



**Politecnico
di Torino**

Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Gestionale
A.a. 2021/2022
Sessione di Laurea luglio 2022

Blockchain, ICOs e Central Bank Digital Currency

Come le criptovalute potrebbero rivoluzionare il mondo
finanziario

Relatrice:

Prof.ssa Laura Rondi

Candidato:

Davide Visconti

INDICE

INTRODUZIONE	1
CAPITOLO 1 – BLOCKCHAIN E CRIPTOVALUTE.....	3
1.1 LA BLOCKCHAIN	3
1.1.1 <i>SIMILITUDINI CON LE ALTRE TECNOLOGIE</i>	4
1.1.2 <i>ARCHITETTURA DI RETE E CRITTOGRAFIA</i>	5
1.1.3 <i>INDIRIZZI, WALLET ED EXCHANGE</i>	8
1.1.4 <i>TRANSAZIONI E MECCANISMI DI CONSENSO</i>	11
1.2 LE CRIPTOVALUTE	15
1.2.1 <i>CARATTERISTICHE E DIFFERENZE CON VALUTE FIAT</i>	15
1.2.2 <i>TIPI DI TOKEN</i>	18
1.2.3 <i>BITCOIN</i>	21
1.2.4 <i>ETHEREUM</i>	27
1.2.5 <i>PANORAMICA E ANDAMENTO DEL MERCATO</i>	34
1.2.6 <i>ULTERIORI CRITICHE E CENNI DI REGOLAMENTAZIONE</i>	37
CAPITOLO 2 – LE INITIAL COIN OFFERINGS	40
2.1 PIATTAFORME E TOKEN	42
2.2 ICO, IEO E IDO	45
2.3 MECCANISMO DELL’ICO	47
2.4 IL WHITE PAPER	51
2.5 FATTORI DI SUCCESSO DI UNA ICO	54
2.6 SIMILITUDINI CON ALTRI METODI DI FINANZIAMENTO	60
2.7 LE MAGGIORI ICOS DELLA STORIA	67
2.8 COLLOCAZIONE GEOGRAFICA	73
2.9 CENNI DI REGOLAMENTAZIONE	79

CAPITOLO 3 – LE STABLECOIN	87
3.1 STABLECOIN	87
3.1.1 <i>TIPI DI STABLECOIN</i>	88
3.1.2 <i>IL CASO TERRA-LUNA E LE RIPERCUSSIONI SUL MERCATO</i>	90
3.1.3 <i>L'UTILIZZO DELLE STABLECOIN NEL MERCATO DELLE CRIPTOVALUTE</i>	94
3.1.4 <i>CRITICHE ALLE STABLECOIN</i>	97
3.1.5 <i>RISCHI PER I MERCATI FINANZIARI</i>	100
3.2 CENTRAL BANK DIGITAL CURRENCY	102
3.2.1 <i>CONTESTO STORICO E IMPORTANZA PER LE BANCHE CENTRALI</i>	103
3.2.2 <i>DIVERSI TIPI DI CBDC</i>	105
3.2.3 <i>BENEFICI DELL'ADOZIONE DI UNA MONETA DIGITALE</i>	106
3.2.4 <i>ULTERIORI RISCHI DELL'ADOZIONE DI UNA MONETA DIGITALE</i>	108
3.2.5 <i>IMPATTO DELLE CBDC SUL CONTESTO ECONOMICO</i>	110
3.2.6 <i>LA SITUAZIONE ATTUALE NEL MONDO</i>	115
CONCLUSIONE	121
BIBLIOGRAFIA	126
SITOGRAFIA	130
FONTI FIGURE	138

INTRODUZIONE

La tecnologia blockchain ha fatto la sua comparsa nel 2009 e da allora ha guadagnato sempre maggior rilievo nella nostra società, arrivando ad imporsi come una delle più grandi innovazioni di questo periodo.

In questo scritto si vuole inizialmente dare una panoramica generale della tecnologia, spiegandone gli aspetti principali ed essenziali da conoscere per interfacciarsi con questo mondo e analizzando quella che è stata una delle prime applicazioni, la criptovaluta, con uno sguardo più attento alle blockchain di Bitcoin ed Ethereum, quelle che al momento hanno riscosso il maggior successo. Dopo aver fatto ciò, si volge lo sguardo alle Initial Coin Offerings, ovvero a quelle operazioni che permettono ad un'azienda di effettuare l'emissione di una moneta da distribuire alla folla in cambio di fondi; l'operazione ha raggiunto una certa popolarità tra il 2017 e il 2018, e si vogliono analizzare i fattori che l'abbiano portata ad avere questa fortuna ed effettuare un paragone con gli altri metodi di finanziamento esistenti, per capire il perché in alcuni stati questa metodologia di raccolta di fondi abbia avuto un boom così rapido e un così alto apprezzamento tra gli imprenditori, accennando anche alle regolamentazioni presenti nelle diverse nazioni.

Infine, nell'ultimo capitolo si vuole analizzare quella che è un'applicazione della tecnologia che ultimamente sta riscuotendo molta fortuna poiché risulta di fondamentale utilizzo nel mercato delle criptovalute, la stablecoin, un tipo di moneta creata con l'intento di mantenere l'equivalenza con una valuta fiat e di combattere quindi la volatilità, che è caratteristica di tutte le altre criptovalute. Tra le stablecoin, nel finale viene dato risalto alle Central Bank Digital Currency, ovvero le stablecoin che vengono emesse direttamente da una banca centrale, soffermandosi su quali siano le ripercussioni

dell'emissione di questo tipo di moneta sull'economia di uno stato e sui i benefici che i cittadini potrebbero avere dall'adozione di questa tecnologia, con un focus finale incentrato sui maggiori progetti che sono attivi in questo settore.

CAPITOLO 1 – BLOCKCHAIN E CRIPTOVALUTE

1.1 LA BLOCKCHAIN

L'origine del termine e del concetto di Blockchain sono attribuiti a Satoshi Nakamoto che nel 2008 pubblicò un paper dal titolo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", proponendo un innovativo metodo di gestione dei pagamenti svincolati dal controllo da parte di un'istituzione finanziaria, attraverso un network peer-to-peer¹ avente funzioni crittografiche avanzate e attraverso l'adozione di una moneta elettronica.

Ad oggi con il termine blockchain intendiamo un registro digitale, decentralizzato e distribuito, nel quale vengono memorizzati i dati che vengono visti come dei "blocchi" sequenziali di informazioni: salvare l'informazione è l'azione essenziale in una blockchain. Se non in casi estremi, non è possibile la modifica o la rimozione dei dati esistenti, ma solo l'aggiunta del nuovo blocco di informazioni in coda a quelli già presenti; per far sì che il sistema sia utilizzabile e utile è importante che sia definito un elevato livello di crittografia dei dati e un protocollo di consenso affidabile di modo che il network risulti accessibile a tutti ma anche sicuro, affidabile e neutrale, ovvero che non sia necessario riporre fiducia negli attori presenti ma solo nel sistema stesso.

Le blockchain si dividono in *pubbliche*, *consortium* e *private*; le prime sono accessibili a tutti e i nodi² che ne fanno parte possono visualizzare il registro ed effettuare o validare transazioni e sono le più comuni e utilizzate in quanto sfruttano a pieno le potenzialità della tecnologia; le ultime vengono utilizzate qualora debba essere presente un'autorità centrale che attraverso dei livelli gerarchici regolamenti l'accessibilità alle informazioni

¹ Con il termine peer-to-peer si intende un'architettura di rete in cui, a differenza delle reti gerarchizzate classiche, ogni nodo che ne fa parte svolge sia funzioni di server che di client.

² Con il termine nodo si indica una macchina che fa parte della blockchain.

con cui ogni nodo sia in grado di interagire, ed infine le *consortium* sono un misto delle due tipologie precedenti e ricoprono un ruolo marginale in confronto alle altre (Chiap et al, 2019).

