UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia e Commercio

CRIPTOVALUTE, IL NUOVO LATO DELL'ECONOMIA

Relatore:
Prof. Camilla Mazzoli

Rapporto Finale di:
Giovanni Cardarelli

Anno Accademico 2021/2022

INDICE

INTRODUZIONE

In un'epoca in cui l'innovazione è questione di tutti i giorni, non si può non soffermarsi come quanto quest'ultima possa inserirsi all'interno del concetto di economia e quanto essa possa venir modificata dal passare degli anni e dalle tecnologie moderne. Al giorno d'oggi le innovazioni sono molte, ma in questo elaborato ci si vuol soffermare sulle criptovalute; amate da molti e odiate da altri, inutile nascondere che siano la "novità" del momento; concetto poco conosciuto e trattato da una piccola fetta degli intermediari che compongono il mercato, molti dei quali son coloro che hanno effettivamente fatto una fortuna derivante dal loro utilizzo, fortuna vista man mano rallentarsi per un motivo puramente matematico: più individui entrano in questo mondo, minori sono le probabilità di estrarne un grosso profitto. L'obiettivo di questo elaborato è quello di andare a definire cosa è una criptovaluta, su quali tecnologie si vada effettivamente a basare ed andare a capire se possano diventare effettivamente una valida alternativa alla moneta tradizionale alla quale noi siamo abituati al giorno d'oggi. L'elaborato è composto di due capitoli; nel primo vengono descritte le criptovalute con una loro definizione, la loro storia ed origine, con annessa spiegazione delle tecnologie utilizzate da quest'ultime, andando a sottolineare le modalità con le quali esse operano, nonché vantaggi e svantaggi derivanti dal loro utilizzo.

Nel secondo, invece, si farà un focus su due tipologie di criptovalute, con una loro successiva spiegazione e contestualizzazione nel mercato.

CAPITOLO 1 - LE CRIPTOVALUTE

1.1 Cosa si intende con criptovaluta

Come chiaramente ci si può aspettare, sia gli strumenti che i mercati finanziari negli anni si son evoluti e hanno rivolto l'attenzione a capire come andare a rispondere alle nuove esigenze, le quali fanno riferimento alle transazioni commerciali, per facilitarne il loro processo e, soprattutto, la loro sicurezza. Figlia dei progressi della crittografia, la criptovaluta è, come recita il nome, una valuta vera e propria la quale però risulta "celata", in quanto viene creata attraverso un sistema di codici per i quali vi è la necessità della conoscenza di un certo codice informatico (le cosiddette "chiavi di accesso", in linguaggio più tecnico). Come riportato dalla Borsa Italiana "*è una rappresentazione digitale di valore ed è utilizzata come mezzo di scambio o detenuta a scopo di investimento*", le quali non sono sottoposte all'emissione, alla garanzia o al controllo da parte di banche centrali o autorità pubbliche.

Non è un elemento tangibile, quindi non troveremo mai qualcosa facente riferimento al concetto di criptovaluta con possibilità di scambio e/o vendita

(quindi siamo di fronte ad una grande differenza con le monete *FIAT* tradizionali standard, ossia le classiche monete a corso legale come euro, sterlina. Dollaro e tutte le altre principali valute) ma ciò non impedisce di essere trattata come ogni altro bene anche con questo "deficit". Solitamente vengono emesse da emittenti privati, quindi non regolate da enti centrali governativi, e sono caratterizzate dall' utilizzo di software altamente specializzati e di tecnologie blockchain, il quale ultimo concetto verrà ripreso poi in seguito.

1.2 Storia ed origine delle criptovalute

La storia delle criptovalute è relativamente recente, con la nascita del Bitcoin nel 2009. Ma in realtà hanno un'origine molto meno giovane.

Precisamente siamo nel 1983, un crittografo americano di nome David Chaum ebbe l'idea di una moneta completamente elettronica, funzionante grazie alla crittografia con il primo nome di "*Ecash*", idea poi successivamente ripresa da altri sviluppatori negli anni 90 come Wei Dai con il progetto simile chiamato "*B-Money*" o Nick Szabo con "*Bit Gold*".

Senza dubbio però l'anno cruciale per le criptovalute è il 2009, anno in cui l'anonimo sviluppatore identificato con lo pseudonimo di Satoshi Nakamoto crea il Bitcoin, la prima vera e propria criptovaluta, innovativo per il concetto della "blockchain".

Dopo di questa nacque una seconda criptovaluta, chiamata “Litecoin”, creata nel 2011 tramite una ramificazione della blockchain di bitcoin. Poi, col passare degli anni le criptovalute sono aumentate a dismisura, migliorando sempre la blockchain. Attualmente nel mercato se ne possono contare più di 17000.

1.3 Caratteristiche, vantaggi e svantaggi

Come ogni altra cosa la mondo, non è tutto rose e fiori, soprattutto quando si parla di criptovalute. C’è innanzitutto da sottolineare un concetto molto importante, ossia che la sua caratteristica principale, l’essere crittografata, ha una duplice valenza: la *protezione delle transazioni* e il *controllo della creazione di nuove monete*.

