano che siano state estratte da pietre meteoritiche, mentre altri ritengono che siano l'eredità degli scambi commerciali avvenuti tra Egiziani e Fenici.[39] Queste perline erano considerate preziose in un'area dove la lavorazione del vetro era costosa e non molto comune, facendo in modo che presentassero un rapporto stock-to-flow particolarmente elevato e preservassero il loro potere d'acquisto nel corso del tempo.[40]

Essendo piccole e preziose, tali perline erano commerciabili su larga scala perché potevano essere combinate in catene, collane e braccialetti; anche se tutto ciò non rappresentava la situazione ideale in quanto vi erano molti tipi diversi di perline invece di una unità standard. Esse erano anche commerciabili in luoghi diversi data la semplicità del loro trasporto. Tuttavia, queste perline in Europa erano tutt'altro che costose e non vantavano alcun ruolo monetario, in quanto lo sviluppo delle tecniche di lavorazione del vetro comportò il fatto che se fossero state utilizzate come moneta, i produttori avrebbero potuto riempire il mercato con migliaia di esse. Per questo motivo, tali perline presentavano, in Europa, un rapporto stock-to-flow piuttosto basso.

Quando i primi esploratori e commercianti europei visitarono l'Africa occidentale nel XIX secolo, notarono l'elevato valore attribuito dai locali a queste perle, e così cominciarono ad importarne in grandi quantità dall'Europa. Ciò seguì fu simile alla storia di O'Keefe, ma data la piccola dimensione delle perline in confronto alle vaste dimensioni della popolazione, il processo fu decisamente più lento ma con conseguenze più grandi e maggiormente tragiche.

Gli Europei furono in grado di acquistare molte delle preziose risorse dell'Africa in cambio delle perline che avevano acquistato in patria a costi praticamente inesistenti.[41] L'invasione dell'Africa da parte degli europei comportò una progressiva diminuzione del rapporto stock-to-flow relativo alle *aggry beads*, che a sua volta comportò la graduale distruzione della loro commerciabilità e l'erosione

[38] Saifedean Ammous (2018), The Bitcoin Standard
[39] Beauty with a Dark Past: The Evolution of Africa Trade Beads (2015), Clary L. J.
[40] Saifedean Ammous (2018). The Bitcoin Standard
[41] Per massimizzare I loro profitti, gli europei riempivano gli scafi delle loro navi con grandi quantità di queste perline, le quali svolgevano anche un ruolo importante nello stabilizzare la barca durante il viaggio.

del loro potere di acquisto nelle mani degli africani che le possedevano, impoverendoli e trasferendo le loro ricchezze agli europei.[42] Le perline *aggry* assunsero successivamente il ruolo di "perline degli schiavi" per il ruolo svolto dalle stesse nell'alimentare la tratta degli schiavi africani verso l'Europa e l'America.[43]

Il rapido crollo di valore di un mezzo monetario è sicuramente tragico, ma per lo meno comporta effetti immediati di breve durata e i possessori di tale moneta possono ricominciare a commerciare, risparmiare e calcolare i prezzi con una nuova unità monetaria. Al contrario, una graduale diminuzione del valore della moneta comporta il progressivo trasferimento della ricchezza dei possessori di quest'ultima agli individui che invece riescono a produrre tale mezzo monetario in quantità elevata e a basso costo.[44]

1.3 Il ruolo delle banche all'interno del sistema monetario

L'offerta di moneta può essere definita come la somma tra l'ammontare di circolante (banconote e monete metalliche) nelle mani del pubblico e i depositi a vista, ossia l'ammontare di ricchezza che gli individui depositano presso una determinata banca.[45] Tale offerta può essere modificata solamente da tre diverse entità: le banche centrali, gli individui e le banche nazionali.

Gli individui possono decidere autonomamente la quantità di moneta da detenere sotto forma di circolante e quanto invece depositare presso una banca. Maggiore sarà la quantità di ricchezza che gli individui destineranno presso i depositi a vista, maggiori saranno i poteri in mano alle singole banche nazionali di poter variare l'offerta di moneta. Supponendo invece che per una qualsiasi motivazione gli individui dovessero perdere fiducia nei confronti del sistema bancario e decidessero quindi di detenere una quantità maggiore di moneta sotto forma di circolante, in questo caso la capacità delle banche di influenzare l'offerta di moneta diventerà più limitata, dato che se le banche perdono le riserve, di conseguenza avranno possibilità ridotte di creare moneta.[46]

Le banche nazionali possono a loro volta influenzare l'offerta di moneta a seconda del fatto che il sistema bancario di cui fanno parte sia a riserva totale o a riserva frazionaria. Nel primo caso, l'unico scopo delle banche è quello di tenere al sicuro il denaro ricevuto dagli individui e, a tal fine, destineranno l'intero importo a riserva. Dato che in questo caso le banche non concedono prestiti, esse non influenzeranno l'offerta di moneta e non trarranno profitto dalla loro attività. Nel secondo

[42] "What is Money? From Aggry Beads to Digital Dollars", estratto di un articolo scritto da Sidd
[43] Ibidem
[44] Ibidem
[45] Mankiw N.G., Taylor M.P., (2019), Macroeconomia
[46] Mankiw N.G., Taylor M.P., (2019), Macroeconomia

caso, invece, le banche sono tenute a rispettare un determinato rapporto tra riserve e depositi (rapporto *rr*)[47], che indica l'ammontare di moneta ricevuta dagli individui che le banche devono necessariamente destinare a riserva. Con la parte restante, le stesse banche possono decidere di concedere prestiti per poter trarre profitto dalla loro attività. È bene ricordare, però, che per mezzo della concessione di prestiti le banche aumentano l'offerta di moneta senza generare al contempo nuova ricchezza, in quanto i soggetti che decidono di richiedere un prestito alla banca sono consapevoli che prima o poi dovranno restituirlo.

Ovviamente la quantità di moneta che è possibile creare non è illimitata, ma è esprimibile mediante un'equazione[48] che mette in relazione i depositi a vista con il rapporto riserve/depositi:

$$Offerta\ totale\ di\ moneta = \left(\frac{1}{rr}\right) x\ Deposito\ iniziale$$

La terza ed ultima entità in grado di influenzare l'offerta monetaria sono le banche centrali, le quali immettono nel sistema la cosiddetta "base monetaria". Quest'ultima, detta anche "moneta ad alto potenziale", è esprimibile come la somma tra l'ammontare di circolante detenuto dal pubblico e l'ammontare delle riserve presso le banche commerciali; e può essere definita come l'insieme delle attività finanziarie che il sistema bancario può costituire come riserva presso la banca centrale a fronte dei propri depositi.[49] La banca centrale, in particolare, può variare l'offerta di base monetaria per mezzo di tre operazioni differenti: le operazioni di mercato aperto, il tasso di rifinanziamento e la fissazione degli obblighi di riserva.[50]

Le operazioni di mercato aperto si riferiscono all'acquisto o vendita da parte della banca centrale di titoli obbligazionari. Se la banca centrale ha intenzione di aumentare l'offerta monetaria, allora procederà alla creazione di nuovo circolante ed acquisterà dal pubblico un certo numero di titoli obbligazionari; al contrario, nel caso avesse intenzione invece di ridurre l'offerta monetaria, procederà alla vendita di titoli obbligazionari per fare in modo che la quantità di circolante diffusa fra il pubblico diminuisca.[51]

La banca centrale determina inoltre il tasso di interesse al quale è disposta a finanziare le banche commerciali nel breve periodo, detto appunto tasso di rifinanziamento. Può accadere, per esempio, che in un dato momento alcune banche nazionali si ritrovino con un coefficiente di riserva inferiore a quello desiderato, trovandosi dunque costrette a richiedere un prestito alla banca centrale di riferimento. Quest'ultima immetterà liquidità nel mercato monetario ricevendo in cambio titoli

[47] Ibidem
[48] Ibidem
[49] "I mercati finanziari", economia.uniroma2.it
[50] Mankiw N.G., Taylor M.P., (2019), Macroeconomia
[51] "I mercati finanziari", economia.uniroma2.it

obbligazionari o altre attività finanziarie non monetarie concesse dalle banche finanziate. Queste ultime si impegnano, in seguito, a riacquistare in un secondo momento le attività finanziarie cedute alla banca centrale.[52]

Un ultimo strumento utilizzabile dalla banca centrale per influenzare l'offerta monetaria riguarda la fissazione degli obblighi di riserva, ossia dell'ammontare minimo di riserva che ogni banca commerciale deve impegnarsi a detenere. La banca centrale potrebbe, dunque, decidere di diminuire l'ammontare di riserva obbligatoria, facendo in modo che le banche nazionali concedano più prestiti ed aumentino a loro volto l'offerta di moneta. Al contrario, la banca centrale potrebbe decidere un aumento della riserva obbligatoria, forzando le banche nazionali a ridurre gli impieghi e, quindi, l'offerta di moneta.[53]

1.3.1 Alcune criticità sull'utilizzo della politica monetaria da parte delle banche centrali: le recessioni e i cicli economici

Considerando che in un libero mercato dei capitali l'offerta di fondi mutuabili è determinata dagli operatori di mercato che decidono di concedere prestiti basandosi sul tasso di interesse corrente, in un'economia con una banca centrale ed un sistema bancario a riserva frazionaria, invece, tale offerta è diretta da un comitato di economisti sotto l'influenza di politici, banchieri, giornalisti e, alle volte, ufficiali dell'esercito.[54]È innanzitutto importante capire la distinzione tra fondi mutuabili e fondi e beni strumentali attuali. In un'economia caratterizzata da un libero mercato e da una moneta solida, i risparmiatori devono rimandare i consumi ad un momento successivo per risparmiare. Questi risparmi vengono depositati dagli individui presso una banca poiché il risparmio è denaro sottratto al consumo da soggetti che ritardano la gratificazione che quest'ultimo potrebbe dare loro nell'immediato per ottenerne di più in futuro. L'ammontare esatto di risparmi diventa l'ammontare esatto di fondi mutuabili disponibili ad essere preso in prestito dai produttori. La disponibilità di beni strumentali è inestricabilmente legata alla riduzione dei consumi: risorse fisiche effettive, lavoro, la terra e i beni strumentali smetteranno di essere impiegati nella provvista di beni di consumo per essere utilizzati, invece, nella produzione di beni strumentali.[55]La scarsità è il punto di partenza fondamentale di tutta l'economia e la sua implicazione più importante risiede nella nozione che tutte le cose presentano un costo opportunità. Nel mercato dei capitali, il costo opportunità del capitale consiste nel ritardare il consumo, mentre il costo opportunità di quest'ultimo consiste invece nel ritardare l'investimento del capitale. Il tasso di interesse è il prezzo che regola questa relazione: nel momento in cui gli individui

[52] Mankiw N.G., Taylor M.P., (2019), Macroeconomia
[53] Ibidem
[54] Saifedean Ammous, (2018). The Bitcoin Standard
[55] Massimo Carboni, "Risparmio, investimento e sistema finanziario" people.unica.it

domandano più investimenti, il tasso di interesse crescerà, incentivando più risparmiatori a destinare una ricchezza maggiore al risparmio. Nel caso in cui, invece, il tasso di interesse dovesse diminuire, ciò incentiverà gli investitori ad intraprendere più progetti di investimento e ad investire in metodi di produzione più tecnologicamente avanzati con un orizzonte temporale più lungo. Un tasso di interesse più basso, quindi, permette la messa a punto di metodi di produzione più efficienti ed efficaci.[56]

Mentre, un'economia avanza e diventa sempre più sofisticata, la connessione tra capitale fisico e mercato dei fondi mutuabili rimane stabile, ma diventa meno chiara nella mente degli individui. Un'economia moderna con una banca centrale è costruita ignorando questo trade-off fondamentale e assumendo che le banche possano finanziare gli investimenti stampando nuova moneta, senza il bisogno che gli individui ritardino i consumi. Poiché la banca centrale controlla l'offerta di moneta e il tasso di interesse, si formerà inevitabilmente una discrepanza tra risparmi e fondi mutuabili. Le banche centrali cercano in genere di favorire la crescita economica, gli investimenti e di accrescere i consumi, e, quindi, tendono ad aumentare l'offerta di moneta e a ridurre il tasso di interesse, comportando un grosso aumento dei fondi mutuabili a discapito dei risparmi. A questo relativamente basso tasso di interesse, le imprese tenderanno ad indebitarsi di più per intraprendere progetti di investimento, piuttosto che fare affidamento ai risparmiatori per finanziare gli stessi progetti.[57] In altre parole, il valore del consumo differito è inferiore al valore del capitale preso in prestito. Senza un sufficiente consumo differito, non ci saranno abbastanza risorse di capitale, terra e lavoro e se i consumatori risparmiano di meno, dovrà esserci anche meno capitale a disposizione per gli investitori. Ricorrere al *signoraggio*[58] per compensare la carenza di risparmio non aumenterà magicamente lo stock di capitale fisico della società; ma l'unico effetto sarà quello di una complessiva svalutazione della moneta esistente accompagnata da un aumento generale del livello dei prezzi. Questa carenza di capitale non è immediatamente evidente, perché le banche centrali e nazionali possono emettere una quantità di moneta sufficiente per i mutuatari, il che rappresenta l'unico vantaggio nell'utilizzo di una moneta non stabile.[59]

In un'economia caratterizzata da una moneta stabile, invece, tale manipolazione del prezzo del capitale sarebbe impossibile: non appena il tasso di interesse viene fissato artificialmente basso, la carenza di risparmi presso le banche si riflette in una riduzione del capitale disponibile per i mutuatari, portando così ad un aumento del tasso di interesse, il quale comporterà a sua volta una riduzione della domanda di prestiti e un aumento dell'offerta di risparmi fino al punto in cui i due si equipareranno.[60]

---

[56] Mankiw N.G., Taylor M.P., (2019), Macroeconomia
[57] "Risparmi Investimentl.FINANZA", da people.unica.it
[58] Con il termine "signoraggio" si fa riferimento all'insieme dei redditi derivanti dall'emissione di moneta. Da Wikipedia, l'enciclopedia libera.
[59] Joseph Salerno (Ludwig Von Mises Institute, 2010). Money: Sound and Unsound
[60] Ibidem

Una moneta non solida rende una manipolazione del genere possibile, ma solo per un breve periodo di tempo dato che le conseguenze non possono essere tardate per sempre. Un tasso di interesse fissato artificialmente basso e l'eccesso di moneta stampata ingannano i produttori ad impegnarsi in un processo di produzione che richiede più risorse di capitale di quelle disponibili. L'eccesso di moneta, insieme ad una mancanza di consumo differito effettivo, inizialmente, spingeranno i produttori a chiedere in prestito con l'illusione che la moneta permetterà loro di comprare tutti i beni strumentali necessari per il processo di produzione. Nel momento in cui sempre più produttori cominciano a fare offerte per sempre meno beni strumentali e risorse di quante se ne aspettavano, la conseguenza naturale è un aumento del prezzo dei beni strumentali necessari al processo produttivo. Questo è il punto nel quale la manipolazione diventa palese, portando al crollo simultaneo di numerosi progetti di investimento, i quali diventano improvvisamente non profittevoli a seguito del cambiamento nel livello dei prezzi dei beni strumentali. L'intervento della banca centrale nel mercato dei capitali permette di intraprendere un numero di progetti di investimento maggiore a seguito della distorsione dei prezzi che porta gli investitori a fare calcoli sbagliati. Tuttavia, l'intervento della banca centrale non può aumentare l'ammontare del capitale attualmente disponibile, e quindi tutti i progetti intrapresi in eccesso non verranno portati a termine rappresentando uno spreco di capitale non necessario. La sospensione di questi progetti, allo stesso tempo, causa un aumento della disoccupazione all'interno dell'economia. Questo fallimento simultaneo dell'intera economia esteso poi alle singole imprese è ciò che viene definito una *recessione.*[61]

Solamente con una comprensione della struttura del capitale e di come la manipolazione del tasso di interesse distrugge ogni incentivo all'accumulazione di capitale, un individuo può capire le cause delle recessioni e le varie fasi del ciclo economico. Il ciclo economico è il risultato naturale della manipolazione del tasso di interesse, la quale distorce il mercato dei capitali facendo credere agli investitori di poter ottenere più capitale di quello disponibile. Quando la banca centrale manipola il tasso di interesse in misura inferiore rispetto al prezzo di mercato, indirizzando le banche nazionali ad aumentare l'offerta di moneta per mezzo dei prestiti, esse per prima cosa riducono l'ammontare dei risparmi disponibili nella società e, inoltre, aumentano la quantità domandata dai mutuatari, indirizzando allo stesso tempo il denaro preso a prestito verso progetti che non potranno essere completati.[62] Quindi, meno è solida la moneta che viene adottata dall'economia e più facile è per la banca centrale manipolare i tassi di interesse, e, quindi, più severi e disastrosi si presenteranno i cicli economici.[63]

[61] Ludovico Bianchi, (2020). "La crisi del 2008: le cause ma soprattutto gli effetti"
[62] Saifedean Ammous, (2018). The Bitcoin Standard
[63] Joseph Salerno (Ludwig von Mises Institute, 2010). Money: Sound and Unsound

Capitolo 2: La moneta digitale

2.1 Bitcoin: che cos'è e a cosa serve

Per capire l'importanza della moneta digitale è utile dare uno sguardo al passato, quando ancora Bitcoin doveva essere inventato e ogni individuo poteva chiaramente distinguere le alternative di pagamento in due categorie non sovrapposte:

- I pagamenti in contante, che vengono effettuati di persona tra due distinte controparti.[64]

- I pagamenti intermediati, che richiedono una terza parte fidata e comprendono assegni, bonifici bancari, carte di credito, carte di debito e servizi più recenti come Paypal.[65]

Entrambe le forme di pagamento presentano alcuni vantaggi e svantaggi, e la maggior parte degli individui ricorre ad una combinazione dei due nelle loro transazioni economiche. Prima dell'invenzione di Bitcoin, i pagamenti intermediati includevano tutte le forme di pagamento digitali. Tuttavia, una delle caratteristiche degli oggetti digitali sin dalla nascita dei computer è che non sono risorse scarse: possono essere prodotti all'infinito, e perciò risulta impossibile utilizzarli come

[64] Saifedean Ammous, (2018). The Bitcoin Standard
[65] Ibidem

moneta. Qualsiasi forma di pagamento elettronico doveva essere effettuata facendo ricorso ad un intermediario a causa del pericolo della doppia spesa[66]: non c'era modo di garantire l'onestà del pagante a meno che non ci fosse una terza parte a supervisionare e in grado di verificare l'integrità dei pagamenti effettuati.