1.1.1 SIMILITUDINI CON LE ALTRE TECNOLOGIE

La tecnologia DLT (Distributed Ledgers³ Technology) presenta una grande somiglianza con la blockchain, tanto che spesso i due termini vengono usati come sinonimi; con il termine “distribuito” in informatica si fa riferimento a un qualcosa che viene memorizzato su diverse macchine: nel caso dei registri con il termine si intende che ogni nodo replica e salva una copia del registro stesso. La sottile differenza tra la blockchain e la DLT sta nel fatto che nel caso della prima le informazioni memorizzate sono collegate tra loro come una catena a cui viene aggiunto ogni volta un blocco, cosa che non è detta nel caso della seconda tecnologia. Si potrebbe quindi affermare che la blockchain sia un caso particolare di Ledger Distribuito.

Un'altra somiglianza si può intravedere con i database distribuiti (DDBMS), in quanto essi non sono altro che un insieme di database correlati tra loro e distribuiti su una rete di computer. Se a primo impatto le tecnologie possono sembrare uguali, vi è però una differenza sostanziale: i database sono progettati per poter inserire e modificare i dati, azione che nella blockchain non può avvenire in quanto è permessa la sola aggiunta in coda dei dati, ma non la modifica di quelli presenti. Questa differenza fa sì che le due tecnologie ricoprano spesso ruoli differenti, in quanto i database sono più veloci ma necessitano di elevati livelli di sicurezza e di controllo degli accessi, essendo possibile a

³ Con il termine *ledgers* ci si riferisce al libro mastro della contabilità.

chiunque modificare i dati e potenzialmente creare un punto di rottura in grado di far collassare l'intero sistema. Questo livello di controllo non è invece necessario nella “catena a blocchi” che è pensata appositamente per essere utilizzata da parti “sconosciute” senza che sia necessaria una regolamentazione degli accessi e senza che venga meno la fiducia nel sistema. Ed è proprio questa la principale rivoluzione della blockchain: il sistema stesso, per come risulta strutturato, è in grado di garantire alle parti coinvolte di lavorare in un ambiente in cui fiducia, immutabilità e sicurezza sono le principali caratteristiche (Gupta, 2018) (Chiap et al, 2019).

1.1.2 ARCHITETTURA DI RETE E CRITTOGRAFIA

Come si è accennato nel paragrafo precedente, l'elemento fondamentale di una blockchain sono i nodi, termine con il quale si indicano tutti i terminali connessi alla rete e facenti parte della blockchain. Tra essi possiamo fare la distinzione tra nodi *light* e nodi *full*: questi archiviano localmente una copia di tutta la blockchain (ad esempio, i full node della blockchain di Bitcoin archiviano al momento circa 380GB di dati⁴) e sono completamente indipendenti, sono cioè in grado di propagare i blocchi e le transazioni e di rifiutare i blocchi ritenuti invalidi senza la necessità di confrontarsi con altri nodi; quegli invece non memorizzano l'intera catena ma ricevono da un nodo full fidato le informazioni delle quali hanno bisogno per funzionare correttamente. È evidente quindi la differenza di fiducia da riporre nel sistema se si fa uso di uno piuttosto che dell'altro: con un light node si guadagna molto in semplicità di utilizzo ma si perde la capacità di

⁴ <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>

verificare in modo indipendente la correttezza dei dati (questo è il tipo di nodo utilizzato dalla grande maggioranza degli utenti).

Solitamente quando ci riferiamo ad una blockchain intendiamo una rete con *architettura e autorità decentralizzate*, ovvero ad una rete le cui risorse sono distribuite tra i vari nodi e nella quale non esiste un'autorità centrale che gestisca il controllo e la regolamentazione; i nodi sono considerati uguali tra di loro e non vi è il rischio che si crei un punto di rottura in grado di far crollare il sistema, cosa che invece può accadere nelle reti con architettura centralizzata. Oltre ai fattori appena citati un altro tipico di una blockchain è la *logica centralizzata*. In contrapposizione agli altri due aspetti decentralizzati, essa è essenziale perché la rete deve essere contraddistinta in ogni istante da un singolo stato: se così non fosse sarebbe possibile avere più stati considerati validi contemporaneamente e qualsiasi nodo potrebbe modificare o aggiungere informazioni senza alterare il funzionamento del sistema, proprio ciò che comunemente si vuole evitare quando si utilizza questo tipo di tecnologia (Chiap et al, 2019).

Per trasferire gli asset su una blockchain vengono utilizzati gli indirizzi, identificatori univoci della destinazione di una determinata transazione (si possono paragonare a dei profili utente di un social network). Per capire come viene creato un indirizzo è di fondamentale importanza avere chiaro il concetto di crittografia⁵.

Il principale tipo di crittografia utilizzato nell'ambito di interesse di questo elaborato è la cosiddetta crittografia a chiave pubblica, uno dei metodi crittografici più utilizzati su internet. L'idea alla base di questa tecnologia è quella di creare due chiavi crittografiche⁶

⁵ Con il termine crittografia si fa riferimento ad un sistema di scrittura secondo determinati codici che consentono di mantenere la segretezza dell'informazione.

⁶ Il termine chiave crittografica indica una stringa alfanumerica che implementa l'algoritmo di codifica dell'informazione.

legate tra loro da una relazione matematica: la chiave *privata* viene generata casualmente e deve rimanere segreta e la chiave *pubblica* viene ricavata a partire da quella privata tramite operazioni matematiche e può essere condivisa con altri utenti. La chiave privata corrisponde solitamente a un numero molto grande rappresentato in esadecimale (nel caso di Bitcoin, ad esempio, la chiave occupa uno spazio di 256 bit). A livello computazionale è molto semplice per un computer generare una chiave privata e da essa la relativa chiave pubblica corrispondente, mentre è quasi impossibile effettuare il processo inverso: ricavare la chiave privata partendo da quella pubblica richiede una potenza di calcolo attualmente non raggiungibile (si parla di milioni di anni di calcolo da parte di un supercomputer moderno).



Figura 1 - Esempio di crittografia a chiave privata. Fonte: criptoinvestire.com

Accanto all'utilizzo delle chiavi per la crittazione dei contenuti viene utilizzata un'altra tecnica denominata *hashing* che, come diremo anche in seguito, sarà anche di fondamentale importanza negli algoritmi di consenso. Una funzione di hash è una funzione che produce una stringa di lunghezza definita a partire da un input di lunghezza arbitraria e ha la caratteristica di essere non invertibile: data la stringa prodotta dalla funzione non è possibile ricavare l'input iniziale se non provando tutte le combinazioni

possibili. Nel paradigma di Internet si usa una combinazione di crittografia a chiave pubblica e hashing per avere una firma digitale; nell'implementare il meccanismo di firma digitale il mittente utilizza una funzione di hash sul messaggio da inviare, dopodiché utilizza la sua chiave privata per criptare l'hash ottenuto e invia il contenuto. Il destinatario utilizzerà la chiave pubblica del mittente per decriptare l'hash e a sua volta calcolerà la funzione di hash sul messaggio ricevuto: se gli hash ottenuti sono uguali si ha la certezza che il messaggio non sia stato modificato da nessuno (ciò cambierebbe l'hash) e che il mittente sia esattamente la persona che ci aspettiamo (utilizzando la chiave pubblica per decriptare siamo certi che il messaggio sia stato criptato con la chiave privata corrispondente, sennò l'operazione non andrebbe a buon fine). Questa procedura fa sì che la firma digitale garantisca l'autenticazione, l'integrità e il non ripudio (il mittente che firma un messaggio non può negare in un secondo momento di averlo firmato) (Carboni, 2017).

1.1.3 INDIRIZZI, WALLET ED EXCHANGE

Le tecniche trattate, come abbiamo precedentemente accennato, sono di fondamentale importanza per la creazione di un indirizzo; prendiamo, ad esempio, la creazione di un indirizzo sulla blockchain di Ethereum: per prima cosa viene generata casualmente una chiave pubblica e a partire da essa viene creata la corrispondente chiave privata; successivamente vengono applicate diverse funzioni di hash alla chiave pubblica e si ottiene così il risultato cercato che, nel caso della blockchain di Ethereum, sarà un risultato simile al seguente: 0x7949635E2877ef8ca37B8526507AC214B0423Ebf.