La moneta tradizionale, come la conosciamo oggi, ha tre funzioni comuni, che sono: la funzione *di unità di conto*, di *mezzo di pagamento* e di *deposito di valore.*

La domanda che ci si pone, quindi, è se può la criptovaluta assolvere a queste tre funzioni

Sulla prima dobbiamo rispondere di no. Risulta praticamente impossibile andare a dare un prezzo a beni e servizi in termini di criptovalute, dato che quest’ultime sono caratterizzate da un’alta volatilità. Ciò significa che il prezzo può variare bruscamente, anche nella stessa giornata, rendendo impossibile basarsi sul valore delle criptovalute. Sulla funzione del mezzo di pagamento dobbiamo sottolineare che le monete virtuali non sono dotate di corso legale nel mondo (o in quasi tutto),

quindi l'accettazione o meno di queste dipende dalla volontà della controparte. Per la terza, invece, bisogna essere al corrente che, nel caso in cui fossero utilizzate come mezzo di pagamento, queste aumenteranno sempre di più di valore, perché il numero di unità di criptovalute producibili è limitato e la loro creazione si riduce nel tempo. Quindi, più transazioni, maggiore sarà il loro valore, le quali però, nel caso in cui avvenissero, devono andare a rispettare un insieme di norme, detto *protocollo*, che vanno a spiegare come i partecipanti potranno effettuare queste transazioni. Di queste avremo una storia, immodificabile, contenuta nella blockchain.

I vantaggi che si possono trovare derivanti dal loro utilizzo sono:

Decentralizzazione: ciò significa che la loro ricchezza risulta distribuita tra molte parti, tra i blocchi della blockchain. Inerente a questo bisogna fare una precisazione, ossia che si può parlare tanto di decentralizzazione quanto concentrazione, perché in realtà la proprietà è altamente concentrata. Pochi investitori vanno a coprire una grossa fetta di percentuale del valore di una criptovaluta.

Anonimato: ossia che ogni utente si registra nel sistema con uno pseudonimo, che garantisce, appunto, l'anonimato. Anche se tutto ciò

significa lasciare una traccia del proprio passaggio che agenzie come la Federal Bureau of Inestigation (FBI) possono andare a decifrare.

Sicurezza: data dalla più volte citata blockchain e dal fatto che le criptovalute sono custodite in dei portafogli virtuali, dove per l'accesso è richiesta una password; quindi solo colui che ne ha diritto può accedervi, anche se non bisogna erroneamente pensare questi *e-wallet* siano perfettamente sicuri.

Velocità: le criptovalute sono caratterizzate da una disponibilità sempre presente e di tempi molto più brevi, a differenza delle monete fiat che possono richiedere dei giorni per effettuare una sola transazione, vedi bonifici ordinari bancari.

Ma presentano anche degli svantaggi:

Sono **volatili**: come già spiegato, non sono caratterizzate da un corso legale; ciò comporta ad possibile utilizzo in operazioni potenzialmente illecite (dato che non vi è garanzia sull'evitare controlli speculativi) o, addirittura, situazioni di riciclaggio di denaro.

Sono **vulnerabili**: eventuali attacchi informativi non sono da sottovalutare che, unito al concetto dell'anonimato, porta all'impossibilità di andare a recuperare la nostra moneta virtuale, dato che vi à la crittografia. Forse è anche per questo che vi è non poco scetticismo in questo ambito.

Sono **costose**: l'estrazione di queste criptovalute richiede molta energia. I costi energetici elevati uniti all'imprevedibilità dell'attività mineraria hanno concentrato tale attività tra poche grandi aziende, i cui ricavi sono considerati enormi.

1.4 Blockchain

Più volte nominata e tirata in ballo, la blockchain è un registro di contabilità condiviso e immutabile che facilita il processo di registrazione delle transazioni e la tracciabilità dei beni in una rete commerciale. Parlando di ciò, bisogna tener conto di una precisazione, ossia che un *asset* può essere tangibile (come un'auto o

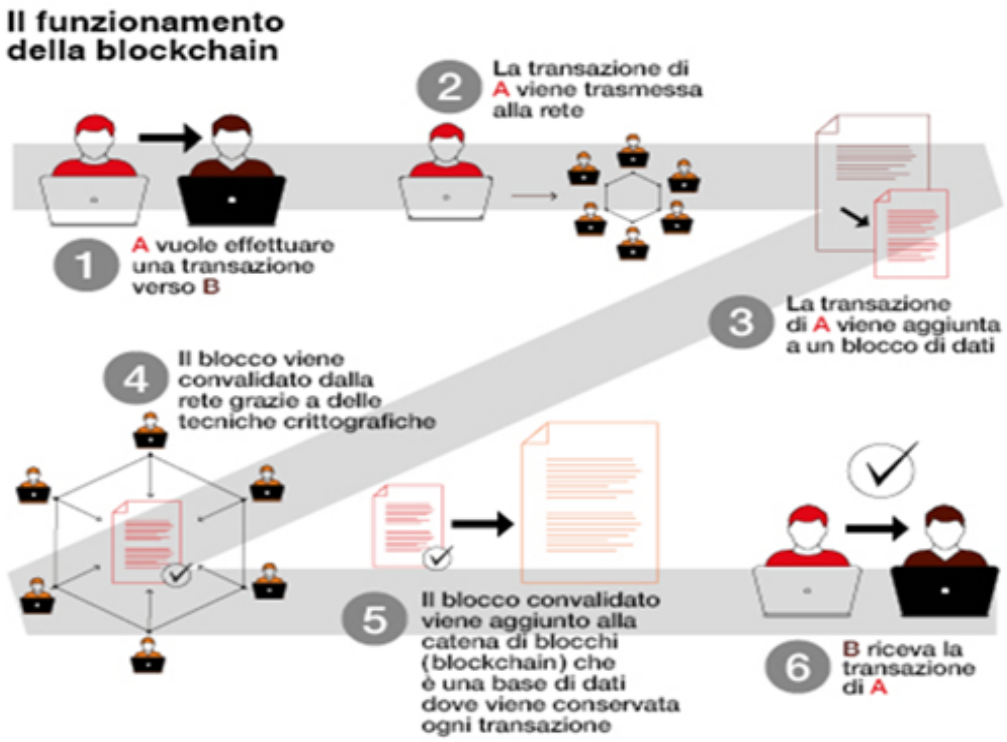
una casa) o intangibile (come un brevetto o un copyright). Tutto ciò che possa aver valore può essere rintracciato e scambiato su una rete "blockchain", riducendo rischi e costi.