Dopo anni di numerosi tentativi ed errori da parte di una molteplicità di programmatori, e facendo affidamento su una vasta gamma di tecnologie diverse, Bitcoin fu la prima soluzione ingegneristica che consentiva pagamenti digitali senza dover fare affidamento su un terzo che svolgesse il ruolo di intermediario. Essendo il primo oggetto digitale verificabilmente scarso in natura, Bitcoin rappresenta il primo esempio di moneta digitale. Ci sono diversi inconvenienti nell'effettuare transazioni mediante terze parti che rendono la moneta digitale una soluzione allettante per diversi individui. Le terze parti sono per la loro natura "un'ulteriore debolezza alla sicurezza delle transazioni"[67]: coinvolgendo un soggetto ulteriore nelle transazioni si introducono intrinsecamente dei rischi, perché si introducono lee possibilità di furti e di guasti tecnici.

L'obiettivo che Satoshi Nakamoto voleva raggiungere mediante Bitcoin consisteva nella creazione di "una forma puramente peer-to-peer di moneta elettronica" che non richiedesse di riporre fiducia in alcune terze parti per le transazioni e la cui fornitura non potesse essere alterata da nessuno. In altre parole, Bitcoin vanterebbe le caratteristiche di una moneta fisica (mancanza di intermediari, finalità delle transazioni) all'interno del mondo digitale, combinandole con una politica monetaria ferrea che non può essere manipolata per produrre inflazione inattesa a discapito dei possessori di tale moneta e a beneficio di un qualsiasi individuo esterno. Nakamoto è riuscito a raggiungere questo obiettivo attraverso l'utilizzo di poche importanti, anche se non ampiamente comprese, tecnologie: una rete peer-to-peer, firme digitali, *hashing, mining* e una tecnologia di conferma *proof of work.*[68]

La rete di Bitcoin ha cominciato a funzionare nel gennaio 2009 ed è stata per certo periodo un progetto oscuro utilizzato da pochi individui all'interno di una mailing list dedicata alla crittografia. Forse la più importante pietra miliare nella vita di Bitcoin è stata la prima volta in cui i *token* presenti all'interno della rete sono passati dall'essere senza alcun valore economico all'avere un vero e proprio prezzo di mercato, decretando che Bitcoin aveva passato il test di mercato: la rete aveva funzionato abbastanza bene da fare in modo che alcuni individui avessero intenzione di scambiare denaro reale per acquistare i token all'interno della rete.

---

[66] "Con il termine "doppia spesa" si fa riferimento a quella pratica mediante la quale viene speso il medesimo titolo valutario due o più volte", da Wikipedia, l'enciclopedia libera

[67] Nick Szabo, (2001). Trusted Third Parties Are Security Holes

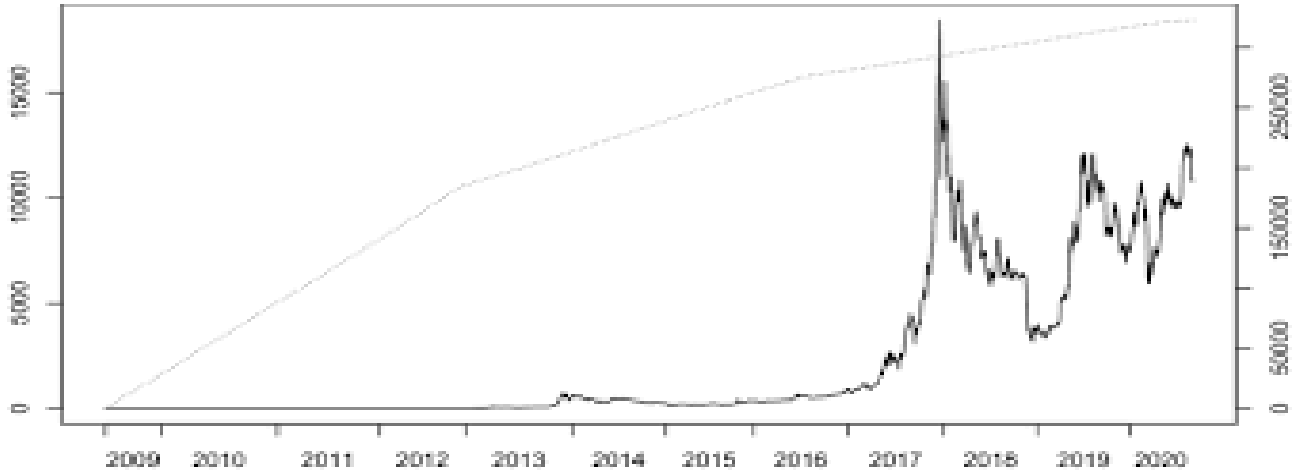
[68] "Bitcoin: che cos'è e come funziona", Borsa Italiana

Questo successe nell'ottobre del 2009, quando un'exchange presente sul web conosciuto come "New Liberty Standard" vendette un bitcoin per un controvalore pari a $0,000994.[69] Nel maggio 2010 vi fu il primo acquisto nel mondo reale, quando qualcuno pagò 10.000 bitcoins per due fette di pizza del valore totale di $25, facendo salire il prezzo di un bitcoin a $0,0025.[70] Con il passare degli anni, sempre più individui vennero a conoscenza di Bitcoin e si interessarono ad acquistarlo, facendo salire il prezzo sempre di più.[71]

Il fatto che la rete peer-to-peer sulla quale si fonda Bitcoin sia stata perfettamente operativa sin dai suoi primi giorni ha dato al suo token digitale un valore collezionabile tra minuscole comunità di crittografi, i quali provarono a cimentarsi in processi di *mining* con il loro stesso PC e cominciarono a scambiarsi i tokens a vicenda. Inoltre, il fatto che i tokens fossero strettamente limitati e non potessero essere replicati ha contribuito a creare il loro status di oggetti da collezione. Dopo essere stati acquistati dagli individui per poterli utilizzare all'interno della rete di Bitcoin, e dopo aver ottenuto un valore economico, Bitcoin cominciò ad essere monetizzato a seguito della crescente domanda di individui che volevano utilizzarlo come riserva di valore.[72]

Essendo nuovo e agli inizi della sua diffusione, il prezzo di Bitcoin ha dato luogo ad evidenti fluttuazioni man mano che ne aumentava la relativa domanda, ma l'impossibilità di aumentarne l'offerta arbitrariamente da parte di alcuna autorità in risposta ai picchi di prezzo contribuisce a spiegare l'incredibile ascesa nel potere di acquisto di tale valuta digitale (vedi grafico)[73]. Quando si verifica un picco nella domanda di bitcoins, i miners non possono aumentarne la produzione come, invece, potrebbero fare i minatori di rame, e nessuna banca centrale può intervenire per aumentarne l'offerta. L'unico modo per il mercato di fronteggiare la domanda in costante crescita di bitcoins consiste nell'aumentarne il prezzo per incentivare i possessori a venderne una parte agli individui che vogliono entrare a far parte della rete.[74]

[69] Factbox: "Ten years of bitcoin", by Reuters Staff (2018)
[70] Ibidem
[71] Nathaniel Popper, (2015). Digital Gold
[72] Saifedean Ammous, (2018). The Bitcoin Standard
[73] Ibidem
[74] Ibidem



2.1.1 La tecnologia Blockchain

La tecnologia della Blockchain venne ideata per la prima volta nel 1991 da un duo di ricercatori americani ed era stata inizialmente pensata per vidimare i documenti digitali, in modo che non fosse possibile retrodatarli o manometterli. Tuttavia, tale tecnologia rimase pressoché inutilizzata fino al 2008, quando venne sfruttata da Satoshi Nakamoto per creare la prima criptovaluta digitale della storia: il bitcoin.[75]

Una blockchain è, in estrema sintesi, una specie di archivio digitale condiviso e decentralizzato consultabile da chiunque faccia parte della rete, e proprio per questa ragione, una volta che delle informazioni vengono registrate al suo interno, sono molto difficili da modificare.

Una blockchain è letteralmente una catena di blocchi contenenti informazioni, e ogni blocco della catena presenta fondamentalmente tre elementi. Il primo elemento sono i dati che vengono memorizzati in quel blocco. Il tipo di dati ivi contenuti dipende, inoltre, dal tipo di blockchain utilizzata. La blockchain di Bitcoin, ad esempio, memorizza all'interno dei blocchi i dettagli di una transazione, come mittente e destinatario, e la quantità di bitcoins che viene scambiata.[76] Il secondo elemento è il cosiddetto "*hash*"[77], ossia una stringa di numeri e lettere che identifica quel blocco e il suo contenuto e che è sempre unica, come una specie di impronta digitale. Ogni volta che viene creato un nuovo blocco viene calcolato un nuovo *hash*, unico e specifico per quel blocco e per quel dato, e se qualche dato all'interno del blocco dovesse successivamente cambiare, allora cambierà

[75] "Che cos'è e come funziona una Blockchain", https://www.youtube.com/watch?v=sX25z_-zMgI&t=178s
[76] "Che cos'è e come funziona una Blockchain", https://www.youtube.com/watch?v=sX25z_-zMgI&t=178s
[77] "Con il termine *hash* ci si riferisce, nel linguaggio informatico, ad una funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita", da Wikipedia, l'enciclopedia libera

anche l'*hash*.[78]Il terzo elemento contenuto in ogni blocco è l'*hash* del blocco precedente ed è proprio la sua presenza all'interno di ogni blocco a dare origine alla catena, ed è anche questo ciò che rende la blockchain così sicura.[79]

Tutte le blockchain presentano alcuni elementi chiave, come la tecnologia di registro distribuito, i record immutabili e i contratti intelligenti.[80]

Grazie alla tecnologia di registro distribuito, tutti i partecipanti alla rete hanno la possibilità di consultare e verificare le transazioni effettuate. Con questo registro condiviso, inoltre, le transazioni vengono registrate una sola volta, scongiurando così il pericolo della duplicazione dei compiti e delle informazioni, tipica delle reti dei business tradizionali.[81]

Il ruolo dei record immutabili è quello di evitare che i partecipanti modifichino o manomettano le transazioni che già sono state registrate all'interno del registro distribuito. Se un record di transazioni contiene un errore, dovrà essere aggiunta una nuova transazione per correggerlo ed entrambe saranno poi visibili.[82]

I contratti intelligenti, o *smart contracts,* sono dei programmi costuditi all'interno di una rete blockchain che vengono attivati nel momento in cui si verificano determinate condizioni. Essi sono utilizzati principalmente per automatizzare la stipula di un accordo, per fare in modo che i soggetti stipulanti siano ex ante consapevoli delle conseguenze delle loro azioni. I contratti intelligenti funzionano rispettando semplici comandi come "if/when..then.." che vengono scritti sotto forma di codici all'interno della blockchain. Mediante tali contratti, una rete di computer svolge alcune azioni al verificarsi di condizioni predeterminate. Queste azioni possono includere il rilascio di fondi verso un preciso individuo, la registrazione di un veicolo, la spedizione di una notifica o l'emissione di un ticket. La blockchain viene successivamente aggiornata quando la transazione è completata, comportando il fatto che essa non possa essere modificata, e solo i membri che hanno ottenuto il permesso ne possono verificare i risultati.[83]

2.1.2 Le catene del PoW e il mining: alcune precisazioni sulla creazione di nuova valuta digitale

Nakamoto ha rimosso la necessità di fare affidamento su terzi costruendo Bitcoin su una base di prove e verifiche molto approfondite e ferree. È giusto dire che la caratteristica centrale di Bitcoin è la

[78] "Che cos'è e come funziona una Blockchain", https://www.youtube.com/watch?v=sX25z_-zMgI&t=178s
[79] Ibidem
[80] "Che cos'è la tecnologia blockchain?", IBM
[81] Ibidem
[82] Ibidem
[83] "What are smart contracts on blockchain?" IBM

verifica, e solamente grazie a questo fatto è riuscito a rimuovere completamente la necessità di porre fiducia su qualcuno.[84] Ogni transazione deve essere registrata da ogni membro della rete in modo che tutti condividano un registro comune di saldi e transazioni. Ogni volta che un membro della rete trasferisce una somma di denaro ad un altro, tutti i partecipanti possono verificare se il mittente dispone realmente di tale somma, e i nodi competono per essere i primi ad aggiornare il registro con un nuovo blocco di transazioni ogni dieci minuti.[85] Affinché un nodo riesca ad aggiungere un blocco di transazioni al registro, deve spendere una determinata quantità di potenza di elaborazione per risolvere problemi matematici particolarmente complessi, detti *hash*, che sono difficili da risolvere ma la cui soluzione è semplice da verificare.[86]

Questo è il sistema definito "Proof-of-Work" (PoW), e solamente con una soluzione corretta un preciso blocco può essere aggiunto e verificato da tutti i membri della rete. Anche se questi problemi matematici non sono correlati con le transazioni aventi ad oggetto un certo ammontare di bitcoins, essi sono indispensabili per il funzionamento del sistema in quanto spingono i nodi verificatori ad impiegare potenza di elaborazione che sarebbe sprecata nel caso in cui siano presentate transazioni fraudolente. Nel momento in cui un nodo risolve correttamente il proof-of-work e comunica le transazioni, gli altri nodi della rete sono chiamati a votarne la validità, e dopo che la maggioranza di essi ha votato per l'approvazione del blocco, quest'ultimo verrà aggiunto alla catena contenente tutti i blocchi di transazioni già approvati in passato. Inoltre, il nodo che riesce ad aggiungere un nuovo blocco alla rete riceve una ricompensa consistente in nuovi bitcoins aggiunti all'offerta complessiva di tale moneta digitale, al quale si aggiungono tutte le commissioni pagate dagli individui che effettuano le transazioni. Questo processo viene chiamato "*mining"*, analogo al mining di metalli preziosi, ed è per questo motivo che i nodi che riescono a risolvere il proof-of-work vengono riconosciuti come "minatori" o "miners".[87]

Mentre in una moderna banca centrale la nuova moneta creata viene impiegata principalmente per finanziare i prestiti e la spesa pubblica, nella rete di Bitcoin le nuove unità monetarie verranno assegnate solamente a chi spende risorse e potenza di elaborazione per l'aggiornamento del registro. Nakamoto ha programmato Bitcoin affinché produca un nuovo blocco ogni dieci minuti, e che la rispettiva ricompensa sia pari a 50 monete per ogni blocco aggiunto nei primi quattro anni di attività, per essere poi dimezzata a 25 monete, e successivamente dimezzata ogni quattro anni, fino ad arrivare a 0 nel 2144.[88]

---

[84] Konrad Graf, (2013). "On the Origins of Bitcoin: Stages of Monetary Evolution"
[85] Saifedean Ammous, (2018). The Bitcoin Standard
[86] "Proof of Work (PoW): Cos'è, Come Funziona, Vantaggi e Svantaggi", www.meteofinanza.com (maggio, 2021)
[87] "Come funziona il mining", Salvatore Aranzulla
[88] "Che cos'è il Block Reward" acedemy.bit2me.com (novembre, 2020)

La quantità di Bitcoin creati è pre-programmata e non può essere modificata, indipendentemente da quanto sforzo ed energia vengano spese nel processo di proof-of-work. Tutto ciò viene garantito tramite un processo chiamato "*difficulty adjustment*"[89]: all'aumentare del numero degli individui che decideranno di detenere una certa quantità di bitcoins, aumenterà di conseguenza anche il valore di mercato di tale moneta e il mining sarà più redditizio, spingendo i minatori a spendere maggiore potenza elettronica e risorse al fine della risoluzione dei calcoli algoritmici necessari alla proof-of-work. Più minatori significa perciò più potenza di elaborazione che comporterebbe una diminuzione dei tempi necessari per la ricerca della soluzione del proof-of-work, facendo così aumentare il tasso di emissione di nuovi bitcoins. Ma all'aumentare della potenza di elaborazione, Bitcoin aumenterà la difficoltà dei problemi matematici necessari per ottenere la ricompensa dell'attività di mining, affinché venga garantito che i blocchi continuino a richiedere dieci minuti per essere prodotti.[90]

La *difficulty adjustment* rappresenta la tecnologia più affidabile per mantenere stabile la moneta e limitare la crescita del rapporto stock-to-flow, rendendo Bitcoin completamente diverso da qualsiasi altra forma di moneta. Mentre l'aumento di valore di una qualsiasi moneta porta ad un aumento delle risorse impiegate nella sua produzione, e quindi ad un aumento della sua offerta, man mano che il valore di Bitcoin aumenta, l'impiego di maggiori sforzi per produrre più unità monetarie non portano all'effettiva produzione di più bitcoins. Al contrario, ciò porta solamente ad un aumento della potenza di elaborazione informatica necessaria per poter aggiungere blocchi di transazioni alla rete di Bitcoin, il che serve solo a rendere la rete più sicura e difficile da compromettere.[91]

2.2. L'offerta di moneta esauribile: i limiti alla creazione di nuovi bitcoins

In passato, è sempre stato possibile produrre un determinato asset mantenendo il relativo tasso di crescita dell'offerta costante, e permettendo allo stesso di mantenere il proprio ruolo monetario, ma la realtà, come sempre, si è dimostrata più complessa della semplice teoria. I governi non consentirebbero mai ai privati di mettere a punto una moneta diversa da quella utilizzata a livello statale e di trasgredire dalla maniera principale mediante la quale il governo finanzia sé stesso e la propria crescita.[92]Così, i governi cercano sempre di monopolizzare la produzione di moneta e affrontano molto spesso un incredibile tentazione nell'aumentarne l'offerta.