La chiave privata è l'elemento fondamentale di un indirizzo nonché l'unico modo che ha il proprietario di dimostrare di essere effettivamente lui a possedere ciò che l'indirizzo contiene: qualora il proprietario perdesse la chiave privata, non sarebbe in alcun modo possibile accedere all'indirizzo.

Per gestire gli indirizzi vengono solitamente utilizzati degli strumenti denominati *wallet*: un wallet permette la memorizzazione delle chiavi pubbliche e private di un indirizzo. È bene ricordare che tutte le informazioni degli indirizzi sono salvate sulla blockchain e di conseguenza non vanno mai perse; di contro però è possibile perdere le chiavi di accesso al proprio wallet rendendo così impossibile accedervi e recuperarne il contenuto (che potrebbe essere economicamente anche molto elevato). Esistono diversi tipi di portafoglio e diverse metodologie di classificazione che non verranno trattate e approfondite; una distinzione significativa è basata sull'ambiente in cui operano i wallet e li distingue così tra *hot storage* e *cold storage*: i primi sono dei wallet collegati ad Internet (ovvero wallet le cui chiavi private sono state generate o sono memorizzate in macchine connesse a Internet), mentre i secondi indicano dei wallet le cui chiavi private non hanno mai avuto accesso a Internet. Un cold wallet ha una sicurezza intrinseca decisamente maggiore: è molto più difficile per un malintenzionato entrare in possesso delle chiavi di accesso di un portafoglio se esse sono memorizzate su un dispositivo non connesso alla rete, ma allo stesso tempo risulta impossibile recuperare la chiave qualora andasse persa (Chiap et al, 2019).

Una menzione particolare, data la popolarità riscossa negli ultimi anni, la meritano gli *exchange*; essi non sono dei wallet, ma possono svolgere anche questa funzione in quanto un utente può sia depositare i suoi fondi delegandone all'exchange stesso la gestione, sia effettuare operazioni di compravendita delle diverse criptovalute (con un processo molto

simile all'acquisto su una borsa valori). La distinzione più rilevante viene fatta tra exchange centralizzati e decentralizzati, con i secondi aventi un peso irrisorio rispetto alla totalità delle transazioni in confronto ai primi. Un exchange centralizzato gestisce i portafogli degli utenti, possedendone anche le chiavi private, e ciò fa sì che l'utente finale abbia una notevole semplificazione per quanto riguarda il comprare criptovalute e il mantenere al sicuro le chiavi, ma è anche al centro di numerose critiche in quanto per molti risulta incomprensibile affidarsi ad una piattaforma con controllo centralizzato per interfacciarsi con una tecnologia che ha nella decentralizzazione il suo punto di forza⁷. Un exchange funziona in un modo molto simile ad una borsa valori in quanto contiene diversi mercati⁸ (ognuno basato sulle proprie regole di domanda e offerta) e, onde evitare spiacevoli sorprese, necessiterebbe di una adeguata conoscenza dei fattori caratterizzanti di un mercato per effettuare investimenti quali possono essere, ad esempio, i diversi tipi di ordini piazzabili, le posizioni che si possono assumere, piuttosto che la profondità del mercato o la leva finanziaria. Inoltre, gli exchange hanno operato per diversi anni senza delle adeguate regolamentazioni dal punto di vista legale e in mercati caratterizzati da bassi volumi e da poca liquidità e questo ha fatto sì che molte persone abbiano mosso ad essi accuse di manipolazione di mercato.

Gli exchange centralizzati sono anche le vittime preferite degli attacchi da parte degli hacker, dato che i loro indirizzi contengono una quantità notevole di criptovalute e un eventuale furto è solitamente molto profittevole ed è difficile smascherarne gli autori; dal 2012 più di 46 exchange hanno perso per via di attacchi informatici complessivamente

⁷<https://it.cointelegraph.com/news/ethereum-s-vitalik-buterin-blasts-centralized-crypto-exchanges-i-hope-they-burn-in-hell>

⁸ Per mercato si intende il luogo dove avviene lo scambio tra due beni (per un exchange i beni in questione sono delle criptovalute o talvolta delle valute fiat).

oltre 2,5 miliardi di dollari⁹, con l'ultimo attacco di oltre 30 milioni di dollari registrato a gennaio 2022 ai danni di Crypto.com, exchange divenuto particolarmente famoso nell'ultimo periodo per la semplicità di utilizzo e per le numerose sponsorizzazioni in ambito sportivo con investimenti di cifre molto rilevanti¹⁰.

1.1.4 TRANSAZIONI E MECCANISMI DI CONSENSO

Quando viene effettuata una transazione valida essa viene scritta sulla blockchain ed implica quindi un cambio di stato nella blockchain stessa; abbiamo visto che una blockchain è logicamente centralizzata per cui deve esserci un solo stato ritenuto valido dai nodi facenti parte del network, ed è proprio qui che entra in gioco il consenso: una transazione viene ritenuta valida se il consenso del network la ritiene valida.

In una blockchain se una transazione è effettuata e validata non è possibile modificarla o annullarla, al contrario di come siamo abituati per molte transazioni monetarie come ad esempio i bonifici bancari. Il primo passo per effettuare una transazione valida è quello di dimostrare di possedere il bene oggetto del trasferimento, operazione resa possibile dal meccanismo della firma digitale; successivamente i nodi devono raggiungere un accordo sullo stato della catena, operazione non banale se si opera in un ambiente potenzialmente ostile come quello di una rete con diverse macchine interconnesse.

I principali attori che partecipano al meccanismo di consenso sono i nodi full e i *miner*; i primi si occupano principalmente di verificare che i nuovi blocchi siano validi e di propagarli quindi sulla rete, mentre gli ultimi hanno il compito di creare i nuovi blocchi

⁹ <https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/>

¹⁰ <https://bebeez.it/fintech/e-crypto-com-il-re-degli-sponsor-dello-sport-ecco-la-mappa-delle-maggiori-sponsorship-crypto-nel-settore/>

e svolgono un'attività comunemente chiamata *mining*. Quando viene effettuata una transazione su una blockchain essa finisce in un pool di transazioni e il miner sceglie le transazioni da raggruppare che finiranno in un nuovo blocco da aggiungere alla catena; una volta che esso è stato creato viene aggiunto in coda e propagato sulla rete dove gli altri nodi si esprimeranno sulla validità dello stesso. Per raggiungere il consenso sono stati sviluppati diversi algoritmi e se ne stanno creando sempre di nuovi per ovviare ai problemi di scalabilità della tecnologia, che ad oggi rappresenta una delle sfide più importanti per l'adozione della stessa su larga scala (Balani et al, 2017).

I due protocolli di consenso maggiormente utilizzati al momento e dei quali accenneremo il funzionamento sono il *Proof of Work (PoW)* e il *Proof of Stake (PoS)*. Il PoW (in italiano “prova del lavoro”) è stato il primo adottato nella blockchain di Bitcoin ed è tutt'ora ancora utilizzato dalla stessa e dalla maggior parte delle altre; in questo algoritmo i miners competono per trovare la soluzione ad un problema matematico complesso, caratterizzato da una determinata difficoltà, e in cui è coinvolto il calcolo di un hash inverso con alcuni vincoli che si risolve soltanto avendo a disposizione una capacità computazionale estremamente elevata. Quando uno dei miners trova la soluzione al problema crea il nuovo blocco e riceve le ricompense pattuite per il lavoro svolto. Questo algoritmo rende estremamente difficile per un malintenzionato sabotare la blockchain o i blocchi parziali in quanto ogni cambiamento implica un ricalcolo di tutti i blocchi successivi affinché essi siano ritenuti validi (se questo non avviene si ha un cambiamento negli hash rispetto alle sequenze precedenti e la nuova la sequenza di blocchi viene ritenuta non valida). Nel Proof of Work si compete quindi sulla potenza di calcolo, misurata in Hashrate/s (cioè in quante funzioni di hash è possibile calcolare in un secondo), e questo rende la blockchain estremamente affidabile: per operare un attacco in

grado di modificare un blocco intermedio si deve essere in grado di ricalcolare i blocchi successivi più velocemente di tutti gli altri miner, si deve cioè possedere più del 50%¹¹ della potenza di calcolo della rete, che nel caso di blockchain di dimensioni rilevanti è praticamente impossibile, come si può notare nella figura sottostante che indica la potenza di calcolo della rete Bitcoin nel 2019 (attualmente la potenza di calcolo è quasi triplicata rispetto a quel momento)¹².