La sua creazione è volta al concetto che il business è fondamentalmente basato su informazioni, le quali devono essere le più accurate e rapide possibili. Ragionandoci sopra viene subito al pensiero che un meccanismo del genere risulta ideale per la trasmissione delle informazioni ma non solo; può inoltre tracciare ordini, account, pagamenti nonché andare a verificare una determinata transazione "end-to-end", ossia l'insieme di tutte quelle operazioni da dover effettuare da un individuo all'altro, le quali sono contenute all'interno di questa catena, con la sicurezza di ripercorrere quanto effettuato ed, eventualmente, andare a trovare errori e/o falle: il che si tramuta, ovviamente, in maggiore fiducia. La transazione che si andrà a creare, compresa degli indirizzi, delle chiavi e di tutto il necessario, come il prezzo o l'oggetto, sarà inclusa in un "blocco". Quest'ultima, però, deve essere confermata: il blocco successivo a quello di riferimento alla transazione è detto, appunto, di "conferma".

Proprio dal nome dell'argomento cui si sta trattando, quanto detto prende forma; significa letteralmente "catena di blocchi", rete informatica di nodi con la gestione in modo univoco e sicuro di un registro pubblico composto da dati ed informazioni. Nel momento in cui ne avviene una nuova, questa viene registrata come un "blocco di dati", il quale si collega agli altri blocchi precedenti presenti

in questa lunga catena. Una volta avvenuto il collegamento, le transazioni sono bloccate tra loro irreversibilmente; ecco creatasi la blockchain.

Figura 1 – Il funzionamento della blockchain



Fonte: kmu.admin.ch

1.5 Meccanismo della ricompensa in blocchi

Quindi l'insieme di questi blocchi fanno parte della lunga catena, dove, all'interno vi sono varie tipologie di operazioni. Con la creazione di un nuovo blocco che viene inviato a tutti gli utenti, per esempio, con una transazione, vi è la necessità che quest'ultima venga approvata. Il compito della generazione del blocco della

conferma spetta agli utenti, la quale creazione non è operazione da poco per quest'ultimi, dato che ciò si tramuta in un grande sforzo sotto il punto di vista di energia e di tempo.

Gli utenti sono spinti ad effettuare quanto detto prima (prendendo in ipotesi un caso di transazione riuscita) perché questa conferma è correlata a delle *rewards,* ossia un incentivo che i *miners* (termine che deriva dal termine "*mining*", cioè "andare a minare, estrarre un blocco") hanno per andare ad approvare una transazione o per andare a prestare i loro dispositivi per andare a compiere calcoli o a risolvere complessi problemi matematici; basti pensare che è possibile (ma risulta non conveniente perché i costi sono maggiori dei possibili guadagni) andare a effettuare tali operazioni anche con un comune smartphone. Questa precisazione è volta a sottolineare che con il termine "dispositivo" o, magari come alcuni esperti citano, "strumento di calcolo", non stiamo parlando di chissà quale diavoleria informatica e tecnologica. Risulta molto più vicina a noi di quanto possiamo immaginare. Tutto ciò fa creare una sorta di competizione tra gli individui partecipanti, chi sarà più veloce a prestare la loro potenza di calcolo per risolvere i vari calcoli matematici, vincerà la competizione.

La ricompensa è rappresentata da una criptovaluta ottenuta dall'estrazione del blocco, la quale è divisa in due parti:

Block Subsidy: l'effettiva sostanza della ricompensa, ossia quante "monete" sono state generate con il nostro operato.

Commissioni di transazione: sono le commissioni pagate che sono incluse nel blocco di riferimento decise dall'utente che ha richiesto la verifica della transazione stessa.

Tale concetto di ricompensa può essere analizzato anche sotto un punto di vista economico, perché risulta l'unico modo per far circolare le nuove criptovalute nel mercato. Ogni qualvolta che un miner va a convalidare un blocco, avrà una ricompensa in questa nuova moneta. Il calcolo, però, non risulta così immediato: le ricompense non sono e non devono essere erroneamente considerate fisse, ma dipendono dai vari e diversi progetti a quali si fa riferimento. Inoltre, va sottolineato che dobbiamo andare a tener conto di quanto le criptovalute circolano, cioè si fa riferimento al concetto che più sono in circolazione, più mantengono il loro valore; bisogna anche andare a verificare quali siano i tempi di trasmissione, perché se questi ultimi aumentano, il valore del asset in cripto diminuisce. Da non dimenticare inoltre delle commissioni di transazione: più la rete risulta affollata, maggiori saranno i costi di queste.

Il concetto della ricompensa in blocchi va anche a favorire la decentralizzazione, una delle caratteristiche principali della blockchain, in quanto la generazione di nuovi blocchi con un loro successivo controllo da parte degli individui stessi