Tuttavia, con l'invenzione di Bitcoin, il mondo è arrivato finalmente ad una forma sintetica di moneta che presenta una regola molto ferrea circa il controllo del suo basso tasso di crescita dell'offerta.

---

[89] "Bitcoin Network Sees Fourth Straight Downward Difficulty Adjustment", www.coindesk.com (luglio, 2021)
[90] Ibidem
[91] Saifedean Ammous, (2018). The Bitcoin Standard
[92] Ibidem

Bitcoin è riuscito ad escludere i governi, i politici, i presidenti, i giornalisti, i leaders rivoluzionari e i dittatori militari dal controllo della propria offerta, la cui crescita è determinata da una funzione programmata e utilizzata da tutti i membri della rete.[93] Mentre nei primi anni dalla creazione di Bitcoin la crescita dell'offerta presentava un tasso piuttosto elevato e la garanzia che l'offerta totale non sarebbe stata modificata non era completamente credibile, con il passare degli anni il tasso di crescita dell'offerta diminuì drasticamente e la credibilità della rete nel mantenere fissa l'offerta di moneta totale è aumentata e continua a salire giorno dopo giorno dato che non vengono apportate modifiche significative al network.[94] I nuovi blocchi contenenti le transazioni vengono aggiunti al registro condiviso all'incirca ogni dieci minuti.

Alla nascita della rete, la remunerazione per ogni blocco era programmata per essere pari a 50 bitcoins. Ogni quattro anni, o dopo l'aggiunta di 210.000 blocchi, la remunerazione relativa diventa esattamente la metà. Il primo dimezzamento ha avuto luogo il 28 novembre 2012, quando la remunerazione diventò pari a 25 bitcoins per ogni blocco aggiunto alla rete.

Il 9 luglio 2016, essa dimezzò nuovamente fino ad arrivare a 12,5 bitcoins per blocco, mentre l'ultimo dimezzamento risale al 2020, facendo arrivare la remunerazione ad essere pari a 6,25 bitcoins per blocco.[95]In linea con tale schema, l'offerta continuerà ad aumentare ad un tasso decrescente, asintoticamente fino a raggiungere un'offerta finale complessiva pari a 21 milioni di monete, prevista per l'anno 2140. Raggiunto tale limite, nessun bitcoin potrà essere emesso e la remunerazione per ogni blocco aggiunto sarà pari a 0.[96]

Il numero esatto di monete in circolazione varierà, ma tale variazione diminuirà all'aumentare dell'offerta totale. Ciò che invece non subirà variazioni è quella che sarà l'offerta complessiva finale, e il fatto che il tasso di crescita dell'offerta continuerà a calare man mano che un numero sempre minore di monete verrà aggiunto allo stock complessivo. (vedi figura 14)[97]

[93] "Inflazione, proteggersi grazie a Bitcoin", www.rezerve.it
[94] Saifedean Ammous, (2018). The Bitcoin Standard
[95] "Cosa fa aumentare il prezzo di Bitcoin" www.senigallianotizie.it (ottobre, 2021)
[96] "Storia breve del bitcoin", www.wired.it (gennaio, 2019)
[97] Fonte: coctbodol.com

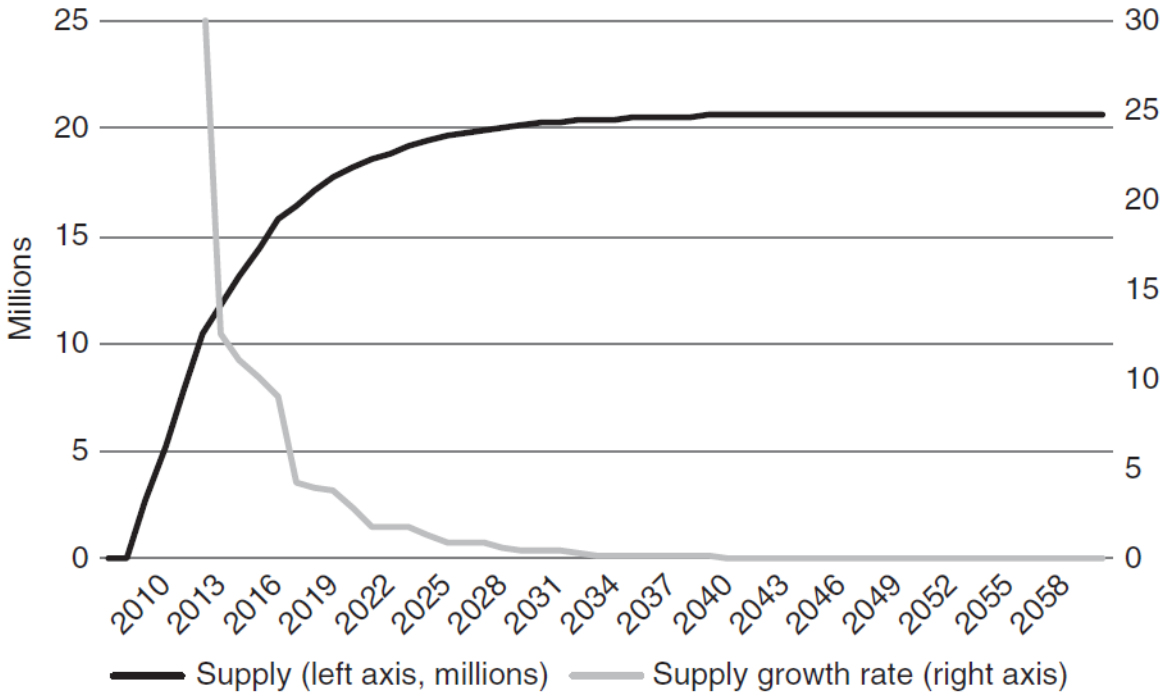


Figure 14 Bitcoin supply and supply growth rate assuming blocks are issued exactly every ten minutes.

Dato che le nuove monete sono prodotte solamente nel momento in cui un nuovo blocco viene aggiunto alla rete, e ogni blocco richiede la risoluzione dei problemi forniti dal sistema di proof-of-work, vi è un costo reale connesso alla produzione di nuovi bitcoins. All'aumentare del prezzo dei bitcoins nel mercato, più nodi entreranno in competizione per trovare la soluzione al PoW e per ricevere, di conseguenza, la remunerazione, facendo in modo che i problemi forniti dal sistema aumentino di difficoltà, rendendo più costoso il procedimento per ottenere la remunerazione. Così, il costo di produzione di un bitcoin aumenterà di pari passo con l'aumento del relativo prezzo di mercato.[98]

Una volta impostato lo schema relativo alla crescita dell'offerta, Nakamoto divise ogni bitcoin in 100.000.000 unità, le quali furono nominate successivamente "*satoshis*"[99], in suo onore. Dividendo ogni bitcoin per un numero di otto cifre, l'offerta totale di bitcoins continuerà a crescere ad un ritmo decrescente fino all'anno 2140, quando tutte le singole unità verranno create e verrà raggiunta la cifra finale pari a 21.000.000 monete.[100]Il tasso di crescita decrescente, tuttavia, significa che le prime

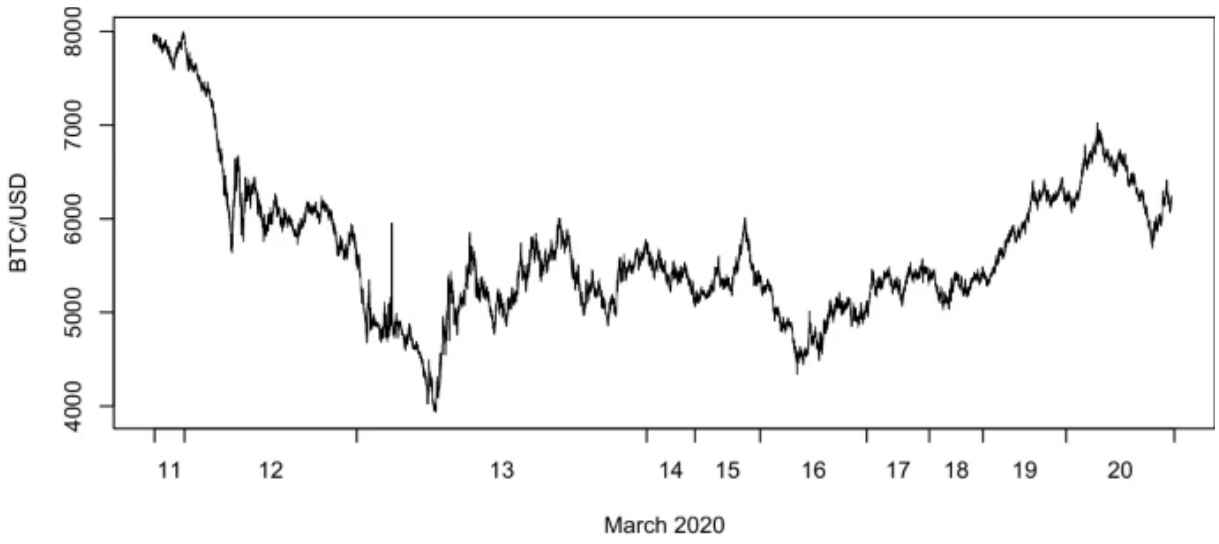
[98] "Perché il Prezzo del bitcoin aumenta?" www.wisdomtree.eu (gennaio, 2021)
[99] Con il termine "*satoshis*" si intende indicare la più piccola parte di un bitcoin momentaneamente registrata all'interno della blockchain.
[100] "What happens to Bitcoin after all 21 million are mined?" www.investopedia.com (ottobre, 2021)

20.000.000 di monete verranno minate entro il 2025, lasciando così un milione di monete da minare nell'arco di un secolo.[101]

2.3 I principali vantaggi di Bitcoin: rispetta tutte e tre le caratteristiche base di ogni moneta?

2.3.1 Mezzo di scambio

Al momento, se una transazione dovesse essere eseguita in Bitcoin, l'acquirente dovrebbe prima acquistarne una certa quantità per poi utilizzarla per il pagamento. Una volta effettuata la transazione, è molto probabile che il venditore riconverta i bitcoins ricevuti nella sua valuta locale in modo da pagare i propri creditori. Tale operazione, tuttavia, supporta il rischio del tasso di cambio che aumenta assieme al livello di volatilità nel mercato di Bitcoin. Per esempio, come si può notare dalla figura sotto riportata[102], la volatilità giornaliera si attesta normalmente intorno al 10% e, in certi giorni, può raggiungere anche picchi pari al 30%. Ciò significa che l'acquisto di un bene il cui valore risulta pari a $1,000 potrebbe costare circa il 10% ($100) in più o in meno a seconda del momento dell'acquisto.[103]



Per fornire un esempio più preciso, consideriamo il periodo che va dall'11 al 13 marzo 2020, che si può osservare dal grafico sopra riportato che presenta le serie temporali dei prezzi di negoziazione ad alta frequenza di Bitcoin su Kraken[104], nel periodo che va dall'11 al 20 marzo 2020.

---

[101] Ibidem
[102] "The volatility of Bitcoin and its role as a medium of exchange and a store of value", Dirk G. Baur, link.springer.com
[103] Ibidem
[104] Kraken rappresenta uno dei primi exchange mai costituiti con lo scopo di acquistare e vendere criptovalute

Ora supponiamo che un determinato bar venda tazze di caffè per 625,000 satoshis[105] che, nei giorni 10 e 11 di marzo 2020, sarebbero stati l'equivalente di $5. Nella mattina del 12 marzo, la stessa tazza di caffè sarebbe risultata leggermente più conveniente, con un valore pari a $4.63, che rappresenta un vantaggio per il consumatore ma uno svantaggio per il proprietario del bar. Poco più tardi, per l'ora di pranzo, la stessa tazza di caffè sarebbe costata solamente $3.75, arrivando fino ad un valore pari a $2.56 durante la notte del 13 marzo. Per il proprietario del bar, questa rappresenta una situazione insostenibile in quanto dovrebbe affrontare grosse perdite derivanti dagli sbalzi di prezzo giornalieri. L'unico modo per evitare questa situazione sarebbe quello di aggiustare il prezzo del prodotto di volta in volta, esprimendolo sempre per mezzo di satoshis. Per continuare a guadagnare $5 da una tazza di caffè, quindi, il proprietario del bar avrebbe dovuto aumentarne il prezzo a 1,250,000 satoshis per il 13 marzo, e quindi raddoppiarlo.[106]

Questo esempio evidenza, inoltre, le notizie inconsistenti riguardanti l'accettazione di Bitcoin da parte delle piccole e grandi imprese. Il ragionamento economico e l'intuizione aiutano a capire che sarebbe molto costoso per qualsiasi società, che si tratti di Apple, Dell, Microsoft o PayPal, accettare Bitcoin come mezzo di pagamento. Ciò che alcune aziende possono offrire è la conversione di Bitcoin attraverso un'exchange predefinito. Questo è simile a effettuare un pagamento in valuta estera che viene poi convertita in valuta locale al momento della transazione.[107]

L'unico modo per eliminare completamente questo rischio sarebbe, per una nazione, adottare Bitcoin come valuta locale e imporre determinate restrizioni sulla conversione dello stesso con altre valute. Tuttavia, al giorno d'oggi non ci sono ragioni valide che possano spingere un paese sviluppato a adottare Bitcoin come valuta locale, in quanto non sarebbe possibile controllarne l'offerta di moneta. Questo è il motivo per cui molte banche centrali di diversi paesi, invece di adottare Bitcoin, valutano l'idea di creare la propria valuta digitale.[108]

2.3.2 Riserva di valore

La credenza che le risorse siano scarse e limitate rappresenta un'incomprensione della natura della scarsità, che rappresenta il concetto chiave dell'economia. La quantità totale di ogni materia prima presente sulla terra è talmente vasta per noi esseri umani che difficilmente può essere misurata o compresa. Dalla superficie terrestre, sono stati estratti al giorno d'oggi a malapena i minerali

[105] Come è stato spiegato in precedenza, il *satoshis* rappresenta la più piccola unità di conto di bitcoin e il mezzo che le permette una notevole flessibilità di pagamento
[106] "The volatility of Bitcoin and its role as a medium of exchange and a store of value", Dirk G. Baur, link.springer.com
[107] "The volatility of Bitcoin and its role as a medium of exchange and a store of value", Dirk G. Baur, link.springer.com
[108] Ibidem

indispensabili per la vita umana, e più si continua a cercare e a scavare, più risorse prima sconosciute vengono alla luce. Ciò che costituisce il limite pratico e realistico alla disponibilità di ogni risorsa è sempre l'ammontare di tempo impiegato nella loro produzione, che rappresenta l'unica reale risorsa scarsa.[109]L'eterno dilemma che gli esseri umani affrontano con il loro tempo riguarda il modo con cui immagazzinare per il futuro il valore che essi producono con il loro tempo. Mentre il tempo per gli esseri umani è una risorsa scarsa, tutto il resto è praticamente inesauribile, e sempre di più ne può essere prodotto qualora gli esseri umani si impegnino nella relativa produzione. Qualsiasi oggetto che gli individui scelgono come riserva di valore, assisterà ad una crescita del proprio valore, e dato che sempre più oggetti possono sempre essere prodotti, gli altri individui potranno sempre più unità del medesimo oggetto con il fine di appropriarsi del valore nello stesso immagazzinato.[110]

Gli abitanti dell'isola di Yap assistettero ad un episodio del genere, quando O'Keefe portò esplosivi fino a Palau al fine di estrarre più pietre Rai, per poi presentarle fino all'isola di Yap ed impossessarsi del valore posseduto fino a quel momento dagli abitanti. Gli africani, a loro volta, furono vittime della medesima situazione quando gli Europei portarono nelle loro terre barche piene di perline aggry. Qualsiasi metallo diverso dall'oro che fu usato come mezzo monetario fu prodotto in quantità tali da portare al collasso del proprio prezzo. Le moderne economie sono caratterizzate dalle banche centrali che pretendono di arginare l'inflazione mentre erodono, gradualmente o velocemente, il valore della loro moneta.