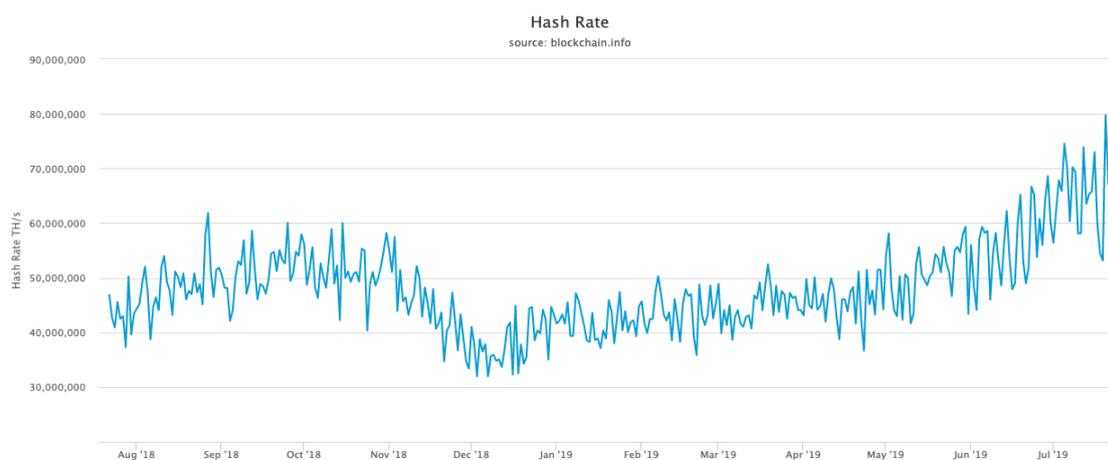


Figura 2 - Potenza di calcolo della rete di Bitcoin. Fonte: blockchain.info.

Di contro però, il sistema non offre un elevato grado di protezione dagli attacchi nel caso in cui la blockchain sia di dimensioni ridotte e, nel caso invece di blockchain di grandi dimensioni, si va incontro ad un uso molto intenso della potenza di calcolo (e quindi di energia elettrica) e si ha un sistema con bassa scalabilità. Solitamente nell'algoritmo la generazione di un blocco ha un tempo piuttosto costante (basato sull'hashrate totale del sistema e periodicamente aggiornato) e aumentando notevolmente le transazioni si arriva ad avere un collo di bottiglia non facile da superare (Jaggi et al, 2021).

¹¹ <https://academy.bit2me.com/it/51-attacco-bitcoin/>

¹² <https://bitinfocharts.com/comparison/bitcoin-hashrate.html#3y>

Per ovviare al problema dell'enorme mole di calcoli da effettuarsi si è pensato all'algoritmo PoS. Al contrario del PoW in questo meccanismo non è importante la potenza di calcolo bensì la quantità di token posseduti: un utente può decidere di lasciare in *stake* le proprie monete (processo che consiste nel “bloccare” le monete sulla piattaforma fino a quando non si conclude l'operazione e che concettualmente si potrebbe paragonare ad un deposito vincolato) e partecipare così al processo di mining. In questo algoritmo i miners vengono chiamati validatori e colui che sarà deputato alla creazione del nuovo blocco viene scelto in base alla quantità di monete che ha in stake: più monete si hanno più è alta la probabilità di essere scelti come validatori e di assicurarsi quindi la ricompensa per la creazione del blocco (a differenza del PoW, nel PoS in realtà non sempre viene donata una ricompensa per la genesi del blocco ma gli utenti che effettuano una transazione pagano delle “tasse” che servono a ricompensare i validatori). In questo modo il processo di creazione del blocco diventa estremamente più rapido in quanto non è necessario effettuare calcoli complessi e si possono mettere in atto dei meccanismi di punizione qualora il validatore tenti di propagare dei blocchi che saranno ritenuti non validi, come ad esempio bruciare le monete detenute in stake e identificare il nodo come malevolo impedendogli di essere nuovamente un validatore. Anche questo sistema è vulnerabile ad un attacco del 51% ma questa volta per effettuarlo non serve un'estrema potenza di calcolo, bensì essere il detentore del 51% delle monete in circolazione sulla blockchain; è dunque evidente che oltre alla difficoltà di possedere una quantità di token così elevata (si pensi al controvalore economico di avere una tale quantità di monete su una blockchain di dimensioni rilevanti), in molti casi sarebbe svantaggioso portare un attacco dato che si avrebbe una progressiva perdita di fiducia degli utenti del sistema che porterebbe in poco tempo a ridimensionare (se non ad azzerare) il valore del token della

blockchain e ad infliggere le maggiori perdite economiche a chi ha effettuato l'attacco data la notevole percentuale di monete in suo possesso (Chiap et al, 2019) (Taylor, 2021).

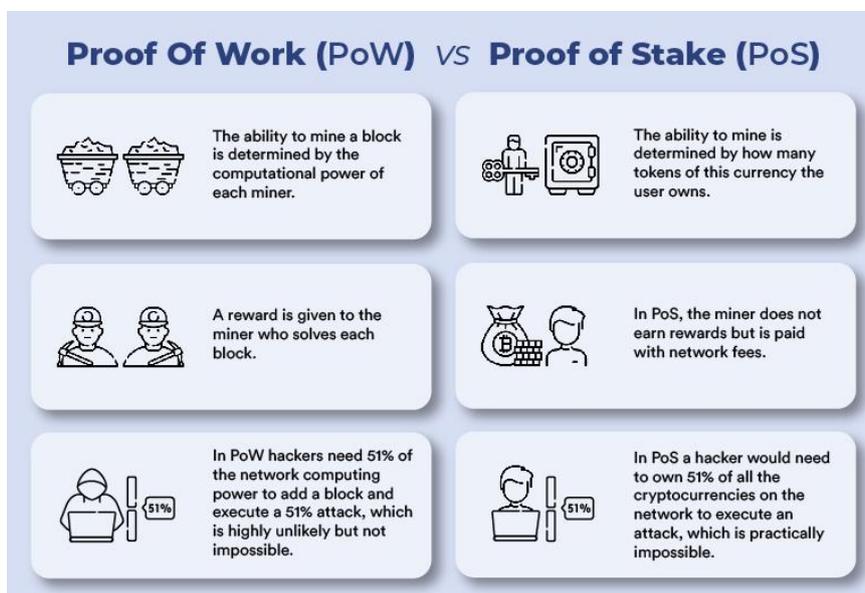


Figura 3 - Differenze tra Pow e PoS. Fonte: blog.bitnovo.com

1.2 LE CRIPTOVALUTE

Le criptovalute sono state la prima applicazione dopo la nascita della tecnologia blockchain; grazie ad esse è possibile ottenere lo scambio di valore (da qui la denominazione di “Internet del valore”) senza la necessità di una terza parte che funga da garante e senza rischiare di incorrere nel rischio di controparte, ma solo riponendo fiducia nel corretto funzionamento del sistema.