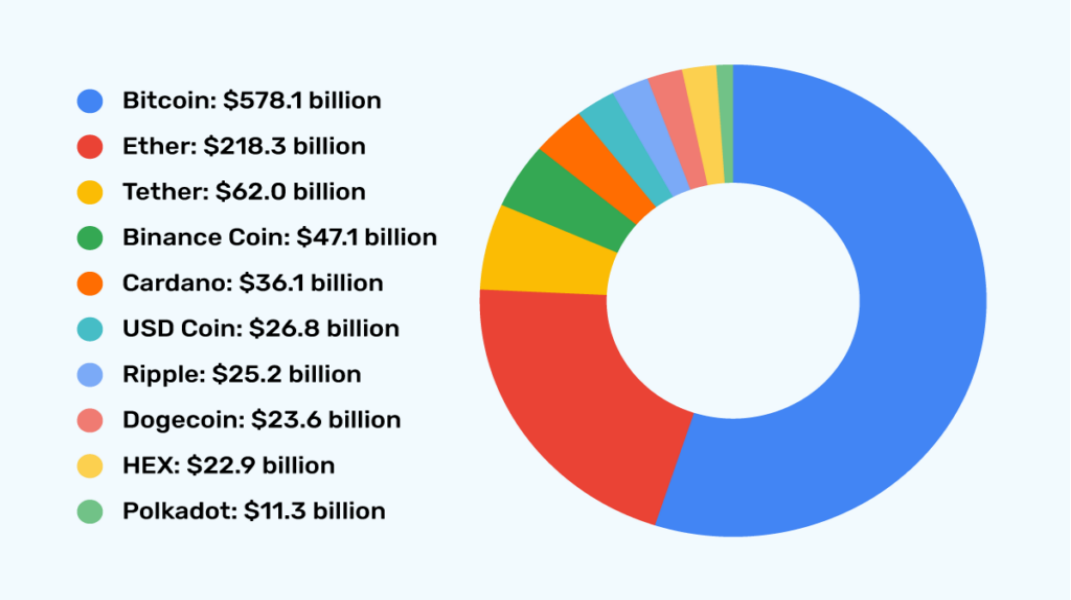
presenti all'interno del sistema senza passare sotto il controllo di un ente centrale rispondono proprio alla caratteristica della non centralità.

CAPITOLO II – NON SOLO BITCOIN

2.1 La prima e più importante moneta digitale

C'è poco da dire. Quando si parla di criptovalute la prima che verrà alle nostre menti sarà sempre lei, il *Bitcoin*, regina indiscussa per popolarità, ma anche per storia ed importanza., nonché di capitalizzazione di mercato; con quest'ultimo termine si intende il valore totale di tutte le monete che sono sottoposte al processo di *mining* ed il calcolo risulta molto semplice: si va a moltiplicare il numero di monete in circolazione per il prezzo di mercato di queste. Si può intendere questo valore come il grado di probabilità che una risorsa rimanga stabile, ma ciò non deve essere inteso come una "regola". Quando siamo di fronte alle criptovalute, non è possibile ragionare in termini di stabilità certa nel futuro, ricordando infatti che queste monete digitali non sono sostenute da alcuna banca o eventuali governi, quindi ne consegue che possono essere soggette a *volatilità*, ossia l'oscillazione del proprio prezzo in un determinato periodo. Anche il bitcoin, che fa registrare la maggiore capitalizzazione di mercato di tutto il settore del criptovalute, è esposto a questo fenomeno.

Figura 2 - Grafico di capitalizzazione del mercato delle principali criptovalute sul mercato



Fonte: kriptomat.io

La sua grande dominanza è sicuramente dovuta al fatto che è stata l'effettiva prima criptovaluta al mondo, risalente all'anno 2009, cioè quando fu introdotto per la prima volta questo *software open-source* da un programmatore anonimo, o più di uno, sotto lo pseudonimo di Satoshi Nakamoto (si dice sia un uomo di trentasette anni giapponese). La sua grossa percentuale nel grafico a torta sovrastante è data anche dalla crescente fiducia che ha suscitato nel tempo. Infatti bitcoin è una moneta digitale, ma il Bitcoin (con l'iniziale del nome maiuscola) è

una rete ed una tecnologia. Ossia, è anche un sistema di pagamento. La sua rete è una rete di tipo *peer-to-peer* (abbreviata in "*P2P"*) caratterizzata che ogni suo nodo può decidere se operare come client o come server, a seconda delle convenienze e delle circostanze. Anche qui si va ad utilizzare la tecnologia della blockchain, senza alcun dubbio un, se non "il", punto di forza che ha contribuito a rendere il bitcoin ciò per cui lo conosciamo oggi.

2.2 Le alternative al bitcoin: le Altcoin

Con l'avvento della prima moneta digitale, risultava abbastanza scontato aspettarsi una risposta sottoforma di proposte di nuove criptovalute alternative: ciò fa riferimento al concetto delle "Altcoin"

Come si può intuire dal nome, il termine altcoin è l'abbreviazione di "moneta alternativa", quindi si fa riferimento a qualsiasi criptovaluta diversa dalla più affermata del mercato. Nate ovviamente dopo il bitcoin, sono state create per cercare di andare ad ovviare dei problemi riscontrati con quest'ultimo (quindi, per un certo verso, quasi da diventare una "rivale" di questa). Queste *coin* sono caratterizzate da una grande attenzione su aspetti come privacy e sicurezza, i punti dove bitcoin veniva considerato più debole, oppure sulla semplificazione dei "requisiti" per partecipare alle varie operazioni, dato che erano necessarie apparecchiature informatiche molto potenti, cosa non possibile da tutti; attenzione

rivolta anche ad ovviare il problema della lentezza dei tempi e nei costi di transazione, dato che le altcoin presentano un loro registro nativo, esattamente come il bitcoin, ma con delle commissioni decisamente più basse. In linea di massima, quindi, il ragionamento dietro alla creazione di quest'ultime sta nel prendere come punto di partenza il bitcoin, per poi aggiungervi dei miglioramenti o delle particolari caratteristiche che possono far suscitare interesse da parte degli investitori, così da andare ad acquisire maggior quota di mercato.

Tutte le altcoin sono diverse, per le caratteristiche del loro progetto o nei loro meccanismi e regole di ricompensa; facciamo un piccolo focus su 2 delle principali monete alternative sul mercato.

2.2.1 Ethereum

Figura 3 – Logo

La prima coin presa in analisi è colei che è sempre stata considerata come storica rivale del bitcoin, seconda moneta digitale per diffusione e capitalizzazione al mondo, la quale risulta una delle più conosciute piattaforme *software open source* decentralizzate basate sulla blockchain. Le prime informazioni inerenti alla piattaforma risalgono al 2013 quando vi sono stati sviluppi da parte del programmatore Vitalik Buterin, ragazzo russo di 19 anni che viveva in Canada. Il suo lancio effettivo, però, è stato nel 2015.