Come gli americani recentemente iniziarono ad utilizzare le loro case come mezzo di risparmio, l'offerta di immobili aumentò vertiginosamente portando al collasso del relativo prezzo. Solamente l'oro è arrivato vicino a risolvere tale problema, il quale, grazie alla sua composizione, ha reso impossibile per chiunque aumentarne arbitrariamente la propria offerta.[111]Tuttavia, con il passaggio a forme di controllo dell'oro da parte dei governi, esso ha perso in parte il proprio ruolo monetario, venendo rimpiazzato dalle cosiddette "monete *fiat*".[112]

Tutto ciò getta luce sull'aspetto sorprendente della natura tecnica di Bitcoin. Per la prima volta, l'umanità ha fatto ricorso ad una materia prima la cui offerta è strettamente limitata. Non importa quante persone utilizzino la rete, quanto salirà il suo valore, e quanto avanzati siano gli strumenti per produrlo, ci potranno essere solamente 21.000.000 bitcoins. Non c'è nessuna possibilità di aumentare l'offerta per eguagliarla alla domanda esistente. Se più individui dovessero domandare più bitcoins, l'unico modo per incontrare la domanda consisterebbe nell'apprezzare l'offerta esistente. Ma dato che ogni bitcoin è suddivisibile in 100 milioni di satoshis, c'è molto spazio per la crescita di Bitcoin

[109] Saifedean Ammous, (2018). The Bitcoin Standard
[110] Ibidem
[111] Saifedean Ammous, (2018). The Bitcoin Standard
[112] "Why do Bitcoin have value?", www.investopedia.com

attraverso l'utilizzo di unità sempre più piccole dello stesso man mano che il valore aumenta. Ciò sancisce la scoperta di un nuovo bene adatto a svolgere il ruolo di riserva di valore.[113]

Prima dell'invenzione di Bitcoin, tutte le forme di moneta erano illimitate nella loro quantità, e quindi inadatte a svolgere il ruolo di riserva di valore. L'immutabile offerta monetaria di Bitcoin lo rende il miglior mezzo per immagazzinare valore, rendendolo quindi la migliore riserva di valore che l'umanità abbia mai visto. Per dirla diversamente, Bitcoin rappresenta l'alternativa più economica per comprare il futuro, in quanto è l'unico mezzo di cui si ha la garanzia che non verrà svalutato nel tempo, a prescindere da quanto aumenterà il suo valore.[114]

In passato, alcuni oggetti fisici furono usati come riserva di valore, la cui funzione non richiede necessariamente una manifestazione fisica, ma averla rende l'offerta di tale riserva difficile da aumentare. Bitcoin, non avendo alcuna manifestazione fisica ed essendo puramente uno strumento digitale, è in grado di raggiungere una rigorosa scarsità. Nessun materiale fisico divisibile e trasportabile aveva mai raggiunto questo prima ad ora. Bitcoin consente agli individui di trasportare valore digitalmente senza alcuna dipendenza dal mondo fisico, e permette di trasferire ingenti somme di denaro da ogni parte del mondo in pochi minuti. Bitcoin, quindi, potrebbe essere la miglior tecnologia per risparmiare mai inventata.[115]

2.3.3 Unità di conto

Dalla fine dell'era del gold standard, il commercio globale è stato profondamente ostacolato dalle differenze nel valore della moneta dei diversi paesi. Questo ha distrutto la capacità degli individui di condurre scambi indiretti utilizzando un unico mezzo di scambio e, al contrario, ha creato un mondo dove per acquistare qualcosa oltre i confini è necessario acquistare prima la valuta del produttore, imitando quasi il baratto. Ciò ha gravemente ostacolato la capacità degli individui di condurre calcoli economici oltre i confini del proprio paese, comportando la crescita di una massiccia industria dei cambi. Il gold standard ha offerto una soluzione a tale problema, in cui una sola forma di denaro, indipendente dal controllo di ogni singolo governo o autorità, era lo standard monetario globalmente riconosciuto. I prezzi poterono essere calibrati in relazione all'oro, facilitando i calcoli oltre i confini geografici dei paesi. A causa della sua natura fisica, tuttavia, esso doveva essere centralizzato e la sua regolazione doveva essere effettuata tra banche centrali. Una volta che l'oro divenne centralizzato, la

[113] "Gold or Bitcoin? Store of value debates rages as Bitcoin grows", www.bloomberg.com
[114] Ibidem
[115] "Bitcoin's intrinsic value: means of payment and store of value", www.invao.org

relativa domanda si dimostrò insostenibile per i governi, i quali ne presero il controllo e lo sostituirono con le monete fiat, la cui offerta è direttamente controllata dagli stessi.[116]

È una domanda aperta se Bitcoin potrebbe potenzialmente svolgere il ruolo di un'unità di conto globale per il commercio e l'attività economica. Affinché ciò fosse possibile, Bitcoin avrebbe bisogno di essere adottato da un numero di individui estremamente elevato, e che questi ultimi lo utilizzino come "moneta di riserva". Rimarrebbe poi da vedere se la stabilità dell'offerta di Bitcoin renderebbe stabile anche il valore di quest'ultimo, dato che le transazioni giornaliere rimarrebbero comunque marginali in relazione alle quantità detenute dai singoli individui. Dato che Bitcoin costituisce meno dell'1% dell'offerta monetaria globale, grandi transazioni individuali su Bitcoin possono avere un grande impatto sul prezzo, e piccole variazioni della domanda possono causare grandi oscillazioni del prezzo.[117] Questa, tuttavia, è una caratteristica della situazione attuale in cui Bitcoin, inteso come rete di regolamento globale e moneta, rappresenta ancora una frazione minima della rete globale di pagamenti e dell'offerta globale di moneta. Acquistare un token Bitcoin, oggi, può essere considerato un investimento nella rapida crescita della rete e nella moneta digitale come riserva di valore, perché è ancora molto piccola ed in grado di moltiplicare le sue dimensioni e il suo valore molto rapidamente.[118]

Se la quota di Bitcoin all'interno dell'offerta globale di moneta e nella rete di pagamenti internazionali dovesse diventare una quota maggioritaria del mercato globale, allora il suo livello della domanda diventerebbe molto più prevedibile e stabile, portando ad una stabilizzazione del valore della moneta. Ipoteticamente, Bitcoin dovrebbe diventare l'unica moneta utilizzata in tutto il mondo per fare in modo che il valore possa rimanere stabile nel tempo. A quel punto, la domanda di bitcoins sarà semplicemente una domanda per detenere denaro liquido, e l'aspetto speculativo che vediamo oggi dovrebbe scomparire. In una situazione del genere, il valore di Bitcoin varierebbe insieme alla preferenza temporale di tutti gli individui in ogni parte del mondo, e l'aumento della domanda di bitcoins come riserva di valore porterebbe solo a piccoli apprezzamenti del loro valore.[119]Nel lungo periodo, la prevedibilità dell'offerta unita alla crescita nel numero di utenti potrebbe rendere le fluttuazioni giornaliere della domanda determinanti meno significative del prezzo, in quanto i market maker sono in grado di coprire e regolare le fluttuazioni della domanda e dell'offerta, portando ad un prezzo più stabile.

[116] Saifedean Ammous, (2018). The Bitcoin Standard
[117] "Criptomoneta e distacco dalla moneta legale: il caso Bitcoin", rivista.dirittobancario.it, 2016
[118] "Bitcoin – Unità di conto Globale" by Fabrizio Angeloni. 2020
[119] Ibidem

2.4 La solidità di Bitcoin

2.4.1 L'evasione fiscale e la criminalità organizzata

Una delle principali miscredenze relative a Bitcoin presente fin dalla su creazione riguarda il fatto che tale criptovaluta possa essere utilizzata dai criminali e dai terroristi. Nel corso degli anni sono stati pubblicati numerosi articoli contenenti informazioni infondate circa il fatto che numerose gang di criminali utilizzano Bitcoin per finanziare le loro attività illegali. Molti di questi articoli sono stati successivamente revocati, ma non prima di aver impresso questa idea nella mente di molti individui.[120]La realtà è che il registro di Bitcoin è accessibile a livello globale e immutabile, di conseguenza conterrà tutte le registrazioni delle transazioni effettuate, persino di quelle servite per finanziare la criminalità.

Non è dunque corretto affermare che Bitcoin è anonimo, in quanto è piuttosto *pseudo-anonimo*. Infatti, è possibile stabilire collegamenti tra identità reali e indirizzi Bitcoin, consentendo così il monitoraggio completo di tutte le transazioni da parte di un indirizzo una volta che la sua identità è stata stabilita.[121]

Quando si parla di anonimato, è utile considerare Bitcoin anonimo tanto quanto Internet: l'anonimato è strettamente correlato a quanto bene un individuo riesce a nascondersi, e all'intensità con la quale gli "investigatori" ricercano il medesimo soggetto all'interno della blockchain. Contrariamente a quanto si possa pensare, la blockchain di Bitcoin rende molto più difficile nascondersi rispetto al Web. È facile disfarsi di un dispositivo, di un indirizzo e-mail o di un indirizzo IP e non utilizzarlo mai più, ma è difficile cancellare completamente ogni singola traccia di un indirizzo Bitcoin.[122]Tutto ciò significa che per qualsiasi crimine che veda la presenza di una vittima e di un criminale, sarebbe sconsigliato a quest'ultimo l'utilizzo di Bitcoin. Infatti, la sua natura pseudo-anonima comporta il fatto che ogni singolo indirizzo potrebbe essere ricollegato a identità del mondo reale, anche dopo molti anni dalla commissione del delitto. Lo stesso sentiero costituito dai pagamenti registrati all'interno del network è stato la ragione per cui sono stati identificati online numerosi spacciatori di droga, catturati a seguito della loro adozione di Bitcoin, ritenuta dagli stessi una moneta completamente anonima. Bitcoin è una tecnologia per il denaro, e quest'ultimo è qualcosa che può essere utilizzato dai criminali in qualsiasi momento. Qualsiasi forma di moneta può essere utilizzata dai criminali o per facilitare i crimini stessi, ma il registro permanente di Bitcoin lo rende poco appetibile per quei crimini nei quali le vittime potrebbero essere in grado di avviare un'indagine. Bitcoin può essere utile per facilitare "crimini senza vittime", nei quali l'assenza di queste ultime

[120] Saifedean Ammous, (2018). The Bitcoin Standard
[121] "Criptovaluta" da Wikipedia, l'enciclopedia libera
[122] Saifedean Ammous, (2018). The Bitcoin Standard

significherà che nessun individuo cercherà di scoprire l'identità del criminale. In realtà, non può esistere un crimine senza vittime, poiché qualora una determinata azione non dovesse ledere alcun individuo non sarebbe qualificabile come crimine.[123]Il medesimo discorso vale per tutti coloro che ritengono che Bitcoin possa facilitare l'evasione fiscale e il riciclaggio di denaro, a causa della temporanea assenza di meccanismi adeguati di tassazione dei profitti realizzati che potrebbero causare danni alle finanze dello Stato.

La pseudo-anonimità di Bitcoin e la perfetta trasparenza del registro delle transazioni rendono tali pratiche pressoché irrealizzabili. Inoltre, l'Australia è stato uno dei primi paesi ad introdurre un'apposita legge antiriciclaggio contro il finanziamento del terrorismo, al fine di mettere a punto meccanismi di tassazione dei profitti derivanti dalle criptovalute.[124]

Uno dei pochi crimini che ha effettivamente fatto affidamento su Bitcoin riguarda il cosiddetto "*ransomware*".[125] Esso si caratterizza da un accesso non autorizzato al computer della vittima per crittografare i suoi file, e rilasciarli successivamente solo dopo aver ottenuto un pagamento, solitamente per mezzo di Bitcoin. Questo forse rappresenta il miglior esempio nel quale Bitcoin potrebbe facilitare l'attività criminale. Tuttavia, tali *ransomware* non sfruttano eventuali debolezze di Bitcoin, bensì la mancanza di sistemi di sicurezza nei singoli computer. Un'azienda che rischia di avere il suo intero sistema informatico bloccato da un hacker anonimo che richiede il pagamento di qualche migliaio di dollari presenta problemi ben più gravi di quelli presentati da quest'ultimo. L'incentivo per gli hacker può essere nell'ordine delle migliaia di dollari, ma l'incentivo per la concorrenza della stessa azienda, per i suoi clienti e fornitori può essere di gran lunga maggiore. In effetti, il *ransomware* ha consentito l'individuazione di eventuali falle nei vari sistemi di sicurezza informatica, la quale sta portando le aziende a adottarne di migliori.[126]Mentre gli hacker possono temporaneamente beneficiare dalle pratiche di *ransomware*, nel lungo periodo le aziende riusciranno ad avere la meglio, essendosi attrezzate con gli opportuni sistemi di sicurezza informatica.

2.4.2 The 51% Attack

Una delle caratteristiche e dei principali punti di forza di Bitcoin e della tecnologia blockchain ad esso collegata è la natura distribuita dei processi di produzione e verifica dei dati. La rete decentralizzata dei nodi assicura che le regole del protocollo vengano rispettate e che tutti i

---

[123] Ibidem
[124] "Criptovaluta" da Wikipedia, l'enciclopedia libera
[125] "Con il termine *ransomware* si fa riferimento ad un particolare malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto da pagare per rimuovere la limitazione" da Wikipedia, l'enciclopedia libera
[126] "Attacco ai Bitcoin: di cosa si tratta, come funzionano e come proteggersi", cybersecurity360.it

partecipanti alla rete abbiano pareri non discordi sull'attuale stato della rete.[127]Inoltre, l'algoritmo di consenso Proof of Work garantisce che i miners possano aggiungere un nuovo blocco alla catena di transazioni solo se i nodi della rete concordano collettivamente sull'accuratezza di tale blocco.[128]

È bene specificare che le prestazioni di un miner si basano sulla potenza di calcolo che lo stesso mette a disposizione per compiere il processo di mining, indicata in genere come *hashrate* o *hashing power*, la quale è distribuita tra diversi nodi sparsi per il mondo, che quindi non è nelle mani di un singolo individuo o organizzazione.[129]Tuttavia, cosa succederebbe se la distribuzione dell'hashrate si dovesse sbilanciare? Cosa accadrebbe qualora una singola entità riuscisse ad ottenere più del 50% dell'hashing power?

Una possibile conseguenza è ciò che viene riconosciuto con il nome di "51% Attack"[130] o anche "attacco della maggioranza". Un attacco del 51% è un potenziale attacco verso un network blockchain, in cui una singola entità o organizzazione riesce a prendere il controllo della maggioranza della potenza di calcolo, causando potenziali danni. In tale scenario, l'attaccante disporrebbe di sufficiente *hashing power* per escludere di propria volontà delle transazioni o cambiarne l'ordine. Potrebbe anche invertire transazioni che ha effettuato mentre possedeva il controllo portando ad una situazione di "*double-spending*".[131] Un attacco della maggioranza di successo permetterebbe all'attaccante di impedire la conferma di una o più transazioni, oppure di ostacolare l'attività di mining degli altri miners, portando al cosiddetto "monopolio di mining". Invece, un attacco del genere non permetterebbe a colui che lo effettua di invertire le transazioni degli altri utenti, né di impedire alle transazioni di venire create e trasmesse alla rete. Modificare la ricompensa per blocco, creare monete dal nulla o rubare monete che non siano mai state di sua appartenenza sono altre azioni altamente improbabili che potrebbero essere tentate dall'attaccante.[132]

Quali sono le probabilità che si verifichi un 51% attack? Dato che una blockchain è mantenuta da una rete condivisa di nodi, tutti i partecipanti collaborano nel processo di raggiungimento del consenso. Inoltre, i network di dimensioni maggiori vantano una maggiore protezione contro attacchi di questo genere, ed è per questo che quella di Bitcoin è considerata la blockchain più sicura.