1.2.1 CARATTERISTICHE E DIFFERENZE CON VALUTE FIAT

Con il termine valuta fiat ci riferiamo al denaro che viene comunemente usato nel mondo moderno, ovvero quello che viene riconosciuto e accettato come metodo di pagamento in

quanto dichiarato a corso legale (l'euro, ad esempio, è una valuta fiat in corso legale in Italia)¹³. La caratteristica principale del denaro fiat è quella di non avere un valore intrinseco (come, ad esempio, il denaro commodity) e può essere considerato come il primo esempio di sistema monetario centralizzato. Nell'utilizzare questo tipo di moneta si ripone fiducia nell'istituzione centrale che la emette (solitamente una banca centrale), che, di concerto con i governi, ha il potere di decidere la quantità di denaro circolante e di modificare l'offerta di moneta per gestire al meglio gli eventi che possono avere ripercussioni sul sistema monetario e, di conseguenza, su tutti i cittadini (la cosiddetta "politica monetaria"). Ovviamente il denaro fiat esiste anche in forma digitale: solo una piccola parte della valuta in corso legale in uno stato è tangibile, la maggior parte esiste solo come facente parte di database informatici (gran parte del denaro posseduto dalle banche, ad esempio, è sotto forma di denaro digitale). Questo tipo di denaro ha tratti in comune con le criptovalute che, come sappiamo, hanno la particolarità di essere completamente digitali; tuttavia, esse si differenziano per il fatto che sono basate su tecnologia blockchain e per il fatto di non essere utilizzate come moneta in corso legale, anche se questa tendenza potrebbe subire un'inversione: nel 2021 il paese di El Salvador ha, per primo al mondo, adottato Bitcoin come moneta in corso legale¹⁴. Già ora, per paesi di dimensioni non particolarmente rilevanti e caratterizzati da economie e monete deboli, si potrebbero avere dei vantaggi nell'adottare come valuta ufficiale una criptovaluta, ma sono presenti ancora numerosi rischi di non poco conto, in primis l'elevata volatilità caratteristica delle valute virtuali a differenza del denaro emesso dalle banche centrali.

¹³ <https://www.treccani.it/enciclopedia/fiat-money/>

¹⁴ <https://www.ilsole24ore.com/art/bitcoin-el-salvador-primi-paese-ad-adottarlo-come-valuta-legale-AExYt8g>

Una criptovaluta viene quindi usata per permettere il trasferimento di valore in un sistema basato su tecnologia blockchain; questa peculiarità fa sì che le criptovalute non siano identiche tra di loro ma che ereditino le proprietà della blockchain sulla quale sono sviluppate. Si possono così avere criptovalute incentrate sulla sicurezza, piuttosto che sulla privacy o sulla decentralizzazione: ogni criptovaluta cerca di risolvere un problema specifico e differente dalle altre.

Ereditando le proprietà della catena a blocchi dalla quale derivano, le criptovalute sono intrinsecamente sicure e senza bisogno di fiducia (se non nel funzionamento del sistema, grazie all'implementazione degli algoritmi visti in precedenza), immutabili (le transazioni non si possono modificare), aperte (non è presente un'autorità centrale di controllo) e neutrali (non discriminano tra gli utenti, ognuno può effettuare transazioni con chiunque altro). Un aspetto importante e caratterizzante di queste valute digitali è la loro politica monetaria: proprio come una banca centrale decide le politiche da attuare per la valuta di propria emissione, il consenso del network le decide per la criptovaluta sviluppata nella piattaforma. Solitamente il tasso di crescita di una criptovaluta è definito da una relazione matematica e ciò rende possibile sapere quante monete sono in circolazione in qualsiasi momento e quante ne saranno in circolazione in futuro. Tra i parametri da conoscere per comprendere la politica monetaria di una criptovaluta giocano un ruolo fondamentale la quantità totale (*total supply*) e la quantità massima (*max supply*), definita dal consenso del network e non modificabile; la prima si riferisce alla quantità di monete che è stata generata fino a quel momento, mentre la seconda indica la quantità massima di monete che potranno essere emesse e distingue tra monete emesse in quantità limitata (ad esempio Bitcoin, la cui *max supply* ammonta a 21 milioni) e monete emesse in quantità illimitata (come ad esempio Ethereum, che al momento ha un'emissione annua di circa il 4% senza

un limite massimo di monete definito a priori)¹⁵. Un ultimo indicatore utile, anche se più difficile da calcolare con precisione, è quello della quantità circolante (circulating supply), che indica la quantità di coin spendibili; questo numero è inferiore alla quantità totale perché da essa vanno dedotte le monete che non possono essere utilizzate perché i proprietari hanno perso le chiavi di accesso agli indirizzi e le monete già prodotte ma non ancora rilasciate dal creatore (Chiap et al, 2019).

1.2.2 TIPI DI TOKEN

Le criptovalute vengono classificate utilizzando diversi parametri e valutando diversi attributi; per avere un'idea della distinzione che verrà proposta bisogna sapere cosa si intende con il termine *smart contract*: uno smart contract è un programma che esegue i termini e le condizioni di un normale contratto e concettualmente può essere equiparato ad esso. La sostanziale differenza risiede nel fatto che nel contratto “intelligente” il rispetto dei termini contrattuali viene gestito automaticamente sulla base di un codice programmato su una blockchain; lo smart contract quindi non è altro che un programma che viene eseguito automaticamente e che contiene delle condizioni che lo rendono caratteristicamente simile ad un comune contratto.

I due termini distinti che vengono utilizzati per descrivere le criptovalute sono quello di moneta (coin) e quello di token, anche se, tendenzialmente, essi vengono usati come sinonimi. La letteratura non ci dice esattamente quando vada usato un termine piuttosto che l'altro, ma espone qualche differenza tra i due: con il termine moneta si descrive un oggetto basato su tecnologia blockchain che ha come unico scopo quello di permettere il

¹⁵ <https://www.wisdomtree.eu/it-it/blog/2021-07-06/ethereum-a-deconstruction-of-crypto-supply>

trasferimento di valore, mentre con il termine di token ci si riferisce ad un oggetto digitale con delle caratteristiche aggiuntive oltre al solo trasferimento di valore, ottenibili grazie all'applicazione di uno smart contract. A loro volta i token possono essere suddivisi in due macrocategorie sulla base della loro modalità di utilizzo: troviamo così gli *utility* token e i *security* token. Gli utility token solitamente vengono emessi da un'azienda per finanziare un progetto e forniscono il diritto di accesso ad un servizio collegato al progetto finanziato (volendo fare un paragone con un altro metodo di finanziamento per le imprese si potrebbe pensare al reward-based crowdfunding)¹⁶; i security token (detti anche equity token) sono assimilabili a delle azioni e quindi sono solitamente collegati ad un asset societario e garantiscono ai possessori dei diritti nei confronti della società emittente, ad esempio potrebbero garantire il diritto ai dividendi (questo metodo di finanziamento presenta diverse analogie con l'equity crowdfunding)¹⁷. Anche per le coin possiamo avere un'ulteriore specializzazione: con il termine *Altcoin* vengono indicate tutte le criptovalute emesse dopo il Bitcoin e con il termine *Stablecoin* ci si riferisce a delle monete che hanno un prezzo fisso che ricalca quello di una valuta fiat, e quindi non sono asset altamente speculativi come invece le altre criptovalute (Chiap et al, 2019). Il prezzo di una stablecoin è ancorato ad un bene fisico ed essa viene spesso usata come tramite per l'acquisto delle altre criptovalute (solitamente si usa convertire la valuta fiat in una stablecoin e si scambia quest'ultima con la criptovaluta desiderata). La stablecoin più utilizzata al momento è *Tether (USDT)*, moneta ancorata al prezzo del dollaro che ha come sottostante il dollaro stesso o un suo equivalente (per ogni Tether emesso deve

¹⁶ Il reward-based crowdfunding è un tipo di finanziamento nel quale le imprese, solitamente start-up nella fase iniziale, richiedono fondi da parte di investitori privati dando in cambio una ricompensa materiale (tipo un prototipo di un prodotto) o in servizi (possibilmente per ricevere anche dei feedback).