Ethereum è il nome della rete. "Ether", invece, della criptovaluta (sottoforma di token, denominati *"ETH"*) utilizzata nella rete.

Come detto, anche qui funziona attraverso una blockchain, dove ogni blocco prima della sua registrazione deve essere validato dagli utenti in piattaforma (il già più volte citato in precedenza "blocco di conferma"). La rete di Ethereum è caratterizzata da un computer virtuale decentralizzato, il cosidetto *EVM* (*Ethereum Virtual Machine*) dove per funzionare ha la necessità di computer (reali) costantemente accesi, che vanno ad offrire una parte della loro potenza di calcolo alla rete. Però, quest'ultimi, necessitano di energia per andare a svolgere la loro funzione: ciò è rappresentata da Ether, che viene vista come una specie di incentivo per gli sviluppatori a realizzare applicazioni di qualità sempre maggiore. Il tutto risulta fondamentale per gli *smart contract*, i quali senza questa criptovaluta, usata per comprare la potenza di calcolo, non esisterebbero.

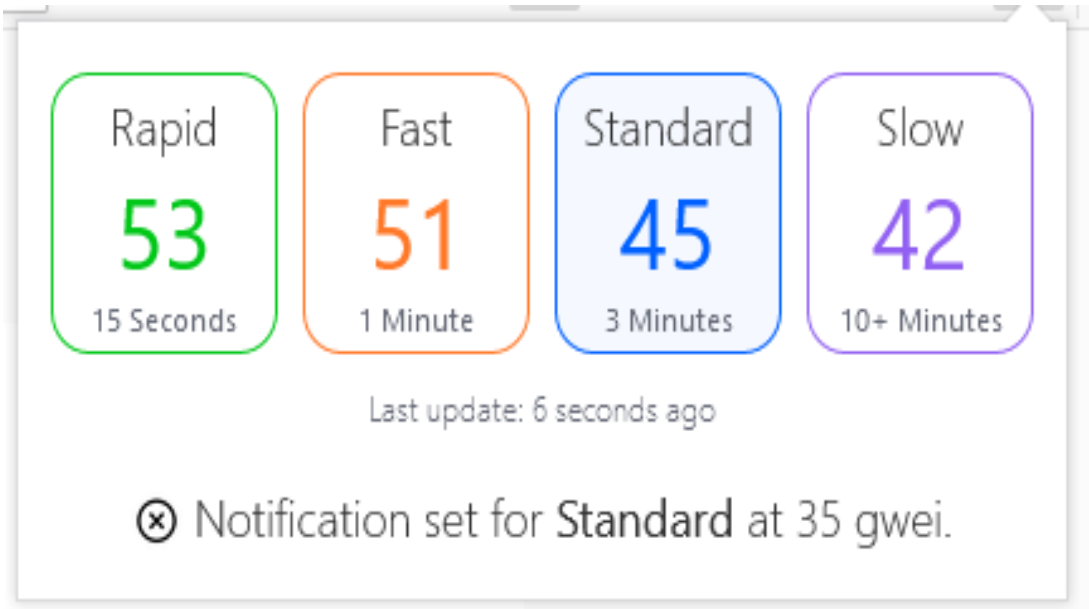
Questi “contratti intelligenti” sono come dei veri e propri contratti cartacei che vanno a regolare termini e condizioni tra le parti di un accordo, ma la differenza principale sta nella loro automaticità e sicurezza. Difatti una volta che le condizioni pattuite sono state soddisfatte, il contratto verrà eseguito automaticamente, senza bisogno dell’intervento di alcun intermediario o derivante dalle parti. La seconda, invece, fa riferimento al fatto che i dati contenuti all’interno sono crittografati, quindi questi consentono agli sviluppatori di andare a creare applicazioni complesse, con determinati codici di programmazione, senza interruzioni, frodi ed intervento di terzi. Se più volte il Bitcoin è stato denominato “L’oro digitale”, l’Eth può essere considerato come il “petrolio digitale”. Questa insolita similitudine deriva dal fatto che gli utenti, per l’esecuzione degli smart contract, vanno a pagare delle commissioni in ETH, che sono definite “gas”, termine utilizzato ragionando sul fatto che i token sono considerati come il “carburante” che consente all’intero sistema di funzionare. Il gas totale per ogni transazione è dato dal prodotto di due componenti:

Gas Price, che rappresenta la “fee” che il mittente effetivamente paga per ogni fase di calcolo risolta. Questo valore andrà ad influenzare la velocità dei miners nella rete per andare a confermare le transazioni. Maggior è il prezzo del gas che il mittente dell’operazione è disposto a pagare, più velocemente faranno l’operazione sapendo che la ricompensa è maggiore.

Il prezzo viene stabilito dividendo 1 Ether in piccole frazioni, denominate *"gwei"*, che corrispondono a 0,000000001 ETH.