Nei primi anni dalla sua nascita, diversi miners si sono uniti alla rete di Bitcoin per contribuire alla sua crescita e sicurezza.[133] Successivamente, a seguito dell'aumento del prezzo di Bitcoin, nuovi miners si sono uniti con l'obiettivo di competere per ottenere la ricompensa assicurata dal blocco

[127] "Cos'è un 51% Attack", Binance Academy, 2018
[128] Ibidem
[129] Ibidem
[130] "Cos'è un 51% Attack", Binance Academy, 2018
[131] Vedi nota 66
[132] "Cos'è un 51% Attack", Binance Academy, 2018
[133] Ibidem

eventualmente aggiunto. Questo contesto di competizione è uno dei motivi per cui la rete di Bitcoin può essere considerata a tutti gli effetti sicura: i miners non hanno incentivo ad investire grandi quantità di tempo e risorse se non con lo scopo di operare onestamente per ricevere la ricompensa del blocco.[134]

Per questi motivi, un attacco della maggioranza ai danni di Bitcoin è piuttosto improbabile vista la grandezza e la sicurezza della rete. All'aumentare delle dimensioni di una blockchain, la possibilità che un singolo individuo o un'organizzazione sia in grado di controllare abbastanza potenza di calcolo da sopraffare gli altri partecipanti crolla rapidamente a livelli molto bassi. Inoltre, modificare i blocchi aggiunti in precedenza diventa sempre più complicato al crescere della catena, in quanto tutti i blocchi sono collegati ed è possibile modificarne uno solo se tutti i blocchi confermati successivamente vengono eliminati.[135] Per la stessa ragione, più alto è il numero di conferme di un blocco, maggiore risulterà il costo per alterare o invertire le transazioni contenute al suo interno. Di conseguenza, un attacco che riuscisse ad andare a buon fine otterrebbe probabilmente la modifica delle transazioni di pochi blocchi recenti, ma per un periodo di tempo piuttosto limitato. Anche se l'attaccante non fosse motivato dai profitti e riuscisse ad eseguire un attacco al 51% con successo, il protocollo di Bitcoin verrebbe modificato rapidamente in risposta all'attacco subito.[136]

2.4.3 Gli attacchi ad Internet e alle strutture informatiche e di comunicazione

Uno dei malintesi più diffusi riguardanti Bitcoin è che quest'ultimo può essere danneggiato o bloccato a seguito del danneggiamento di Internet o delle importanti infrastrutture di comunicazione sulle quali Bitcoin si basa. Il problema principale di questi scenari riguarda il fatto che essi considerano Bitcoin come se esso fosse una rete nel senso tradizionale di insieme di hardware e infrastrutture dedicate che presentano punti critici, e che quindi possono essere facilmente attaccate e compromesse.[137]

Tuttavia, Bitcoin è un protocollo software; è un processo interno che può essere eseguito su uno qualsiasi dei miliardi di computer distribuiti in tutto il mondo. Bitcoin non ha un singolo punto debole e nemmeno una singola struttura hardware indispensabile sulla quale di basa in una qualsiasi parte del mondo. Da questo punto di vista, si potrebbe affermare che Bitcoin è simile ad Internet, in quanto identifica un protocollo che permette ai computer di potersi collegare tra di loro, e non rappresenta l'infrastruttura che li collega.[138]La quantità di dati richiesta per trasmettere informazioni su Bitcoin non è molto grande e rappresenta solo una piccola frazione della quantità totale di traffico presente

[134] Ibidem
[135] "Cos'è un 51% Attack", Binance Academy, 2018
[136] Ibidem
[137] Saifedean Ammous, (2018). The Bitcoin Standard
[138] "Internet e Bitcoin: due tecnologie odiate a confronto", 2018, medium.com

su Internet. Inoltre, Bitcoin non ha bisogno di un'infrastruttura così estesa come il resto di Internet, perché la sua blockchain ha bisogno solamente di trasmettere 1 megabyte di dati ogni dieci minuti. Esistono innumerevoli tecnologie cablate e wireless per la trasmissione di dati in tutto il mondo, e ogni singolo utente ha bisogno solo di una di queste per essere in grado di connettersi alla rete.[139]

Per creare un mondo in cui nessun utente Bitcoin sia in grado di connettersi con gli altri utenti, la portata del disastro che sarebbe necessario che si verifichi nei confronti delle informazioni, dei dati e delle infrastrutture di connettività mondiali dovrebbe essere assolutamente devastante. La vita della società moderna dipende in larga misura dalla connettività, e molti servizi vitali e questioni di vita o di morte si basano continuamente su queste infrastrutture di comunicazione. Quindi, provare a disattivare tutte le infrastrutture dell'Internet contemporaneamente potrebbe causare danni significativi a qualsiasi società senza riuscire però ad arginare il flusso di Bitcoin, in quanto i dispositivi isolati possono sempre connettersi tra di loro utilizzando protocolli e informazioni criptate.[140] Ci sono semplicemente troppi computer e connessioni sparsi per tutto il mondo, utilizzati da un numero incalcolabile di individui, perché una qualsiasi forza sia in grado di farli smettere di funzionare simultaneamente. L'unico scenario immaginabile in cui ciò potrebbe accadere sarebbe attraverso una sorta di scenario apocalittico dopo il quale non rimarrebbe nessun individuo a chiedersi se Bitcoin risulti ancora operativo o meno.

Per questi motivi, di tutte le minacce che vengono menzionate nei confronti di Bitcoin, probabilmente questa è quella meno credibile e significativa.

2.5 Bitcoin e la sostenibilità ambientale

Come già citato in precedenza, la creazione di nuovi bitcoins avviene grazie ad un processo chiamato *mining*, che prevede la risoluzione di complessi problemi matematici. Perciò, tale processo presuppone che i vincitori saranno coloro che metteranno a disposizione del network una potenza di calcolo maggiore rispetto agli altri, aggiudicandosi così la ricompensa prevista.[141] La creazione di nuovi bitcoins richiede dunque il lavoro di numerosissimi computer ad alta potenza che utilizzino, quindi, una elevata quantità di energia elettrica, generata per il 60% dall'impiego di combustibili fossili, tra cui il carbone.[142]

Lo stesso Elon Musk, in data 13 maggio 2021, ha pubblicato un post su Twitter dove affermava che Tesla avrebbe sospeso ogni tipo di pagamento che avesse ad oggetto Bitcoin a causa del largo uso di

[139] Ibidem
[140] Saifedean Ammous, (2018). The Bitcoin Standard
[141] "I Bitcoin e l'inquinamento: anche il mondo digitale crea emissioni", 2021. www.abenergie.it
[142] "Bitcoin" da Wikipedia, l'enciclopedia libera

combustibili fossili utilizzati per portare a termine ogni singola transazione.[143] Infatti, una sola transazione in Bitcoin consuma circa quanto 1.122.196 pagamenti con una carta Visa, i quali equivalgono a 36 giorni di consumo elettrico di una casa di una famiglia media americana. Inoltre, qualora il prezzo delle criptovalute e di Bitcoin dovesse salire, allo stesso modo salirebbero i consumi elettrici necessari per le transazioni.[144] Questo spiega come nel 2019 il consumo di elettricità del Bitcoin si è quadruplicato rispetto all'anno precedente, e, nello stesso anno, è stato stimato che le attività di mining in tutto il mondo attingono a fonti di energia con un ritmo di circa 120 terawattora all'anno, pari al consumo di una nazione di medie dimensioni.[145]

Il dato più preoccupante riguarda le emissioni di anidride carbonica provocate dall'estrazione di Bitcoin si attestano tra le 22 e le 22,9 tonnellate in un anno, livelli equivalenti a quelli prodotti dalla Giordania e dallo Sri Lanka. Tali numeri, poi, potrebbero addirittura moltiplicarsi qualora venga preso in considerazione, oltre a Bitcoin, il consumo energetico collegato a tutte le altre criptovalute.[146] Una valida idea che potrebbe essere impiegata nel futuro allo scopo di ridurre il livello di inquinamento causato dall'utilizzo delle criptovalute potrebbe essere quella proposta da Arun Ghosh, esperto di blockchain di KPMG.[147]

Secondo Ghosh, la blockchain assieme all'Internet of Things potrebbe finalmente rappresentare una soluzione alla gestione delle emissioni di CO2. La blockchain, in accordo con tale visione, potrebbe rivelarsi un utile strumento in grado di immagazzinare i dati raccolti dai sensori che monitorano costantemente l'inquinamento idrico e atmosferico, gestendone al contempo la compensazione automatica attraverso gli smart contracts.

Esistono, inoltre, alcuni progetti simili che prevedono l'uso della blockchain per migliorare il sistema delle cosiddette transazioni di crediti di carbonio. Il progetto più conosciuto è forse quello relativo ad Ibm, che grazie ad Energy Blockchain Labs[148] ha creato una piattaforma blockchain efficiente e trasparente capace di consentire alle organizzazioni ad alte emissioni di monitorare costantemente la propria impronta di carbonio e acquistare i crediti che servono a bilanciare le emissioni.

Secondo Ibm, la sua adozione potrebbe portare in 10 mesi ad una riduzione del 20 – 50% delle emissioni. Tale esperimento per ora è in fase di test in Cina, responsabile di circa un quarto delle

[143] Elon Musk on Twitter: Tesla & Bitcoin. www.twitter.com
[144] "Quanto inquinano I Bitcoin? L'impatto sull'ambiente e l'alternativa ecosostenibile", 2021. Corriere della Sera
[145] "Quanto inquinano I Bitcoin? L'impatto sull'ambiente e l'alternativa ecosostenibile", 2021. Corriere della Sera
[146] Ibidem
[147] "Quanto inquinano I Bitcoin? L'impatto sull'ambiente e l'alternativa ecosostenibile", 2021. Corriere della Sera
[148] Energy Blockchain Labs Inc., IBM

emissioni mondiali di biossido di carbonio.[149] Ma Cao Yin, fondatore di Energy Lab, spiega che potrebbe essere presto disponibile al resto del mondo:

"*Vogliamo creare un nuovo ecosistema energetico per le persone che parte dalle persone e vogliamo produrre un diverso tipo di energia verde, molto più economica in tutto il mondo, non solo in Cina"*[150]

Un altro progetto altrettanto valido riguarda la startup americana Nori[151], in procinto di lanciare una piattaforma aperta basata sulla blockchain con lo scopo di compensare le emissioni di CO2. In questo caso, la soluzione è rappresentata dal fatto che le aziende che la adotteranno potranno azzerare la loro impronta di carbonio acquistando crediti di compensazione delle emissioni usando una criptovaluta: ad ogni tonnellata di CO2 rimossa verrà assegnato un Nori, cioè una sorta di bitcoin destinato ad aumentare di valore nel mercato futuro del carbonio sulla base della domanda e dell'offerta di certificati.[152] Così, secondo gli sviluppatori, sarà facile stabilire un prezzo di riferimento unico globale per l'anidride carbonica: una tonnellata varrebbe sempre e comunque un Nori. E, secondo tale progetto, l'anidride carbonica da prodotto di scarto diventerebbe un vero e proprio generatore di valore. I proventi, tolta una commissione pari al 10%, verrebbero infatti usati per finanziare gli agricoltori che aderiscono a programmi di agricoltura rigenerativa, volta a incrementare la capacità del terreno di trattenere l'anidride carbonica.[153]

[149] "Come la blockchain può aiutare la lotta all'inquinamento", 2020. Eugenio Spagnuolo via Wired
[150] Ibidem
[151] Nori, Crypto with a Cause. www.nori.com
[152] "Come la blockchain può aiutare la lotta all'inquinamento", 2020. Eugenio Spagnuolo via Wired
[153] Ibidem

Capitolo 3: Le alternative coins

3.1 Le alternative coins: che cosa sono e a cosa servono

Sebbene Bitcoin sia stato il primo esempio di moneta elettronica peer-to-peer, non è stato certamente l'ultimo. Una volta che il design di Nakamoto è uscito allo scoperto e la valuta è riuscita a guadagnare valore e adottanti, in molti l'hanno copiata con lo scopo di creare tecnologie simili. Namecoin[154] è stata la prima valuta di questo tipo, che ha utilizzato il codice Bitcoin ed ha iniziato ad operare nell'aprile 2011. Secondo coinmarketcap.com[155], sono 1042 le valute digitali messe a punto nell'arco di tempo che va dalla creazione di Bitcoin fino a Marzo 2022. Diversamente dal pensiero comune che queste valute esistano con lo scopo di competere con Bitcoin e poterlo sorpassare in futuro, in realtà esse non sono in competizione con quest'ultimo in quanto non potranno mai avere le proprietà che rendono Bitcoin l'unica moneta elettronica completamente affidabile. Affinché una data tecnologia possa funzionare come moneta digitale, deve essere completamente svincolata dal controllo di terzi; il suo funzionamento deve essere conforme alla volontà dell'utente secondo il protocollo, senza la possibilità per terzi di interferire nelle transazioni. Dopo anni di continue creazioni di numerose alternative coins, sembra impossibile che una qualsiasi moneta digitale ricrei il medesimo stallo contraddittorio che esiste tra i possessori di bitcoins e impedisca a qualsiasi utente di controllare pagamenti all'interno della tecnologia blockchain.[156]

Bitcoin è stato progettato da un programmatore noto solamente per mezzo di uno pseudonimo, la cui vera identità è ancora sconosciuta. Egli ha inviato il progetto ad una oscura mailing list per programmatori di computer interessati alla crittografia e, dopo aver ricevuto svariati feedback sul proprio progetto nel corso di alcuni mesi, ha lanciato la rete con il defunto programmatore Hal Finney, scomparso nell'agosto 2014. Dopo alcuni giorni di transazioni con Finney e di esperimenti con il software, diversi membri hanno cominciato ad unirsi alla rete per effettuare transazioni e per dedicarsi

[154] Fonte: www.namecoin.org
[155] https://coinmarketcap.com/coins/views/all/
[156] Saifedean Ammous, (2018). The Bitcoin Standard

al mining. Nakamoto scomparve a metà del 2010, affermando di "spostare l'attenzione verso nuovi progetti"[157], e molto probabilmente nessun individuo da allora ha mai più avuto sue notizie. Con ogni probabilità, vi sono almeno 1 milione di bitcoins detenuti in un portafoglio che è oppure è stato di proprietà dello stesso Nakamoto, e tali monete non sono mai state utilizzate. Nakamoto utilizzò la massima cautela per assicurarsi che non venisse mai identificato, e fino ad oggi non ci sono prove convincenti per identificare chi sia il vero Nakamoto. Tutti i suoi scritti e le sue comunicazioni sono stati esaminati ossessivamente da investigatori e giornalisti senza alcun risultato. Poiché Nakamoto e Finney non sono più con noi, Bitcoin non ha avuto alcuna figura di autorità centrale o leader che potesse dettarne la direzione o esercitarne l'influenza nel corso del suo sviluppo. Persino Gavin Andresen, che era in stretto contatto con Nakamoto, nonché uno dei volti maggiormente identificabili di Bitcoin, ha fallito ripetutamente nell'esercitare influenza sulla direzione dell'evoluzione di Bitcoin.[158] Bitcoin ha continuato a crescere e prosperare, mentre l'autorità di qualsiasi individuo o organizzazione su di esso è diminuita fino al punto da diventare insignificante. Bitcoin può essere inteso come un pezzo di codice sovrano, in quanto non esiste alcuna autorità al di fuori di esso che possa controllarne il comportamento. Solamente le regole di Bitcoin sono in grado di controllarlo, e la possibilità di modificare queste regole in qualsiasi modo è diventata estremamente impraticabile. È la sovranità del codice Bitcoin, supportata dalla tecnologia proof-of-work, che rende quest'ultimo una soluzione completamente efficace al problema della doppia spesa, nonché una moneta digitale di successo. Ed è proprio questa caratteristica che le altre monete digitali non riescono a replicare. Infatti, guardando in faccia ad ognuna delle altre criptovalute create dopo Bitcoin si assiste ad una profonda crisi esistenziale: Bitcoin esiste già, e presenta una sicurezza, una potenza di calcolo e una base utenti già consolidata che le altre valute digitali difficilmente potranno raggiungere. Inoltre, ogni individuo non avrà alcun incentivo ad adottare una criptovaluta più piccola e meno sicura rispetto a Bitcoin. Poiché la replica del codice necessario a generare una nuova criptovaluta presenta costi pressoché inesistenti e le alternative disponibili aumentano sempre di più, è molto probabile che nessuna valuta digitale registrerà alcun tipo di crescita o slancio significativo a meno che non ci sia un team attivo dedicato a coltivarla, farla crescere, proteggerla e aggiornarla continuamente.[159] Essendo la prima invenzione di questo tipo, Bitcoin ha dimostrato che il suo valore e la sua solidità come valuta digitale sono stati sufficienti per garantire una domanda in costante crescita, permettendole così di avere successo anche se l'unica persona dietro a tale progetto era un programmatore anonimo che non ha speso alcuna somma per promuovere tale tecnologia. Essendo fondamentalmente imitazioni che sono molto facili da ricreare, tutte le alternative coins non possiedono il lusso di avere una domanda in costante espansione, ragion per cui devono costruire e

[157] "Satoshi's final statement", Bitcoin Stack Exchange
[158] "Bitcoin project blocks out Gavin Andresen over Satoshi Nakamoto claims", www.theguardian.com
[159] Saifedean Ammous, (2018). The Bitcoin Standard

aumentare attivamente tale domanda. Questo è il motivo per cui praticamente tutte le *altcoins* hanno un team al comando delle stesse; il quale ha lanciato il progetto, lo ha commercializzato, ne ha progettato le opportune strategie di marketing ed infine lo ha inserito nei comunicati stampa alla stregua delle notizie che vediamo ogni giorno, avendo così anche il vantaggio di minare un gran numero di monete prima che qualcuno ne avesse sentito parlare.[160]

Questi team sono individui noti pubblicamente e, per quanto ci provino, non possono dimostrare in alcun modo credibile di non avere alcun controllo sulla direzione della valuta. Perciò, dopo la creazione di Bitcoin, chiunque tenti di costruire una criptovaluta alternativa avrà successo solamente qualora investisse ingenti somme in tale progetto, rendendolo effettivamente sotto il suo controllo. E finché esisterà un individuo o organizzazione con potere sovrano su una valuta digitale, allora quest'ultima non potrà essere intesa come una forma di moneta, ma piuttosto una forma di pagamento intermedio e molto inefficiente.[161] Ciò presenta un dilemma che i progettisti di altcoins affrontano costantemente: senza una gestione attiva da parte di un team di sviluppatori e marketers, nessuna valuta digitale attirerà mai l'attenzione e il capitale del pubblico in un mare di oltre 1.000 altcoins. Tuttavia, con la gestione attiva, lo sviluppo e l'implementazione delle campagne di marketing da parte di un team, la moneta in questione non potrà dimostrare in modo credibile di non essere controllata da questi individui. Con un gruppo di sviluppatori che controlla la maggior parte delle monete, la potenza di elaborazione e l'esperienza di codifica, la valuta è praticamente centralizzata, al pari di tutte le monete fiat esistenti, in cui gli interessi del team determinano il suo percorso di sviluppo.[162]Non c'è nulla di sbagliato in una valuta digitale centralizzata; tuttavia, c'è qualcosa di profondamente sbagliato in una valuta digitale centralizzata che adotta un design altamente ingombrante ed inefficiente il cui unico vantaggio consiste nella rimozione di un singolo svantaggio. Tale problema è più pronunciato per le valute digitali che iniziano con un'offerta iniziale di monete, la quale crea un gruppo completamente trasparente di sviluppatori che comunica pubblicamente con gli investitori, rendendo l'intero progetto effettivamente centralizzato. I tentativi e le continue tribolazioni di Ethereum, la moneta digitale più grande in termini di valore di mercato dopo Bitcoin, illustrano vividamente questo punto.