¹⁷ Nell'equity crowdfunding la società richiede fondi a finanziatori privati in cambio di partecipazioni nella società.

essere posto a riserva un dollaro). Qualche anno fa sono state mosse pesanti critiche alla stablecoin, accusando l'emittente di non aver veramente depositato quantità di beni tali da equivalere il valore delle monete emesse e di non fornire le adeguate informazioni riguardo la composizione dei suddetti beni, ma Tether ha recentemente divulgato le informazioni riguardanti la composizione del sottostante¹⁸, tranquillizzando gli investitori e tutti coloro che ripongono fede nelle criptovalute, poiché un'eventuale crollo dell'USDT avrebbe potuto minare la fiducia nell'intero sistema dato che, in termini di volume giornaliero, questa moneta è la più scambiata sulle diverse Blockchain¹⁹.

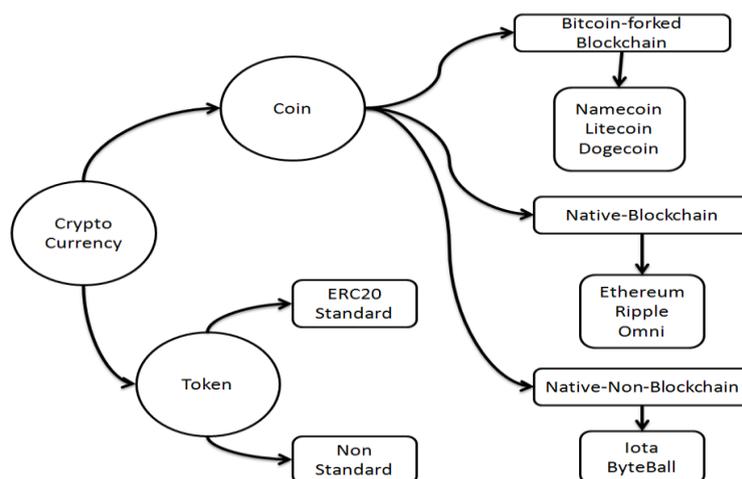


Figura 4 - Coin vs Token. Fonte: packtpub.com

¹⁸ <https://tether.to/en/transparency/#reports>

¹⁹ <https://coinmarketcap.com/currencies/tether/>

1.2.3 BITCOIN

Parlando di criptovalute è doveroso soffermarsi sul bitcoin, la prima criptovaluta creata e tuttora quella con la maggior capitalizzazione, arrivata a superare il trilione di dollari nel corso del 2021²⁰. Il white paper della moneta è stato pubblicato da Satoshi Nakamoto, probabile pseudonimo di un personaggio la cui identità rimane ignota; il paper non è altro che un documento informativo che si pone come obiettivo quello di spiegare al pubblico le caratteristiche e le iniziali applicazioni di un prodotto o di un servizio senza dover rispettare i numerosi vincoli richiesti da documenti informativi fortemente regolamentati. Si pensi ad una richiesta di finanziamento da parte di un'impresa: le informazioni che essa è obbligata a fornire sul progetto sono molto precise e sottoposte a regolamentazioni ferree, soprattutto nel caso di finanziamenti tramite l'emissione di azioni o di prestito dalle banche; per il finanziamento tramite emissione di un token è sufficiente rilasciare il *white paper*, documento che al momento non è soggetto a particolari regolamentazioni (anzi, svolge più una funzione di vendita e marketing) e che rende molto più veloce ed economico il finanziamento dell'impresa a discapito però degli investitori, che risultano maggiormente esposti alle asimmetrie informative e di conseguenza ad eventuali truffe presenti nel mercato.

La politica monetaria del bitcoin prevede l'emissione totale di 21 milioni di monete; il bitcoin è una moneta "minabile", ovvero può essere creata e acquisita tramite il processo minerario. Come abbiamo accennato, i miners competono per la creazione del nuovo blocco e una volta che esso è generato viene riconosciuto al creatore una quantità della moneta digitale come ricompensa; l'ammontare del premio, inizialmente pari a 50 BTC,

²⁰ <https://coinmarketcap.com/currencies/bitcoin/>

viene dimezzato ogni 210000 blocchi, che temporalmente corrispondono a circa quattro anni. Il fenomeno con cui avviene il dimezzamento della ricompensa è chiamato *halving* e l'ultimo al quale abbiamo assistito è avvenuto a maggio 2020 e ha portato la ricompensa per la genesi del blocco a 6,25 BTC dai 12,5 precedenti. Attualmente sono stati emessi circa il 90% del totale dei bitcoin e si stima che circa un 20% delle monete sia stato perduto²¹, nel senso che i proprietari degli indirizzi hanno perso le chiavi di accesso e quindi non possono rientrarne in possesso; di questo passo l'emissione di bitcoin terminerà nel 2140, quando la ricompensa sarà pari a 1 satoshi che è l'unità di misura minima della moneta ed è pari a 10^{-8} BTC (1 bitcoin corrisponde a 100 milioni di satoshi).



Figura 5 - Andamento della capitalizzazione di mercato di bitcoin. Fonte: coinmarketcap.com

L'utilizzo sempre più frequente della valuta digitale e la sua politica monetaria fanno sì che il bitcoin sia una risorsa scarsa e caratterizzata da deflazione (rispetto al numero di

²¹<https://www.ilsole24ore.com/art/i-bitcoin-emessi-sono-90percento-totale-circa-20percento-e-sparito-sempre-AETWwp4>

monete emesse) e questo porta molte persone a considerarlo un bene rifugio, una sorta di oro digitale; in effetti la risorsa virtuale condivide con la materia prima il fatto di essere scarsa e inalterabile, ma, a differenza di questa, il bitcoin ha una volatilità decisamente superiore all'oro (come si può vedere anche dall'andamento altalenante della sua capitalizzazione) e dimostra nell'andamento una certa correlazione con i mercati finanziari e con l'inflazione, caratteristiche opposte a quelle dell'investimento sicuro²². Per capire se effettivamente la moneta potrà essere catalogata come bene rifugio bisognerà vedere come si evolverà la sua correlazione con i mercati e se si ridurrà la sua volatilità avvicinandoci al numero massimo di monete immettibili in circolazione.

Un importante fattore che ha permesso al bitcoin di diventare così popolare è sicuramente la sicurezza intrinseca della sua blockchain. Come abbiamo accennato in precedenza le blockchain non sono tutte uguali, ma si differenziano per diversi aspetti soprattutto sulla base dell'obiettivo che intendono perseguire. Le tre caratteristiche fondamentali della blockchain sono *decentralizzazione*, *sicurezza* e *scalabilità*, ma nella pratica non è possibile perseguire al meglio ognuna delle tre caratteristiche, come viene evidenziato dal trilemma della scalabilità, che afferma che un sistema basato su questa tecnologia può avere al massimo solo due di queste proprietà (Chiap et al, 2019).