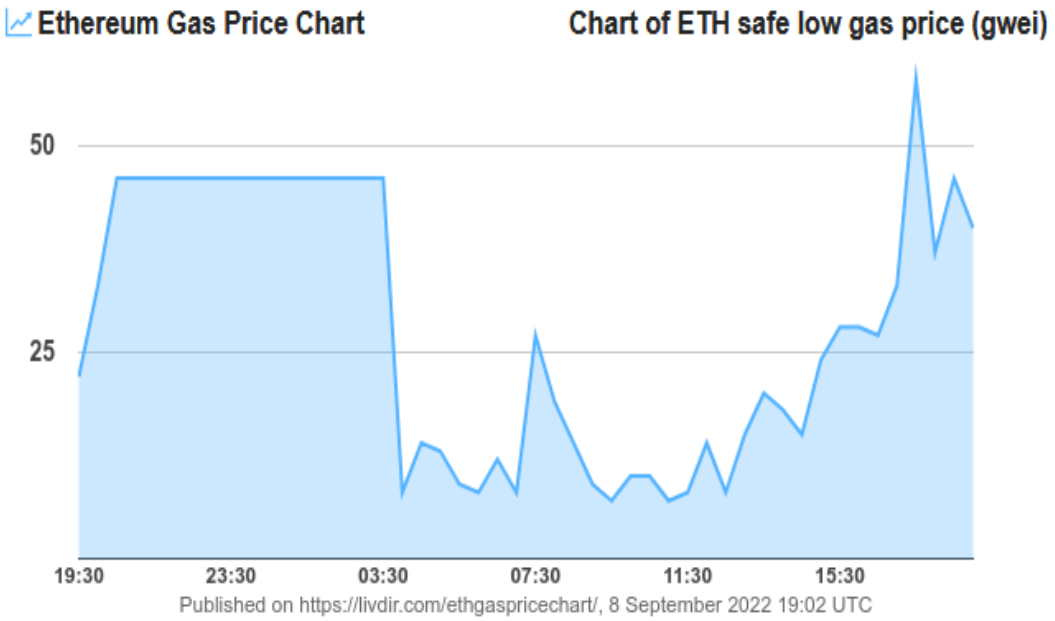
Gas Limit, che consiste nel numero massimo di calcoli che l'esecutore dell'operazione è autorizzato ad effettuare.

Figura 4 – Esempio del gasprice, in gwei



Fonte: gasnow.org

Figura 5 – Grafico dell'andamento del gas price in gwei in 24 ore



Fonte: livdir.com

2.2.2 Cardano

Figura 6 - Logo

L'altra altcoin presa in analisi è il risultato della volontà di unione tra ciò che era più importante del Bitcoin (il concetto di *deposito di valore*) e di Ethereum (i *contratti intelligenti*). Nato dall'idea di Charles Hoskinson, ex co-fondatore di

Ethereum (dal quale si staccò dato che il progetto prese una piega che non rispecchiava più a pieno quanto da lui voluto) è una piattaforma *open-source* decentralizzata creata dove alla base vi è l'*ADA*, la sua valuta digitale, che può essere utilizzata per inviare e ricevere fondi digitali. Si dice che il nome dato derivi dalla contessa del XIX secolo, Augusta Ada Lovelace, matematica inglese riconosciuta come la prima programmatrice di computer. Chiamato "l'Ethereum del Giappone" poiché il primo target di acquirenti è stato proprio il paese nipponico che, nel 2015, rappresentava il 95% dei sostenitori di questo progetto.
Seguendo il pensiero del suo fondatore, è bene andare a sottolineare che la blockchain è stata sottoposta fondamentalmente a tre stadi evolutivi:

> **Blockchain di prima generazione**, quella facente riferimento al bitcoin, dove l'obiettivo era di rispondere all'esigenza di andare a creare nuove forme di trasferimento monetario senza l'intervento degli intermediari. Il problema che sorgeva in questa prima generazione, però, era quello che questa tecnologia era limitata alle sole transazioni monetarie, senza possibilità di inserimento di condizioni una volta avvenuta la transazione.

> **Blockchain di seconda generazione** (Ethereum e smart contract), quella dove si possono scambiare non solo denaro, ma anche altri beni (come, per esempio, proprietà e azioni) in modo sicuro e senza intermediari.

Blockchain di terza generazione, quella di Cardano.

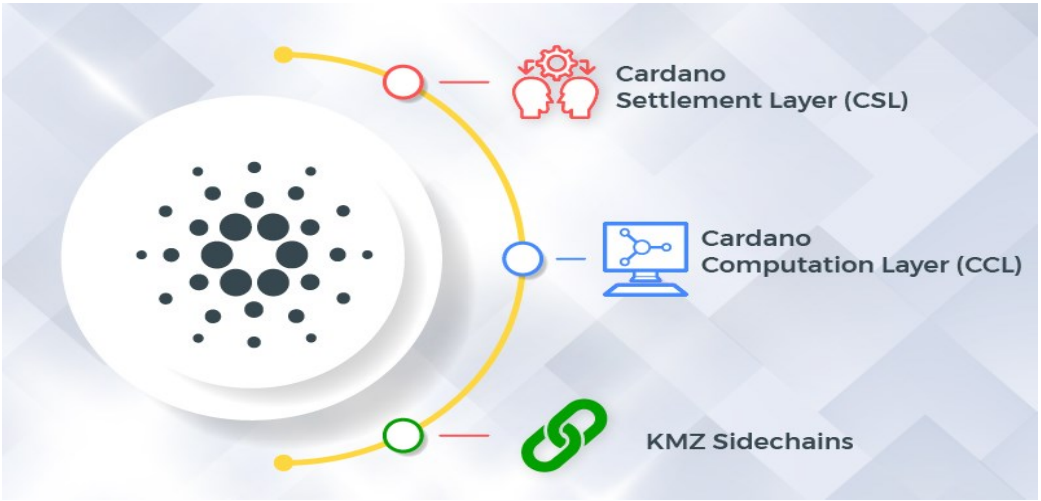
L'obiettivo dei creatori è quello di migliorare la scalabilità, la sicurezza, la governance e l'interoperabilità tra sistemi e regolamenti finanziari tradizionali. Quest'ultima mira a creare una specie di "internet delle blockchain", utilizzando le cosiddette *sidechain*., che servono per andare a migliorare le prestazioni di un'altra catena di blocchi. La piattaforma Cardano lavora sul protocollo di consenso "Ouroboros", creato da Cardano stesso nella fase iniziale della sua creazione, che risulta il primo protocollo *Proof of Stake* (*PoS*) progettato per ridurre al minimo in quantitativo di energia derivante dal mining, Proof of Work (PoW), andando ad eliminare enormi risorse di calcolo utilizzate dall'algoritmo di prova del lavoro

Nel sistema di Cardano, infatti, esistono due metodologie con le quali si va a dare il consenso per la verifica delle transazioni. La prima è la PoW, utilizzata da Bitcoin, con la risoluzione di calcoli matematici. La seconda, invece, è la PoS, che risulta più efficiente sotto il punto di vista di consumi energetici dato che non si basa sul mining; ciò è sostituito da più individui casuali che vanno a validare la transazione prima di essere inserita nella catena di blocchi.