L'Organizzazione Autonoma Decentralizzata (DAO)[163] è stata la prima implementazione di contratti intelligenti sulla rete di Ethereum. Dopo che oltre 150 millioni di dollari furono investiti in questo progetto, un utente malintenzionato è stato in grado di eseguire il codice, dirottando così un terzo di tutte le risorse del DAO direttamente sul proprio account.[164] Sarebbe probabilmente inesatto

[160] Saifedean Ammous, (2018). The Bitcoin Standard
[161] ibidem
[162] Ibidem
[163] "Decentralized Autonomous Organization", da Wikipedia, l'enciclopedia libera
[164] "The DAO Attack: Understanding What Happened", www.coindesk.com

descrivere questo attacco come un furto, perché tutti i depositanti avevano accettato il fatto che i loro soldi sarebbero stati controllati dal codice e da nessun'altro, e l'attaccante non ha fatto altro che eseguire il codice accettato da tutti i depositanti. All'indomani dell'attacco DAO, gli sviluppatori di Ethereum crearono una nuova versione di quest'ultimo in cui fino ad ora non si è mai verificato questo scomodo errore, confiscando i fondi dell'attaccante e distribuendoli alle vittime in proporzione all'investimento effettuato. Tuttavia, se la seconda rete più grande al mondo in termini di potenza di elaborazione può avere il suo record blockchain alterato quando le transazioni non sono conformi agli interessi del team di sviluppo, allora l'idea che una qualsiasi tra le alternative coins sia effettivamente regolata solamente dalla potenza di elaborazione non è affatto credibile. La concentrazione di proprietà di valuta, la potenza di elaborazione e la capacità di programmazione nelle mani di un gruppo di persone che sono effettivamente partner di un'impresa vanifica l'intero scopo di utilizzare una struttura blockchain. Inoltre, risulta assai difficile prevedere che tali criptovalute emesse privatamente raggiungeranno effettivamente lo status di valuta globale pur avendo alle spalle un team visibile. Se tali valute digitali centralizzate si dovessero apprezzare in modo significativo, un piccolo team di creatori diventerebbe estremamente ricco e dotato del potere di riscuotere anzianità, un ruolo riservato agli Stati-Nazione nel mondo moderno.[165] Le banche centrali e i governi nazionali non accetteranno di buon grado questo indebolimento della loro autorità e sarebbe relativamente facile per loro convincere uno o più membri dei team dietro a tali valute a distruggerle o alterarne il funzionamento in modo da impedire loro di competere con le valute nazionali.

Nessuna *altcoin* ha mai dimostrato nulla di simile all'impressionante resilienza al cambiamento di Bitcoin, dovuta alla sua natura veramente decentralizzata e ai forti incentivi per tutti a rispettare le regole del consenso dello status quo. Bitcoin può vantare questo traguardo dopo essere sopravvissuto per oltre nove anni nelle terre selvagge di Internet, senza alcuna autorità che avesse il potere di controllarlo, e dopo aver respinto numerose campagne altamente coordinate e ben finanziate per alterarlo. In confronto, le *altcoins* presentano la cultura inconfondibile di individui carismatici che lavorano insieme su un progetto di squadra. Anche se questo sarebbe ottimo per una nuova start-up, esso rappresenta un grosso impedimento per un progetto che vuole dimostrare un impegno credibile verso una politica monetaria fissa. Se i team dietro ad una particolare altcoin decidessero di cambiare la sua politica monetaria, ciò rappresenterebbe un compito relativamente facile da portare a termine. Ethereum, ad esempio, non ha ancora chiara quale sarà la sua politica monetaria in futuro, lasciando la questione alla discussione della propria comunità.[166]

[165] Saifedean Ammous, (2018). The Bitcoin Standard
[166] "Ethereum Road Map", www.ethereum.org

Anche se questo può fare miracoli per lo spirito della comunità di Ethereum, non rappresenta il modo corretto per costruire una moneta globale. Che sia perché sono consapevoli di questo punto, o per evitare scontri con l'autorità politica, la maggior parte delle alternative coins non si commercializza come un concorrente di Bitcoin, bensì come una valuta volta a perseguire scopi differenti da quest'ultimo. Tuttavia, il fatto che le nuove app richiedano la propria valuta decentralizzata rappresenta la speranza disperatamente ingenua che risolvere in qualche modo il problema della mancanza di coincidenza dei desideri possa essere economicamente redditizio.[167] C'è una ragione per cui le aziende del mondo reale non emettono la propria moneta, ed è per il fatto che nessuno vuole detenere valuta spendibile solo in un'azienda. Il punto di detenere denaro consiste nel detenere liquidità che può essere spesa il più facilmente possibile. Detenere forme di denaro che possono essere spese solo presso particolari fornitori offre pochissima liquidità, ed è praticamente inutile. Gli individui preferiranno naturalmente detenere mezzi di pagamento liquidi, e qualsiasi azienda che insista sul pagamento per mezzo della propria valuta di libero scambio introdurrà solamente costi e rischi significativamente elevati per i suoi potenziali clienti. Anche nelle aziende che richiedono una qualche forma di token operativo, come nei parchi divertimento o nei casinò, il valore di questo è sempre fisso rispetto al denaro liquido, permettendo così ai clienti di essere consapevoli in ogni momento di ciò che stanno ottenendo e di fare calcoli economici accurati.[168]Non c'è nulla di originale o difficile nel copiare il design di Bitcoin producendo così un *copycat* leggermente diverso dall'originale, e migliaia di individui lo hanno già fatto. Con il tempo, ci si può aspettare che un numero sempre più elevato di queste monete entreranno nel mercato, diluendo il marchio di tutte le altre *altcoins*. Le valute digitali diverse da Bitcoin sono, nel complesso, *easy money*.

3.2 Alcune delle principali *alternative coins* degne di nota

3.2.1 Ethereum

Ethereum è una blockchain di seconda generazione, inventata nel 2013 da Vitalik Buterin, che era stato precedentemente il cofondatore del periodico *Bitcoin Magazine*[169]. Buterin cercò di capire essenzialmente come creare una piattaforma che avesse delle caratteristiche in comune con Bitcoin, ma che potesse essere utilizzata per costruire delle applicazioni più complesse, come le assicurazioni decentralizzate o nuovi strumenti finanziari. Per questo motivo, Ethereum è stato concepito come una piattaforma che permette di implementare i cosiddetti "smart contract"[170], agenti autonomi che

[167] Saifedean Ammous, (2018). The Bitcoin Standard
[168] Ibidem
[169] "Vitalik Buterin", da Wikipedia, l'enciclopedia libera
[170] Vedi nota 83

vivono sulla blockchain e permettono di creare applicazioni di nuovo tipo che non hanno bisogno di intermediari e che sfruttano le caratteristiche base di Bitcoin ma con una flessibilità che permette ad un qualsiasi sviluppatore medio di interagire con la complessità della blockchain e di studiare dei casi d'uso nuovi.

Una delle più importanti applicazioni di Ethereum nel mondo odierno è relativa alla cosiddetta DeFi[171], termine che si usa per indicare la finanza decentralizzata, la quale offre i medesimi servizi della finanza tradizionale, ma in più anche la possibilità per le aziende di creare le proprie monete virtuali all'interno della blockchain di Ethereum. La DeFi offre inoltre la possibilità, qualora si disponga di una certa quantità di ETH, la valuta nativa di Ethereum, o di altre criptovalute, di richiedere un prestito e di utilizzare le proprie criptovalute come collaterale, esattamente come nel caso di un mutuo. Un'altra funzionalità offerta dalla DeFi riguarda i cosiddetti *Flash Loan*[172], i quali consentono di prendere a prestito un certo ammontare di criptovalute e farci determinate operazioni purché chi riceve il prestito sia in grado di ritornare la somma nella stessa transazione. Tali *flash loans* vengono più frequentemente utilizzati per chiudere delle posizioni di prestito e aprirne delle nuove allo stesso tempo.

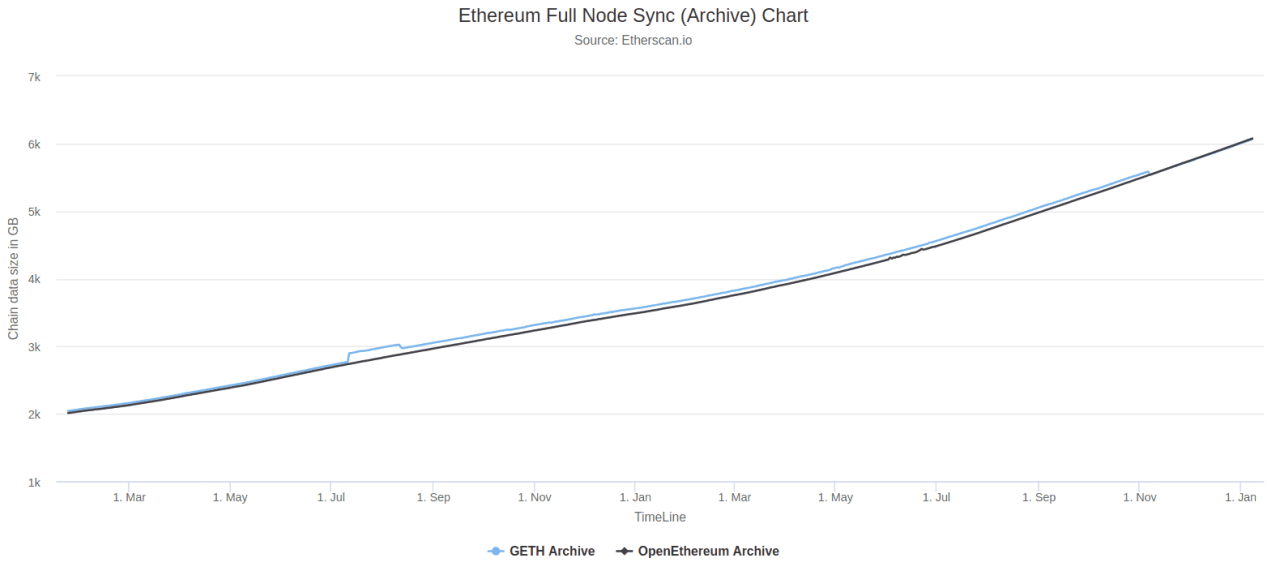
Ethereum, tuttavia, al pari di tutte le altre criptovalute, presenta problemi legati per lo più alla scalabilità, alla sicurezza e alla sostenibilità.[173]

Dovendo fare un enorme e dispendioso lavoro computazionale, Ethereum dovrà consumare un elevato ammontare di energia elettrica, specialmente durante il processo di validazione delle transazioni (*proof of work*). Inoltre, il tutto diviene ancora più problematico dato il fatto che vi è una relazione diretta tra la crescita di Ethereum e i problemi legati all'inquinamento.

Ethereum, pagando il prezzo della decentralizzazione, e quindi di possedere così tanti nodi che lavorano in sincrono per garantire sicurezza e trasparenza, è in grado di sostenere un numero piuttosto basso di transazioni al secondo (circa venti)[174], le quali possono essere sufficienti per il momento dato che l'intero progetto rappresenta ancora un interesse di nicchia; tuttavia, un tale numero risulterà sempre meno soddisfacente all'aumentare degli individui che decidono di possedere ETH. Oltre a ciò, Ethereum con il tempo diventa sempre più "grande": la lista di transazioni all'interno della propria blockchain, man mano che si espande, raggiunge picchi di potenza informatica sempre più importanti. Come si può vedere dal grafico[175], al momento le dimensioni di Ethereum si attestano sui 6 terabyte.

---

171 "Finanza decentralizzata (DeFi)", www.ethereum.org
172 "Cosa sono i flash loan nella DeFi?", Binance Academy
173 Fonte: www.ethereum.org
174 "La scalabilità blockchain e criptovalute", www.criptonauti.it
175 "Nodes and clients", www.ethereum.org



Tale problema è di fatto ineliminabile, sicché diminuire le dimensioni della lista significherebbe eliminare un certo numero di transazioni ivi contenute, andando quindi contro al concetto stesso di blockchain.

Ethereum presenta una road map[176] ben definita che, nel lungo termine, consentirà di risolvere appieno i principali problemi della piattaforma stessa. Lo strumento principale mediante il quale risolvere tali problemi è rappresentato da Ethereum 2.0[177], il quale è la risultante dei continui e molteplici upgrades che sono stati effettuati nel tempo su Ethereum 1.0. Ethereum 2.0 rappresenta un update sostanziale che cambierà proprio l'intero funzionamento della piattaforma, a partire dal meccanismo di consenso proof-of-work che verrà convertito in un meccanismo *proof-of-stake*[178]. In secondo luogo, verrà migliorata anche la scalabilità, permettendo di effettuare molte più transazioni al secondo e facendo in modo allo stesso tempo che i nodi abbiano un peso informatico minore. Eliminando poi i *miners* che devono minare le transazioni, produrre lavoro e consumare energia, si andranno a diminuire drasticamente le emissioni, risolvendo in parte il problema legato alla sostenibilità ambientale.[179]

Entrando maggiormente nello specifico per quanto riguarda la road map di Ethereum, quest'ultima si articola in cinque diverse fasi che scompongono in step il passaggio da Ethereum a Ethereum 2.0. La prima fase (phase 0) è consistita nel lancio della *ruth chain*[180] che opera parallelamente ad Ethereum,

[176] "Road Map", www.ethereum.org
[177] "Ethereum 2.0, che cos'è e perché è così importante", www.tomshw.it
[178] "Ethereum: problemi di scalabilità – PoS non basta?", www.critptovaluta.it; per maggiori approfondimenti si guardi la pagina web relativa al meccanismo di consenso Proof of Stake fornita da Wikipedia.
[179] Fonte: www.ethereum.org

[180] Con questo termine si fa riferimento alla "beacon chain", introdotta da Ethereum nel Dicembre 2020, la quale ha introdotto ufficialmente il meccanismo di consenso proof of stake

con l'obiettivo di fissare le basi per il successivo lancio di Ethereum 2.0 senza interrompere l'operatività dello stesso Ethereum. La seconda fase (phase 1) ha visto l'attivazione dello sharding, con l'introduzione delle *shard chain*[181] utilizzate però soltanto per il salvataggio dei dati. La terza fase (phase 1,5) consisterà nell'abbandono di Ethereum e del meccanismo proof-of-work a favore di Ethereum 2.0 e del meccanismo di consenso proof-of-stake, con la contestuale implementazione della *eth2 chain*[182]. Successivamente, la quarta fase (phase 2) prevede che gli shard vengano supportati appieno, includendo qualsiasi tipo di transazioni. Infine, dalla quinta fase (phase 3+) in poi, l'obiettivo principale della piattaforma è quello di migliorare continuamente la scalabilità, la sicurezza e l'efficienza, cercando al contempo di diminuire sempre di più le emissioni. [183]

3.2.2 Cardano

Lo sviluppo del progetto Cardano ha avuto inizio nel 2015 ed è stato infine lanciato nel 2017 da Charles Hoskinson, matematico e co-fondatore di Ethereum[184]. Hoskinson, dopo aver lasciato Ethereum, ha co-fondato "Yosh", una società di ingegneria blockchain la cui attività principale consiste nello sviluppo dello stesso Cardano, svolta insieme alla Fondazione Cardano e alla società Emurgo[185].

La piattaforma prende il nome da Gerolamo Cardano, un importante matematico italiano tra i più influenti durante il Rinascimento, mentre la criptovaluta "ADA", ossia la coin nativa della blockchain di Cardano, prende il nome dalla contessa Ada Lovelace, matematica e scrittrice inglese nota per essere considerata uno dei primi programmatori di computer.

Cardano afferma di superare i limiti esistenti nel mercato delle criptovalute, con riferimento principalemente alla lentezza e rigidità di Bitcoin e all'insicurezza e bassa scalabilità di Ethereum, ed è considerato dai suoi sviluppatori una criptovaluta di terza generazione, famosa per essere il primo progetto blockchain sviluppato seguendo una filosofia scientifica da un team di accademici e ingegneri.

Cardano è inoltre il primo protocollo blockchain decentralizzato peer review che utilizza un approccio scientifico. Per peer review, in italiano "revisione paritaria"[186], si intende, nel mondo della ricerca e dell'università, la revisione critica che un lavoro o una pubblicazione riceve da un ente centrale o da

[181] Con questo termine si fa riferimento ad una tecnologia che verrà introdotta da Ethereum nel 2023, al fine di migliorare la scalabilità e l'efficienza della piattaforma stessa
[182] "Ethereum upgrades (formerly eth2)", www.ethereum.org
[183] Fonte: www.ethereum.org
[184] "Charles Hoskinson", da Wikipedia, l'enciclopedia libera
[185] "Cardano (criptovaluta)", da Wikipedia, l'enciclopedia libera
[186] "Cardano: What Is Peer Review?", www.medium.com

specialisti del settore; e, in questo contesto, si intende che tutti i cambiamenti e le nuove funzionalità devono essere sviluppate, previste e concordate dagli accademici prima di entrare in vigore. Questo processo costringe gli autori ad adeguarsi ai migliori livelli di qualità e performance; tuttavia, nonostante i risultati ottimizzati, tutto ciò comporterà anche delle tempistiche molto più lunghe.