²² <https://www.ilsole24ore.com/art/bitcoin-sara-l-oro-digitale-prospettive-e-limiti-ADERWWOB>

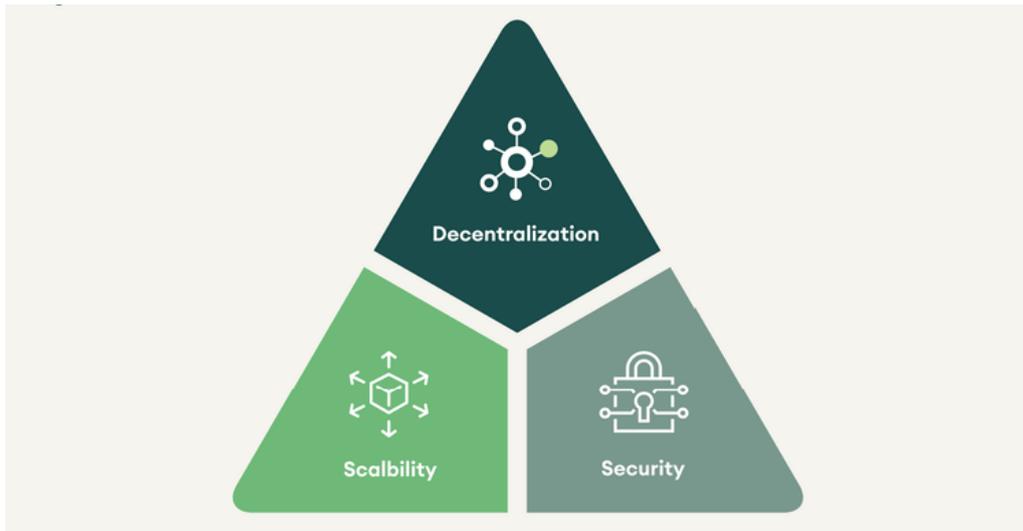


Figura 6 - Trilemma della scalabilità. Fonte: tuttcrypto.it

Nella blockchain Bitcoin si è data molta importanza alla decentralizzazione e alla sicurezza a discapito della scalabilità, infatti, come abbiamo visto, per creare i blocchi bisogna risolvere un problema matematico molto complesso che richiede una potenza di calcolo notevole e lo stesso blocco ha una struttura particolare: al suo interno oltre alle transazioni (presenti in numero limitato dato che il fondatore nel white paper ha deciso di limitare la dimensione massima del blocco a 1MB) vi è un *block header* (intestazione del blocco) che contiene, tra le altre informazioni, un hash di riferimento al blocco precedente e un hash che riassume tutte le transazioni e che, per le proprietà delle funzioni di hash viste in precedenza, rende facilmente individuabile e di conseguenza rifiutabile una modifica della catena.

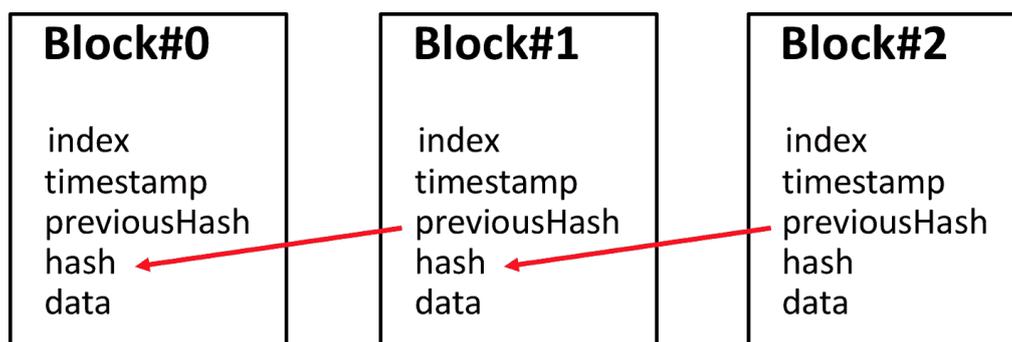


Figura 7 - Collegamento tra i blocchi di una blockchain. Fonte: academy.bit2me.com

Questo meccanismo è quindi particolarmente sicuro e affidabile ma difficilmente scalabile; infatti, all'aumentare delle transazioni, si ha una notevole diminuzione della velocità con le quali vengono processate e un aumento del costo per sostenerle che ricade in capo all'utilizzatore (a fine 2017, ad esempio, le transazioni nei pool in attesa di conferma erano più di 180000)²³. Per tentare di arginare il problema è stata introdotta la *SegWit*, che consiste essenzialmente in una modifica della dimensione del blocco di modo da riuscire a contenere più transazioni, e il *Lighting Network*, un protocollo di pagamento di secondo livello che sostanzialmente consente agli utenti di aprire un canale di pagamento bidirezionale sul quale effettuare transazioni che verranno registrate sulla blockchain solo quando verrà chiuso il canale di comunicazione: questo metodo è molto pratico e consente di velocizzare la rete poiché, se si devono effettuare numerose transazioni con lo stesso utente, dà la possibilità di tenere aperto un canale per il tempo necessario e procedere alla registrazione on-chain delle transazioni nel momento in cui non si ha più la necessità di effettuarne di nuove.

²³<https://it.cointelegraph.com/news/unconfirmed-transactions-on-bitcoin-network-at-highest-level-since-2017>

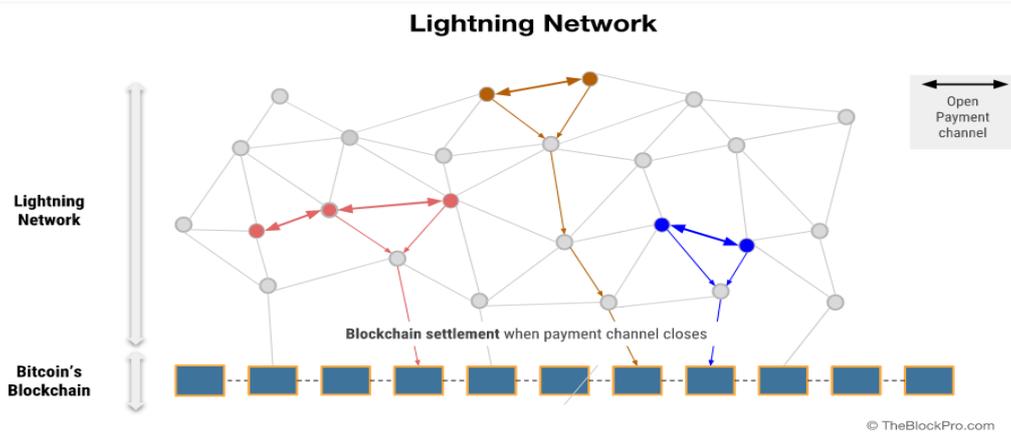


Figura 8 - Il Lightning Network. Fonte: theblockpro.com

Un'altra critica che viene spesso mossa a Bitcoin è quella di non essere “realmente” decentralizzato in quanto, fino a non molto tempo fa, la Cina era responsabile di più dei due terzi del mining globale²⁴ e il 50% dell’hashrate totale era concentrato nelle cinque maggiori mining farm cinesi²⁵; questo scenario è però in evoluzione poiché la Cina ha deciso di porre un veto al mining di criptovalute costringendo molti miners a spostarsi verso paesi in cui il costo dell’energia elettrica è basso. Si è avuta così un’impennata del mining in paesi come il Kazakistan (dove però ultimamente la crescita del prezzo dell’energia sta causando non pochi problemi)²⁶ e il Texas²⁷ (paese nel quale molta energia elettrica prodotta è di natura rinnovabile data l’abbondanza di vento e sole) e gli Stati Uniti sono diventati così lo stato al mondo dove si concentra maggiormente la capacità di mining.

In ultima istanza viene mossa a bitcoin anche una critica per quanto riguarda l’eccessivo consumo di energia necessario per sostenere la blockchain, dovuto al fatto che nel

²⁴ <https://www-statista-com.ezproxy.biblio.polito.it/statistics/1200477/bitcoin-mining-by-country/>

²⁵ <https://www-statista-com.ezproxy.biblio.polito.it/statistics/731416/market-share-of-mining-pools/>

²⁶ <https://www.ilsole24ore.com/art/kazakhstan-protoste-spaventano-miners-criptovalute-AEnwAX6>

²⁷ https://www.repubblica.it/esteri/2021/07/22/news/cina_usa_texas_minatori_miniere_bitcoin_migrazion_e_fuga_bitmain_bit_mining_criptovalute-311328018/

meccanismo di consenso Proof of Work implementato, si compete sulla potenza di calcolo, fattore che richiede una notevole quantità di energia elettrica; ad oggi Bitcoin consuma circa 133 terawattora all'anno, più del fabbisogno di una nazione come la Svezia²⁸, rendendo così le transazioni tutt'altro che green dal punto di vista ambientale: si stima che una sola transazione in bitcoin consumi più energia elettrica di più di un milione di transazioni con una carta VISA²⁹.