Il protocollo lavora su layer differenti; sul primo, il CSL (Cardano Settlement Layer) si trovano tutte le informazioni inerenti alle transazioni ed è sempre su

questo livello che vengono trasferiti i token della piattaforma, gli ADA (il token viene utilizzato in maniera simile a come viene utilizzato attualmente il contante); il secondo, il CCL (Cardano Control Layer) va a gestire i dati degli account, ossia informazioni degli smart contract. Questa netta separazione è molto utile per aggiornamenti mirati e separati, andando ad aumentare la sicurezza, perché se un layer risulta compromesso, non significa che lo sia anche l'altro.

Figura 7 – Le specifiche di Cardano



Fonte: criptovalute24.com

2.3 La ricerca alla stabilità: le Stablecoin

I prezzi delle criptovalute sono caratterizzati dalla loro volatilità e da questa ne può discendere un'opportunità di un ingente guadagno ma anche di una tanto

grande perdita. Ma non tutte sono così oscillanti, alcune hanno la peculiarità di essere definite stabili: si sta facendo riferimento alle *Stablecoin.* Nome che deriva dall'unione delle parole "stabile" e "moneta", sono state create con l'obiettivo di non subire le stesse oscillazioni che una moneta, come per esempio il bitcoin, può tranquillamente subire. La differenza principale sta che queste sono ancorate ad un bene di cui ne vanno a formare la loro rappresentazione digitale. Le variazioni che andranno a subire saranno le stesse che subirà il bene prescelto e di solito questo è, perlomeno di regola, un mezzo di scambio, il cui valore risulta sotto un controllo centrale. Ciò comporta che la transazione viene reputata molto più sicura e certa poiché il rischio di trovare il valore modificato dopo averla effettuata risulta molto minore. Ma non è da escludere che anche qui vi possono essere delle oscillazioni, le quali però sono reputate molto più contenute perché avvengono secondo un cambio fisso. Da non scambiare per delle valute *FIAT*: le Stablecoin possono essere accostate anche all'oro, il quale è anch'esso incline a delle grandi oscillazioni, ma queste avvengono in un arco di tempo decisamente più ampio. Per il concetto della loro stabilità vengono soprannominate "*AntiBitcoin*".
Possono essere classificate in tre macrocategorie:

Stablecoin ancorate a valuta FIAT: stabilità di valore nel tempo; ogni token che viene creato è garantito da una moneta in valuta ufficiale, di solito il dollaro, che viene depositato, rappresentando così la garanzia

collaterale di valore del token. Come detto prima, non solo valute FIAT, ma anche altri beni come materie prime e metalli, ma il funzionamento rimane invariato.

Stablecoin ancorate a valute digitali: il bene materiale viene sostituito da un'altra criptovaluta che va quindi ad assumere la funzione di collaterale. Sono garantite da una riserva di monete digitali in numero maggiore a quello dei token emessi, per rispondere ad eventuali oscillazioni di valore.

Stablecoin algoritmiche: qui il sistema diventa decentralizzato e non collateralizzato, dato che non vi sono coperture: alla base vi è un algoritmo che opera in automatico con gli smart contract e con questo meccanismo viene preso un valore di riferimento, solitamente il dollaro, con la conseguenza che se il prezzo delle Stablecoin dovesse aumentare e il valore ritenuto "di soglia" dovesse essere superato, con l'algoritmo vengono emessi nuovi token.

Da un punto di vista strutturale, gli stablecoin sono generalmente costruiti sopra il protocollo blockchain di Ethereum: ciò fa si che gli utenti possono andare ad utilizzare le loro coin in qualsiasi altra applicazione che è progettata in maniera simile. Risultano impossibili da estrarre con il processo di mining, l'unico modo

per ottenerli è quello di trasferire il denaro *FIAT* sul conto dell'organizzazione in questione o comprarli direttamente sul mercato delle criptovalute.