Secondo Hoskinson, l'umanità ha attraversato tre diverse generazioni blockchain: la prima fa riferimento alla generazione di Bitcoin e del trasferimento di denaro, la quale rispose alle esigenze degli individui di potersi scambiare denaro tra di loro, senza però prevedere la possibilità di aggiungere determinate condizioni a tali transazioni, le quali avrebbero avuto bisogno di script molto complessi. La soluzione fu fornita dai cosiddetti *smart contracts*[187], o contratti intelligenti, i quali aiutarono a scambiare denaro, proprietà, azioni o qualsiasi altra cosa di valore in modo trasparente e senza conflitti, evitando i servizi di intermediazione. Nacquero così le blockchain di seconda generazione con l'avvento di Ethereum, le quali hanno dimostrato al mondo come la blockchain possa evolversi da un semplice meccanismo di pagamento a qualcosa di molto più significativo e potente. Tuttavia, anche questa generazione presentava diversi problemi, riguardanti principalmente la scalabilità e la governance. Hoskinson sapeva che la blockchain avrebbe dovuto evolversi ancora di più, e così radunò gli elementi positivi delle prime due generazioni e aggiunse alcuni elementi propri, ottenendo come risultato la blockchain di terza generazione conosciuta come Cardano.[188]

Cardano punta a risolvere il famoso trilemma della blockchain[189], e riuscire quindi ad ottenere il massimo risultato per quanto riguarda la scalabilità, l'interoperatività e la sostenibilità. Per scalabilità, gli individui fanno invariabilmente riferimento al numero di transazioni al secondo e alla velocità effettiva; tuttavia, secondo Hoskinson, tutto ciò rappresenta soltanto una parte del problema: la scalabilità totale presenta a sua volta altri due elementi, i quali sono la rete e il ridimensionamento dei dati. Per quanto riguarda la velocità effettiva, Bitcoin gestisce 7 transazioni al secondo, mentre Ethereum circa 20, il che non è nemmeno lontanamente accettabile per un sistema finanziario: basti pensare al fatto che Visa gestisce circa 24 mila transazioni al secondo. Cardano ha quindi pensato di risolvere questo problema implementando un meccanismo di consenso conosciuto con il nome "Ouroborus"[190], il quale è un algoritmo proof-of-stake sicuro e revisionato secondo il processo di revisione paritaria.

Ouroborus deriva da "uroboro", termine che fa riferimento ad un simbolo molto antico rappresentante un drago o un serpente che si morde la coda, così formando una figura senza un inizio e senza una

---

[187] Vedi nota 83
[188] "Cardano: What Is It, History and How to Buy", www.finance.yahoo.com
[189] "Il trilemma della blockchain è una condizione che riguarda i tre principi fondamentali della tecnologia ossia sicurezza, scalabilità e decentralizzazione. Inizialmente espresso da Vitalik Buterin, il trilemma afferma che tutte le blockchain possono risolvere solo due dei problemi appena citati", www.investire.biz
[190] "Cardano (criptovaluta)", da Wikipedia, l'enciclopedia libera

fine, ossia un ciclo che si ripete all'infinito[191]. Ouroborus, innanzitutto, divide il tempo in epoche, composte a loro volta da slot, con una durata di 20 secondi e funzionano in modo ciclico. Gli slot, invece, posso essere immaginati come dei turni di lavoro all'interno di una fabbrica: l'intervallo di tempo tra un turno di lavoro e un altro, e quindi tra uno slot e un altro, può essere modificato all'interno dell'algoritmo. Ogni epoca ha un leader di slot, il quale viene eletto in modo casuale per rendere il sistema il più imparziale possibile. Questi leader svolgono un ruolo simile ai miners nel protocollo proof-of-work, e quindi sono i responsabili della creazione con validazione dei blocchi da aggiungere successivamente alla blockchain di Cardano, e svolgono quindi un ruolo fondamentale per l'ecosistema. Se un leader non dovesse riuscire a creare un blocco di transazioni perderebbe la sua opportunità e un altro prenderà il suo posto: l'obiettivo in ogni caso è riuscire a produrre almeno il 50% dei blocchi in una data epoca. Ouroborus nel suo insieme consente quindi il decentramento della rete Cardano e le consente di scalare in modo sostenibile con un fabbisogno energetico minimo, senza andare a compromettere la sicurezza.[192]

Le transazioni comportano dati, pertanto all'aumentare del numero di transazioni aumenta anche il fabbisogno di risorse di rete; quindi, se un sistema deve scalare fino a milioni di utenti, la rete avrà bisogno di centinaia o migliaia di terabyte e quindi di risorse per sostenerli. Per risolvere questo problema, Cardano sta esaminando un nuovo tipo di tecnologia chiamato "RINA"[193]: si tratta essenzialmente di un nuovo tipo di reti strutturanti che utilizzano politiche e principi ingegneristici, con l'obiettivo di creare una rete eterogenea che permette di dare privacy, trasparenza e scalabilità.

Per interoperabilità si intende la capacità di un sistema, ad esempio di una blockchain, di cooperare e scambiare informazioni con altri sistemi. La visione di Cardano è quella di creare un Internet di blockchain implementando le cosiddette "*sidechain*"[194], che consistono in catene parallele che corrono lungo la catena principale alla quale saranno collegate, con l'obiettivo di ottenere una versione complessa di una blockchain e l'interoperabilità tra le catene.

Secondo Hoskinson, il problema della sostenibilità è il più difficile da risolvere. Fondamentalmente, come può Cardano accedere a dei fondi per investire nel suo sviluppo e nella sua crescita economica? Di solito, le blockchain tradizionali, quando necessitano di sovvenzioni per finanziare il loro sviluppo, possono trovarle attraverso due metodologie: le ICO e gli interventi esterni.

Tuttavia entrambe le metodologie presentano alcuni punti deboli: con le ICO si riceverebbero somme ingenti senza alcun modello sostenibile e si aggiungerebbero token non necessari alla rete e ancora incompleti; mentre attraverso degli investimenti esterni si potrebbe avere un problema di

[191] "Uroboro", da Wikipedia, l'enciclopedia libera
[192] Fonte: www.cardano.org
[193] Recursive Inter Network Architecture
[194] "Cos'è un sidechain?", www.academy.bit2me.com

centralizzazione, poiché, qualora una grande azienda dovesse decidere di concedere un'ingente quantità di sovvenzioni ad una società, potrebbe dirigere il modo in cui gli sviluppi si evolvono nel sistema, avendo così una parte predominante all'interno del medesimo. La soluzione adottata da Cardano è stata quella di creare una tesoreria: ogni volta che un blocco viene aggiunto alla catena, una parte di quella ricompensa verrà aggiunta alla tesoreria. Perciò, se un individuo o organizzazione vorrà svilupparsi e portare alcuni cambiamenti nell'ecosistema presenterà un voto alla tesoreria per chiedere delle sovvenzioni.[195]

La road map di Cardano si articola su cinque diverse fasi. La prima fase, denominata "Byron", ha l'obiettivo di consentire agli utenti di scambiare e trasferire ADA e, durante tale fase, fu lanciata la "My Net Cardano". La seconda fase, "Shelley", ha l'obiettivo di assicurare che la tecnologia in atto sia un sistema completamente decentralizzato e autonomo. La terza fase, "Goguen", vedrà invece l'integrazione dei contratti intelligenti, mentre la quarta fase, "Basho", sarà basata sul miglioramento delle prestazioni. La quinta fase, infine, denominata "Voltaire", prevede che Yosh aggiungerà un sistema di tesoreria ed una governance.[196]

3.2.3 Polkadot

Polkadot è un progetto blockchain sviluppato da Parity Technologies, società guidata da Gavin Wood e Jutta Steiner, entrambi ex dirigenti di Ethereum. Il progetto è supportato dalla web3 Foundation, un'organizzazione strettamente correlata che fornisce al progetto finanziamenti, sicurezza, ricerca e collaborazione, anch'essa fondata da Gavin Wood.[197]

Sebbene il White Paper originale di Polkadot abbia visto la luce nell'ottobre del 2016, soltanto un anno dopo furono raccolti i fondi attraverso una ICO, la quale fu in grado di raccogliere oltre 140 milioni di dollari vendendo il 50% dei token "DOT", ossia la valuta nativa di Polkadot. Tuttavia, poco dopo l'offerta iniziale di moneta, accadde un tragico evento: il 60% dei 140 milioni raccolti, i quali erano detenuti nel wallet di Parity Technologies, andarono persi per sempre a causa di un errore tecnico commesso da un membro del team. Nonostante questo sfortunato evento, Polkadot resistette e condusse altre due vendite private, una nel 2019 e la seconda nell'estate del 2020, grazie alle quali raccolse oltre 50 milioni di dollari.[198] Finalmente, dopo 4 anni dalla pubblicazione del White Paper, nell'estate del 2020 Polkadot fa il suo primo esordio nel mercato delle criptovalute, posizionandosi direttamente nella top 10 delle più capitalizzate.

---

[195] "Cardano: Tutto quello che devi sapere su ADA", www.comprarebitcoin.com
[196] Fonte: www.cardano.org
[197] "Polkadot (cryptocurrency)", da Wikipedia, l'enciclopedia libera
[198] "The Story Of Polkadot Starts With The 2017 ICO: 2,000% ROI For Early Investors", www.cryptopotato.com

Polkadot è una blockchain di ultima generazione che punta a risolvere un grosso problema nell'attuale panorama blockchain: il fatto che centinaia di blockchain siano completamente isolate tra di loro e abbiano poche capacità di comunicazione. Difatti, Polkadot è un protocollo che unisce un'intera rete di blockchain appositamente costruite, consentendo loro di poter operare senza soluzione di continuità insieme e su larga scala, mantenendo quindi le migliori caratteristiche di molteplici blockchain specializzate.[199] Poiché Polkadot consente a qualsiasi tipologia di dati di essere inviato a qualsiasi tipologia di blockchain, sblocca una vasta gamma di casi d'uso nel mondo reale. Una sola blockchain non è sufficiente per sopportare un reale futuro delle applicazioni decentralizzate perché sono ancora troppo limitanti, mentre aggregando più catene specializzate in un'unica rete consente di effettuare transazioni eseguite in parallelo. Questo sistema va a rimuovere i colli di bottiglia che causano rallentamenti della rete e aumenti dei costi, rendendo le transazioni più veloci ed economiche. Polkadot possiede già le tecnologie necessarie per implementare questo sistema, a differenza di Ethereum 2.0, il quale si era posto il medesimo obiettivo.[200]

Il design di Polkadot offre diversi vantaggi rispetto alle reti esterne o *legacy*, tra cui lo *sharding*, la scalabilità, l'aggiornabilità, una governance trasparente ed una componibilità cross-chain.[201]

Polkadot è una blockchain che potremmo anche definire "condivisa", cioè che collega diverse catene insieme in una singola rete, ovvero la blockchain principale chiamata anche *Relay Chain*[202], consentendo a queste blockchain secondarie, appunto le *parachain*, di elaborare transazioni in parallelo, consentendo lo scambio di dati in sicurezza. Lo *sharding* consiste proprio nell'avere una serie di blockchain separate, diverse e specializzate che dialogano tutte con la catena principale. Grazie all'eterogeneità unica di Polkadot e al modello di *sharding,* ogni catena della rete può essere ottimizzata per uno specifico compito piuttosto che essere costretta ad adattarsi ad un unico modello. Quindi più catene e più specializzazione si riflettono in una maggiore possibilità di innovazione.[203]

Per quanto concerne l'aggiornabilità, è bene sottolineare che ai tempi odierni, ci siamo abituati al fatto che le applicazioni all'interno dei nostri smartphone si aggiornano continuamente per restare al passo con i tempi, e man mano gli sviluppatori correggono i bug prima che possano causare dei problemi. Come tutti i software, anche le blockchain presentano il bisogno di essere aggiornate, al fine di rimanere rilevanti in questo mondo in continua evoluzione ma, a differenza di un'app, aggiornare una blockchain è decisamente più difficile. Di solito, le blockchain convenzionali richiedono un *fork,* ossia una biforcazione della rete che spesso richiede mesi di lavoro, e a volte tali *hard fork* sono particolarmente controversi a tal punto da far dividere un'intera community di utenti.

[199] Fonte. www.polkadot.network
[200] Ibidem
[201] Ibidem
[202] Ibidem
[203] Fonte. www.polkadot.network

Polkadot va a rivoluzionare questo processo, consentendo alla blockchain di aggiornarsi senza la necessità di un *hard fork* e facendo in modo che gli aggiornamenti della rete vengano emanati attraverso un sistema di governance trasparente e *on-chain*: sarà la comunità stessa a decidere e il concilio ad eseguire.[204] Con questa funzione, Polkadot consente ai prodotti di rimanere agili, adattandosi ed evolvendo di pari passo con la tecnologia. Polkadot è governata da tutti coloro che possiedono una certa quantità di DOT, i quali sono in grado di proporre una modifica al protocollo, di votare sulle proposte esistenti e di eleggere i membri del consiglio, i quali poi rappresenteranno le parti interessate all'interno della governance di Polkadot. Quindi possedere dei token DOT equivale quasi a possedere una Nazione che ti permette di avere un potere decisionale.[205] Per quanto riguarda la componibilità *cross chain,* è bene ricordare che le prime blockchain era come dei giardini murati, chiusi alle altre reti; tuttavia, poiché il numero di catene per casi d'uso specifici continua ad aumentare, aumenta anche la necessità di comunicazione e interoperabilità inter-catena. La componibilità *cross chain* e il passaggio dei messaggi di Polkadot consentono alle *parachain* di comunicare, scambiare valore e condividere funzionalità, aprendo le porte ad una nuova ondata di innovazione. Quindi, grazie alla capacità di Polkadot di fare da ponte tra le altre blockchain, le *parachain* di Polkadot saranno anche in grado di interagire con protocolli popolari di finanza decentralizzata e crypto asset come Ethereum.[206]

Conclusioni e prospettive future

Alla luce di quanto esposto all'interno dell'elaborato, risulta dubbio se e quando le criptovalute, in primis Bitcoin, assumeranno in futuro un ruolo sempre più dominante all'interno della nostra società, e se entreranno presto in un'aspra competizione con le banche centrali. L'attuale guerra russo-ucraina ha, per certi versi, accelerato l'adozione delle criptovalute come mezzo di pagamento per diversi motivi: primo fra tutti, la drammatica svalutazione del rublo e le sempre più stringenti sanzioni imposte dall'Occidente hanno spinto la Russia a considerare l'ipotesi di adottare la criptovalute per poter, in parte, sanare l'economia e procedere con gli scambi commerciali; in secondo luogo, l'Ucraina ha accelerato l'approvazione dei disegni di legge per legalizzare appieno Bitcoin e le altre criptovalute, in modo da ricevere aiuti di natura monetaria dal resto del mondo in maniera più rapida ed efficace. Tale accelerazione nell'adozione delle criptovalute, confermata anche dal CEO di BlackRock Larry Fink, comporterà il fatto che prima o poi il prezzo di Bitcoin tenderà a stabilizzarsi all'aumentare del numero di paesi che adotteranno formalmente la crypto in questione. Nel settembre del 2021, il presidente in carica dello Stato di El Salvador Nayib Bukele ha sancito una svolta epocale

[204] "No More Forks: A Case for the Polkadot Approach to Blockchain Upgrades", www.nasdaq.com
[205] Fonte. www.polkadot.network
[206] Ibidem

nella storia delle criptovalute: egli ha deciso formalmente di introdurre un disegno di legge che sanciva il fatto che El Salvador sarebbe diventata la prima nazione nella storia a rendere Bitcoin una moneta a corso legale. Tale decisione, anche se non supportata a pieno dalla Banca Mondiale, rappresenta solo un piccolo passo verso la stabilizzazione del prezzo di Bitcoin, evento che renderà quest'ultimo unità di conto a tutti gli effetti. Allo stesso tempo, molte aziende potrebbero convincersi ad adottare Bitcoin destinando ad esso parte del loro *balance sheet*, anche se al giorno d'oggi ciò viene fatto solo da poche aziende quali MicroStrategy e Tesla. Un'altra questione fondamentale riguarda il fatto che all'interno del panorama crypto, vi sono moltissimi progetti scadenti e senza alcuna prospettiva futura. Progetti come Dogecoin, Shiba Inu, Apecoin e molte altri hanno l'unico obiettivo di attirare speculatori al fine di registrare aumenti di prezzo sorprendenti all'interno dei mercati finanziari. Anche se suddette valute digitali sono in grado di registrare rendimenti pari all'80-90% giornalieri, non hanno alcuna prospettiva di vita e sono destinate, prima o poi, a scomparire. Tali criptovalute, conosciute con il nome di "*shitcoin*", presentano anche molteplici rischi: nell'ottobre 2021, poco dopo l'uscita della celebre serie TV "Squid Game", una criptovaluta denominata allo stesso modo venne lanciata all'interno di un famoso exchange attirando immediatamente l'attenzione di numerosi investitori, e registrando aumenti di prezzo quasi paradossali. Tuttavia, poco dopo che la coin in questione registrò un aumento del prezzo pari al 120%, gli sviluppatori chiusero il progetto e si intascarono l'intero ammontare investito dagli speculatori, sparendo per sempre. Tutti questi progetti, privi di una visione e di una reale praticità, sono destinati, come già affermato, a scomparire per sempre; e il recente crollo del mercato delle criptovalute ha accelerato tale processo di scrematura.