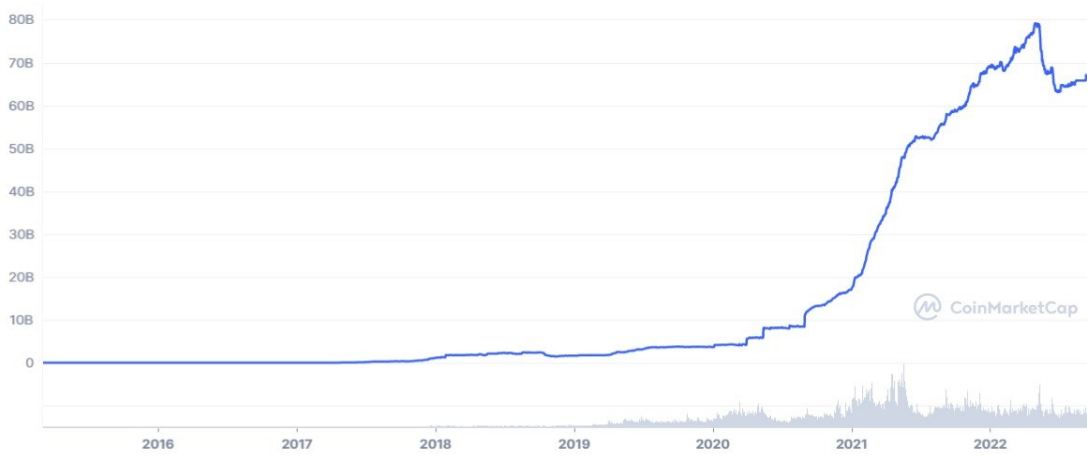
2.3.1 Tether

Figura 8 - Logo

Tether è il più grande stablecoin del mondo delle criptovalute. Poche sono le informazioni che trapelano riguardanti la sua fondazione ma risulta originariamente nato come *Realcoin* nel 2014, con un nome quasi a voler sottolineare differenza con le altre monete digitali, ed ha raggiunto in pochi anni grande fama mondiale tanto da essere tra la coin con maggiore capitalizzazione di mercato al mondo; basti pensare che oggi circa l'80% di tutti gli asset Bitcoin viene scambiato in criptovaluta Tether. Nella maggioranza dei casi, l'unità di Tether viene accostata e legata al prezzo di un dollaro e si fa riferimento alla sigla *USDT*; ma il progetto non si limita solamente al dollaro ed ingloba altre stablecoin: un Tether può essere anche legato al prezzo di un euro (*EURT*) e al prezzo di uno yuan cinese (*CNHT*). Per l'USDT, ancorandosi al dollaro, va a

creare un'ottima stabilità (dato che il suo valore non dipende dalla frequenza con cui la moneta viene acquistata e venduta) ma risultano prevedibili delle piccole oscillazioni, che girano tra i valori di 0,99 e 1,02 dollari. Le transazioni di Tether sono basate sulla piattaforma *Omni Layer* che ne va a garantire la sicurezza, la quale è basata a sua volta sulla blockchain di Bitcoin. Presenta delle commissioni applicate sul deposito e sul prelievo della moneta *FIAT* che sono in base al volume complessivo degli importi negli ultimi trenta giorni: da 100000 a 999999 dollari è dello 0,4%, da un milione a dieci milioni di dollari del 1%, al di sopra del 3%, quindi stiamo parlando di commissioni piccole, addirittura zero per il passaggio di denaro da un conto USDT all'altro per non ingenti somme di denaro. Importante non escludere il concetto che questa Stablecoin può essere utilizzata anche su altre blockchain come per esempio quella di Ethereum, dove i token coniati in questo caso, prendono il nome di "*ERC20*". Non risulta largamente accettato per l'acquisto di beni e servizi online; quindi, con il suo acquisto gli investitori hanno l'obiettivo di andare a detenere Tether in modo che in futuro possano andare a scambiarlo con altre criptovalute o convertire una moneta digitale in un'altra; quindi possono tenere i loro beni digitali simili alle valute *FIAT* ma allo stesso tempo mantenere la capacità di scambiarle facilmente con le altre criptovalute sul mercato, data la sua alta integrabilità nelle piattaforme di scambio.

Figura 9 - Capitalizzazione di mercato dal 2016 fino ad oggi, con il punto massimo raggiunto di 79,17 B di euro



Fonte: Coinmarketcap.com

CONCLUSIONI

Questo elaborato si è incentrato sulle caratteristiche di alcune delle nuove monete digitali in modo da comprendere se quest'ultime possano effettivamente in un futuro proporsi come un valido sostituto alle attuali valute *FIAT*; negli anni abbiamo visto un crescente interesse nei confronti di questo mondo, tanto da avere delle capitalizzazioni di mercato non indifferenti. Sicuramente ciò è il prodotto delle implementazioni e tecnologie inserite come la Blockchain, che garantisce una maggiore sicurezza, minori costi di transazione e una maggiore velocità per le informazioni. L'anno 2021 è stato un anno degno di grande nota per le criptovalute, con punte di valore per le singole monete incredibili per poi arrestare il loro "rally dei prezzi" drasticamente. Questo è stato un grande campanello d'allarme per gli investitori e per tutta l'economia in generale: il valore del dollaro e di tutte le altre valute a corso legale hanno dietro una collateralizzazione, una centralizzazione che va a dare garanzia del loro valore; invece quello delle monete digitali, come il Bitcoin, non è retto da alcuna garanzia data la sua decentralizzazione, la quale può risultare un bene ma anche un male perché il suo valore può variare bruscamente anche nelle stessa giornata. Per ovviare a questo problema sono entrate in gioco negli anni le Stablecoin, che puntano alla stabilità

ancorandosi ad un bene fisico od a una valuta *FIAT*, sapendo che le loro oscillazioni sono abbastanza contenute. Le criptovalute per potersi realmente affermare dovrebbero aver bisogno di un sistema di regole, nazionali ed internazionali, più efficiente di quello attuale che possano ridurre al minimo le probabilità di usi illeciti di queste piattaforme, nonché dalla volontà dei vari Paesi di attivarsi per andare incontro a questo nuovo mondo. Le fondamenta sono sicuramente buone, poiché nel corso degl'anni sono entrate in maniera molto più profonda nei servizi finanziari e nella cultura generale, ma ancora devono lavorare per esser degne di definirsi alternative alla pari delle valute FIAT e ciò non fa altro che avvalorare questa tesi.

SITOGRAFIA

https://www.agendadigitale.eu

https://www.blockchain4innovation.it

https://www.borsaitaliana.it

https://www.cmcmarkets.com

https://www.coinbase.com

https://www.conotoxia.com

https://www.consob.it

https://www.criptovaluta.it

https://www.ecb.europa.eu

https://www.gasnow.org

https://www.geeksforgeeks.org

https://www.ibm.com

https://www.investopedia.com

https://www.kmu.admin.ch

https://www.livdir.com

https://www.medium.com

https://www.mercati24.com

https://www.money.it

https://www.pmf-research.eu

https://www.techcompany360.it

https://www.thebalance.com

https://www.webeconomia.it