Un'altra questione interessante riguarda il fatto che Bitcoin, in futuro, potrebbe essere abbandonato a favore di altre criptovalute che presentano vantaggi molto più pratici e riducono al minimo gli svantaggi. Tuttavia, come affermato nel capitolo 3, al giorno d'oggi non esiste nessuna criptovaluta che riesca ad operare meglio di Bitcoin, a parità di obiettivi e di mission. Ethereum, per esempio, è un progetto molto valido che con ogni probabilità continuerà a coesistere con Bitcoin, non avendo uno scopo che lo pone in competizione con quest'ultimo. In secondo luogo, Bitcoin è stato nell'ombra per quasi un decennio prima di venire adottato globalmente, e questo sarebbe il percorso che qualsiasi altra criptovaluta all'interno del mercato dovrà compiere prima di avere anche solo una possibilità di poter battere Bitcoin. Cardano, a differenza di Ethereum, presenta uno scopo che lo pone in diretta competizione con Bitcoin, dato che la sua mission sarebbe quella di "fare meglio rispetto a Bitcoin", e ciò rappresenta il motivo per cui questa criptovaluta suscita pareri contrastanti tra gli investitori. Avendo capito che battere Bitcoin rappresenta un'impresa davvero ardua, tutte le alternative coins all'interno del mercato crypto presentano uno scopo ben definito che delinea il loro spettro di operatività, il quale difficilmente va ad interferire con quello dello stesso Bitcoin, ragion per cui abbiamo motivo di credere che molti validi progetti all'interno della blockchain continueranno a

coesistere assieme a quest'ultimo. Come abbiamo discusso nel capitolo 2, l'offerta limitata di Bitcoin presenta una delle caratteristiche fondamentali che pongono questa criptovaluta in diretta competizione con le monete fiat e, quindi, con le banche centrali. Tale caratteristica, infatti, implica che Bitcoin non potrà essere colpito dall'inflazione e quindi potrebbe rappresentare una soluzione a diversi problemi di natura macroeconomica. Per questo motivo, è ragionevole attendersi che nel lungo periodo vi sarà una sempre più rapida transizione verso l'adozione delle criptovalute, a discapito delle monete fiat oggi conosciute. In molti credono invece che Bitcoin perderà la sua attuale popolarità e verrà piano piano abbandonato fino a scomparire; tuttavia, questa visione, seppur possibile, non presenta alcuna premessa plausibile che possa supportarla. Anche Ethereum potrebbe attirare nel tempo sempre più investimenti da parte di individui e organizzazioni, specialmente dopo il recente lancio del Metaverso, della realtà NFT e dopo il passaggio a Ethereum 2.0, previsto per il 2023. In conclusione, soltanto il tempo ci dirà se Bitcoin, Ethereum e le altre criptovalute rappresentano seriamente una svolta epocale nel mondo della macroeconomia, in quanto, al momento, tutto ciò che possiamo fare sono solo semplici supposizioni.

BIBLIOGRAFIA

1. *OpenEdition journals*. Palermo, L. "Sulla teoria e sulla funzione della moneta nel XIV secolo" (2016). Scaricato da: https://journals.openedition.org/mefrm/3390
2. *Università di Macerata*. "Economia Monetaria e Moneta" (2015). Scaricato da: https://docenti.unimc.it/raffaella.coppier/teaching/2019/20263/files/evoluzione-della-moneta
3. *Corporate Finance Institute*. "Hard Money – Overview, Pros and Cons". Scaricato da: https://corporatefinanceinstitute.com/resources/knowledge/credit/hard-money/
4. *Investopedia.* A. Hayes, "Hard Money Definition" (Giugno 16, 2021). Scaricato da: https://www.investopedia.com/terms/h/hardmoney.asp
5. *Medium*. C. Clerici, "Il concetto di scarsità nella determinazione del valore di Bitcoin" (Agosto 9, 2019). Scaricato da: https://medium.com/@carloclerici/il-concetto-di-scarsita-nella-determinazione-del-valore-di-bitcoin-c716c0ad3fff
6. *Create Global Future.* C. Parrado, "Easy Money Trap". https://createglobalfuture.com/easy-money-trap/

7. *FX Empire.* B. Mason, "Come funzione il mining di criptiovalute? Che cos'è l'Hashrate?" (Marzo 1, 2020). Scaricato da: https://www.fxempire.it/education/article/come-funziona-il-mining-di-criptovalute-e-cosa-e-lhashrate-130810
8. *Scenarieconomici.it.* F. Lugano, "Iperinflazione: casi storici e loro cause, e perché non dovremmo averne paura" (Ottobre 11, 2013). https://scenarieconomici.it/iperinflazione-casi-storici-e-loro-cause-e-perche-non-dovremmo-averne-paura/
9. *Linkedin.* M. Geremicca, "I Rai di Yap e la blockchain del 1830" (Marzo 22, 2018). Scaricato da: https://it.linkedin.com/pulse/i-rai-di-yap-e-la-blockchain-del-1830-marco-geremicca-3
10. *Beads Guru.* L.J. Clary, "Beauty with a Dark Past: The Evolution of African Trade Beads" (2015). Scaricato da: https://beadsguru.blogspot.com/2015/01/beauty-with-dark-past-evolution-of.html
11. *How Money Works.* Sidd, "What is Money? From Aggry Beads to Digital Dollars". Scaricato da: https://whatismoney.info/what-is-money/
12. *Università degli Studi di Roma Tor Vergata.* "I mercati finanziari". Scaricato da: https://economia.uniroma2.it/cdl/triennio/clemif/corso/materiali/190/
13. *Università degli Studi di Cagliari.* M. Carboni, "Risparmio, investimento e sistema finanziario". Scaricato da: https://www.people.unica.it
14. *Orizzonti Politici.* L. Bianchi, "La crisi del 2008: le cause ma soprattutto gli effetti" (Settembre 7, 2020). Scaricato da: https://www.orizzontipolitici.it/la-crisi-del-2008-le-cause-ma-soprattutto-gli-effetti/
15. *Youtube.* Te lo spiego, "Che cos'è e come funziona una Blockchain" (Aprile 23, 2021). Scaricato da: https://www.youtube.com/watch?v=sX25z_-zMgI
16. *Reddit.* K. Graf, "On the Origins of Bitcoin: Stages of Monetary Evolution" (2014). https://www.reddit.com/r/Bitcoin/comments/1p2xfe/on_the_origins_of_bitcoin_stages_of_monetary/
17. *MeteoFinanza.* LorenzoB, "Proof of Work (PoW): Cos'è, Come Funziona, Vantaggi e Svantaggi" (Maggio 6, 2021). Scaricato da: https://www.meteofinanza.com/proof-of-work/
18. *Salvatore Aranzulla,* "Come Funziona il Mining". https://www.aranzulla.it/come-funziona-il-mining-1293103.html
19. *Bit2Me Academy.* "Che cos'è il Block Reward?" (2022). Scaricato da: https://academy.bit2me.com/it/che-%C3%A8-il-premio-in-blocco/#:~:text=Il%20Block%20Reward%20(ricompensa%20del,economico%20che%20sostiene%20una%20blockchain.
20. *CoinDesk.* O. Godbole, "Bitcoin Network Sees Fourth Straight Downward Difficulty Adjustment" (Settembre 14, 2021). https://www.coindesk.com/markets/2021/07/19/bitcoin-network-sees-fourth-straight-downward-difficulty-adjustment/

21. *Rezerve.* "Inflazione, proteggersi grazie a Bitcoin". https://www.rezerve.it/bitcoin-e-inflazione/#:~:text=Bitcoin%20come%20protezione%20dall'inflazione&text=Non%20essendo%20possibile%20un%20intervento,fatto%20dall'aumento%20dei%20prezzi.
22. *Senigallia Notizie.* "Cosa fa aumentare il prezzo di Bitcoin" (Ottobre 18, 2021). Scaricato da: https://www.senigallianotizie.it/1327538196/cosa-fa-aumentare-il-prezzo-di-bitcoin
23. *Wired.* E. Spagnuolo, "Storia breve del Bitcoin" (Gennaio 3, 2019) e "Come la blockchain può aiutare la lotta all'inquinamento" (Gennaio 27, 2020). Scaricati da: https://www.wired.it/economia/finanza/2019/01/03/bitcoin-2009-trasformazione-storia/; https://www.wired.it/attualita/ambiente/2020/01/27/blockchain-lotta-inquinamento/
24. *WisdomTree Europe.* J. Guthrie, "Perché il prezzo del Bitcoin aumenta" (Gennaio 21, 2021). Scaricato da: https://www.wisdomtree.eu/it-it/blog/2021-01-21/making-sense-of-bitcoin-price-increases
25. *Investopedia.* A. Hayes, "What Happens to Bitcoin After All 21 Millions Are Mined?" (Marzo 5, 2022). Scaricato da: https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/#:~:text=Bitcoin%20mining%20fees%20will%20disappear,block%20rewards%20and%20transaction%20fees.
26. *SpringerLink.* D.G. Baur & T. Dimpfl, "The volatility of Bitcoin and its role as a medium of exchange and a store of value" (Gennaio 5, 2021). Scaricato da: https://link.springer.com/article/10.1007/s00181-020-01990-5#:~:text=Bitcoin%20is%20a%20cryptocurrency%20but,days%2C%20weeks%2C%20or%20months.
27. *Investopedia.* J. Kelleher, "Why Do Bitcoins Have Value?" (Marzo 15, 2022). Scaricato da: https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp#:~:text=Bitcoin%20demonstrates%20some%20attributes%20for,of%20the%20global%20currency%20market.
28. *Invao.* "Bitcoin's Intrinsic Value: Means of Payment and Store of Value" (Settembre 30, 2019). Scaricato da: https://invao.org/bitcoins-intrinsic-value-means-of-payment-and-store-of-value/#:~:text=Bitcoin%20is%20a%20service%20commodity,not%20be%20the%20case%20today.
29. *Rivista di Diritto Bancario.* G. Lemme, "Criptomoneta e distacco dalla moneta legale: il caso Bitcoin" (2016). Scaricato da: https://rivista.dirittobancario.it/criptomoneta-e-distacco-dalla-moneta-legale-il-caso-bitcoin
30. *Filippo Angeloni.* F. Angeloni, "Bitcoin – Unità di conto Globale" (2020). Scaricato da: https://www.filippoangeloni.com/bitcoin-unita-di-conto-globale/

31. *Cyber Security 360*. "Attacco a Bitcoin: di cosa si tratta, come funzionano e come proteggersi" (Agosto 19, 2021). Scaricato da: https://www.cybersecurity360.it/nuove-minacce/attacco-ai-bitcoin-di-cosa-si-tratta-come-funzionano-e-come-proteggersi/
32. *Medium*. "Internet e Bitcoin: due tecnologie odiate a confronto" (Aprile 16, 2018). Scaricato: https://medium.com/@novaminingita/internet-e-bitcoin-due-tecnologie-odiate-a-confronto-ea630487351e
33. *Abenergie.* "I Bitcoin e l'inquinamento: anche il mondo digitale crea emissioni" (Agosto 5, 2021). Scaricato da: https://www.abenergie.it/blog/2021/08/bitcoin-inquinamento
34. *Corriere della Sera.* A. Conzonato, "Quanto inquinano i Bitcoin?" (Maggio 17, 2021). https://www.corriere.it/economia/finanza/21_maggio_17/quanto-inquinano-bitcoin-l-impatto-sull-ambiente-l-alternativa-ecosostenibile-2231eba2-b40e-11eb-92ee-af36a1f66d3c.shtml
35. *Bitcoin Stack Exchange.* "Satoshi's Final Statement" (Aprile 2018). Scaricato da: https://bitcoin.stackexchange.com/questions/28108/satoshis-final-statement
36. *The Guardian.* "Bitcoin project blocks out Gavin Andresen over Satoshi Nakamoto claims" (Maggio 6, 2016). https://www.theguardian.com/technology/2016/may/06/bitcoin-project-blocks-out-gavin-andresen-over-satoshi-nakamoto-claims
37. *CoinDesk.* D. Siegel, "The DAO Attack: Understanding What Happened" (Giugno 25, 2016). Scaricato da: https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/
38. *Criptonauti.it.* "La scalabilità blockchain e criptovalute, cosa significa?". Scaricato da: https://www.criptonauti.it/scalabilita-blockchain-e-criptovalute-cosa-significa/
39. *Tom's Hardware.* A. Crea, "Ethereum 2.0, che cos'è e perchè è così importante" (Settembre 13, 2021). Scaricato da: https://www.tomshw.it/altro/ethereum-2-0-cose-e-perche-e-cosi-importante/
40. *Criptovaluta.it.* G. Grossi, "Ethereum: problemi di scalabilità – PoS non basta?" (Novembre 23, 2021). Scaricato da: https://www.criptovaluta.it/25963/ethereum-problemi-di-scalabilita-pos-non-basta-ecco-la-soluzione
41. *Medium*. M. Vinicius, "Cardano: What is Peer Review?" (Marzo 25, 2021). Scaricato da: https://medium.com/adazulpoolenus/cardano-what-is-peer-review-know-here-livecoins-5890c3a1e731
42. *Bit2Me Academy*. "Cos'è un sidechain?". https://academy.bit2me.com/it/cos%27%C3%A8-sidechain-sidechain/
43. *Comprarebitcoin.com*. "Cardano: Tutto quello che devi sapere su ADA". Scaricato da: https://www.comprarebitcoin.com/cardano/
44. *CryptoPotato.* J. Lyanchev, "The Story Of Polkadot Starts With The 2017 ICO: 2,000% ROI For Early Investors" (Agosto 20, 2020). Scaricato da: https://cryptopotato.com/the-story-of-

polkadot-starts-with-the-2017-ico-2000-roi-for-early-investors/#:~:text=For%20Early%20Investors-,The%20Story%20Of%20Polkadot%20Starts%20With%20The%202017,2%2C000%25%20ROI%20For%20Early%20Investors&text=Following%20the%20successful%20DOT%20redenomination,of%20the%20biggest%20cryptocurrency%20projects.

45. *Investire.biz.* G. Guazzo, "Bitcoin e trilemma della blockchain: cosa è e possibile soluzione" (Novembre 27, 2020). Scaricato da: https://investire.biz/articoli/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-bitcoin-trilemma-blockchain-cosa-funzionamento-soluzione-lightning-network
46. N. Gregory Mankiw, Mark P. Taylor, "Macroeconomia", Sesta edizione italiana, Zanichelli
47. Saifedean Ammous, "The Bitcoin Standard: The Decentralized Alternative to Central Banking" (2017), Wiley
48. A. Fekete, "Whither Gold?" (1997)
49. J. Salerno, "Money: Sound and Unsound" (2010), Ludwig von Mises Institute
50. R. Jastram, "The Golden Costant: The English and American Experience" (2009), Edward Elgar Publishing Ltd.
51. N. Szabo, "Trusted Third Parties Are Security Holes" (2001)
52. N. Popper, "Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money" (2016), HarperCollins

SITOGRAFIA

1. https://www.ecb.europa.eu/ecb/educational/hicp/html/index.it.html#:~:text=Si%20ha%20inflazione%20quando%20si,valore%20della%20moneta%20nel%20tempo.
2. https://it.wikipedia.org/wiki/Moneta
3. https://it.wikipedia.org/wiki/Riserva_di_valore#:~:text=Una%20riserva%20di%20valore%20%C3%A8,pericolo%20che%20si%20%22deteriori%22.
4. https://it.wikipedia.org/wiki/Iperinflazione
5. https://it.wikipedia.org/wiki/Peng%C5%91_ungherese
6. https://it.wikipedia.org/wiki/Rai_(moneta)
7. https://www.bancaditalia.it/servizi-cittadino/musei-collezioni/mostra-moneta/esplora/Mini_guida_bassa_risoluzione.pdf
8. https://it.wikipedia.org/wiki/Signoraggio
9. https://it.wikipedia.org/wiki/Doppia_spesa
10. https://www.borsaitaliana.it/notizie/sotto-la-lente/bitcoin-172.htm

11. https://it.wikipedia.org/wiki/Funzione_di_hash
12. https://www.ibm.com/it-it/topics/what-is-blockchain#:~:text=Definizione%20della%20blockchain%3A%20La%20blockchain,beni%20in%20una%20rete%20commerciale.
13. https://www.ibm.com/topics/smart-contracts
14. https://www.bloomberg.com/professional/blog/gold-or-bitcoin-store-of-value-debate-rages-as-bitcoin-grows
15. https://it.wikipedia.org/wiki/Criptovaluta
16. https://academy.binance.com/it/articles/what-is-a-51-percent-attack
17. https://it.wikipedia.org/wiki/Ransomware
18. https://it.wikipedia.org/wiki/Bitcoin
19. https://twitter.com/elonmusk/status/1392602041025843203
20. https://www.ibm.com/case-studies/energy-blockchain-labs-inc
21. https://nori.com/token
22. https://www.namecoin.org/
23. https://coinmarketcap.com/
24. https://it.wikipedia.org/wiki/Decentralized_autonomous_organization
25. https://ethereum.org/en/upgrades/
26. https://it.wikipedia.org/wiki/Vitalik_Buterin
27. https://ethereum.org/it/defi/
28. https://academy.binance.com/it/articles/what-are-flash-loans-in-defi
29. https://ethereum.org/en/developers/docs/nodes-and-clients/
30. https://it.wikipedia.org/wiki/Charles_Hoskinson
31. https://it.wikipedia.org/wiki/Cardano_(criptovaluta)
32. https://finance.yahoo.com/news/cardano-history-buy-125608009.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEuOetR0iYaLj-rhpq48BbfaODpsbqeNLG6LBVdcnsw7o-Ot-7xUggUJ9fUOTGmSCh-YGDN7Nu30a8RLImqzBw4iJbkh8Cy2OV7XwRJumUfxYDvxmPJ2ifFfQ1LHHQ5c0mvMEoC4iA92eWE6q0A9NwHOza0BWsRzn79rH_ZLJWwQ
33. https://it.wikipedia.org/wiki/Uroboro
34. https://cardano.org/
35. https://en.wikipedia.org/wiki/Polkadot_(cryptocurrency)
36. https://polkadot.network/
37. https://www.nasdaq.com/articles/no-more-forks%3A-a-case-for-the-polkadot-approach-to-blockchain-upgrades-2021-09-09