È quindi evidente come l'adozione del bitcoin come valuta a corso legale sia al momento di difficile applicazione soprattutto in nazioni di dimensioni elevate, ma, in base a come verrà aggiornata la tecnologia e in base allo scopo ultimo al quale si vorrà arrivare, sono attuabili diversi cambiamenti che, se condivisi dal consenso del network, potrebbero portare a rivoluzionare la blockchain, anche se la rete non sembra voler viaggiare in questa direzione ma sembra, al contrario, apprezzare le criticità del bitcoin che lo rendono più simile ad un bene rifugio nel quale riporre fiducia anche per il futuro.

1.2.4 ETHEREUM

Ethereum nasce da una ICO lanciata nel 2014, durata 42 giorni e alla quale era possibile partecipare solo pagando in bitcoin³⁰. La prima apparizione pubblica di Ethereum la dobbiamo a Vitalik Buterin, scrittore e programmatore russo-canadese nonché appassionato conoscitore di Bitcoin, che nel 2013 decide di scrivere il white paper di quella che è attualmente la blockchain più utilizzata al mondo secondo Bloomberg; la

²⁸<https://lab24.ilsole24ore.com/green-generation/bitcoin-brucia-l-energia-un-intero-paese-ecco-quanto-e-perche-consuma.php#>

²⁹<https://www-statista-com.ezproxy.biblio.polito.it/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/>

³⁰<https://academy.youngplatform.com/criptovalute/ethereum-ico/#5>

versione che conosciamo del white paper è una versione aggiornata rispetto alla prima e viene pubblicata nel 2014.

Rispetto a Bitcoin, Ethereum è un sistema maggiormente complesso che si prefigge obiettivi diversi rispetto alla blockchain pensata da Nakamoto (tanto che spesso ci si riferisce alla blockchain di Bitcoin come Blockchain 1.0 in contrapposizione alla Blockchain 2.0 con la quale si indica quella di Ethereum). Ethereum non vuole essere solo una piattaforma decentralizzata che permetta lo scambio di valore, ma è pensata per essere un supercomputer, distribuito e sempre attivo, in grado di eseguire applicazioni (DApps)³¹ e che permetta agli utenti di relazionarsi tra di loro in modo totalmente automatico attraverso l'uso degli smart contracts (Takashima, 2017). La blockchain è pubblica e, attraverso gli smart contract, può essere programmata ed è quindi adattabile a diversi scenari e scopi; ogni nodo della rete implementa una *Ethereum virtual machine*, una sorta di CPU virtuale dedicata ad eseguire delle istruzioni per la blockchain e sulla quale possono essere eseguite le applicazioni e i contratti. Per essere eseguiti correttamente talvolta i “contratti intelligenti” devono poter reperire informazioni dal mondo esterno e ciò è reso possibile grazie ai cosiddetti *oracoli*, che non sono altro che dei servizi progettati appositamente per la blockchain e che le forniscono i dati provenienti dal mondo esterno per consentire la corretta esecuzione dei contratti che necessitano di informazioni esterne.

³¹ <https://ethereum.org/it/dapps/#what-are-dapps>

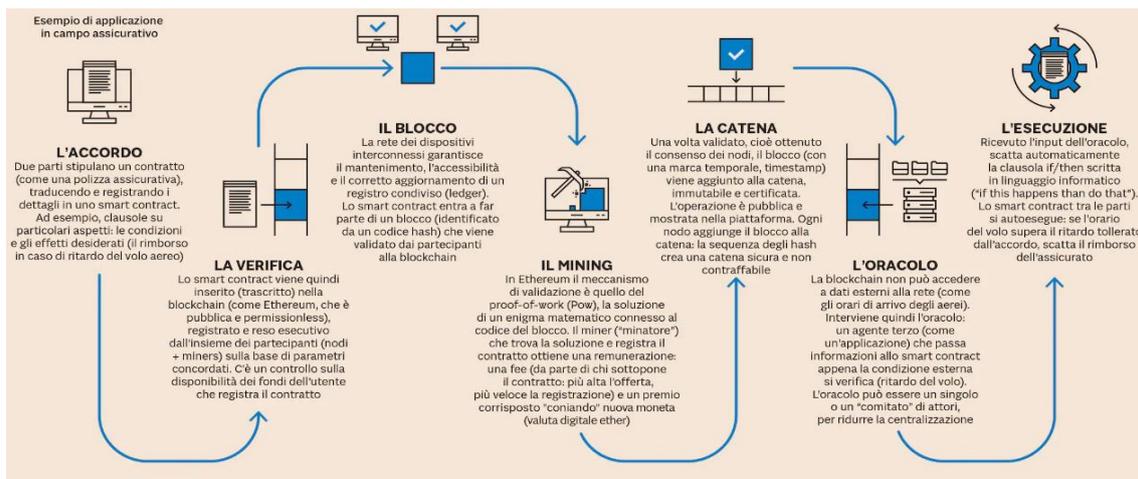


Figura 9 - Esempio dell'esecuzione di uno smart contract. Fonte: ilsole24ore.com

Dal punto di vista tecnologico si capisce subito quanto Ethereum sia rivoluzionario: gli sviluppatori, siano essi utenti privati o aziende, possono creare programmi da eseguire su quello che fondamentalmente si comporta come un supercomputer realizzato come una rete decentralizzata di computer; così facendo si ha il vantaggio di avere a disposizione una potenza di calcolo di molto superiore a quella dei server centralizzati e si guadagna anche in sicurezza, essendo molto più difficile per un malintenzionato mettere offline o effettuare un attacco hacker ad un'applicazione che viene eseguita contemporaneamente su più macchine; inoltre viene data a tutti la possibilità di creare delle applicazioni su tecnologia blockchain senza dover creare la propria blockchain, operazione che risulterebbe molto costosa e complessa dato che richiederebbe, tra le altre cose, anche la presenza di numerosi utenti disposti a mettere a disposizione la loro potenza di calcolo. Come viene usata la potenza di calcolo è un'altra caratteristica differente tra Bitcoin ed Ethereum: nel primo tutta la potenza viene usata per minare le transazioni mentre nel secondo è usata per rendere possibile l'esecuzione di applicazioni e di smart contract (particolarità che, tra l'altro, rende possibile l'emissione di token sulla blockchain).

La possibilità di eseguire applicazioni in modo decentralizzato potrebbe portare ad una rivoluzione dal punto di vista della gestione dei dati, soprattutto se si pensa che al momento i dati personali che vengono condivisi dagli utenti sui social network, sulle app di messaggistica, piuttosto che su programmi di archiviazione in cloud, vengono salvati nei server centrali delle aziende; con lo sviluppo delle applicazioni su blockchain gli utenti tornerebbero in possesso dei loro dati in quanto essi non dovrebbero essere obbligatoriamente condivisi e memorizzati su un server centralizzato e aumenterebbe esponenzialmente la difficoltà di censurare i contenuti dato che non basterebbe semplicemente mettere offline i server dell'azienda da oscurare; d'altro canto non si avrebbe la possibilità di avere un controllo delle informazioni, fatto che potrebbe diventare anche nocivo (si pensi, ad esempio, all'assalto del Congresso USA di inizio 2021, organizzato quasi totalmente su un social network che è poi stato messo offline per evitare il ripetersi di un evento simile)³².

L'utilizzo di smart contract e delle criptovalute ha permesso anche la nascita delle DAO (Decentralized Autonomous Organizations), organizzazioni dove i membri interagiscono tra di loro regolati da un protocollo condiviso e scritto sotto forma di codice di programmazione sulla blockchain; in pratica una DAO può essere equiparata ad una normale azienda ma la governance è regolata da uno smart contract al quale tutti devono sottostare e che definisce le azioni da intraprendere sulla base delle decisioni degli shareholders. Solitamente il sottostante economico della società è in criptovalute e gli eventuali profitti dell'organizzazione vengono distribuiti in criptovalute.

³² <https://www.open.online/2021/01/11/usa-amazon-parler-offline/>

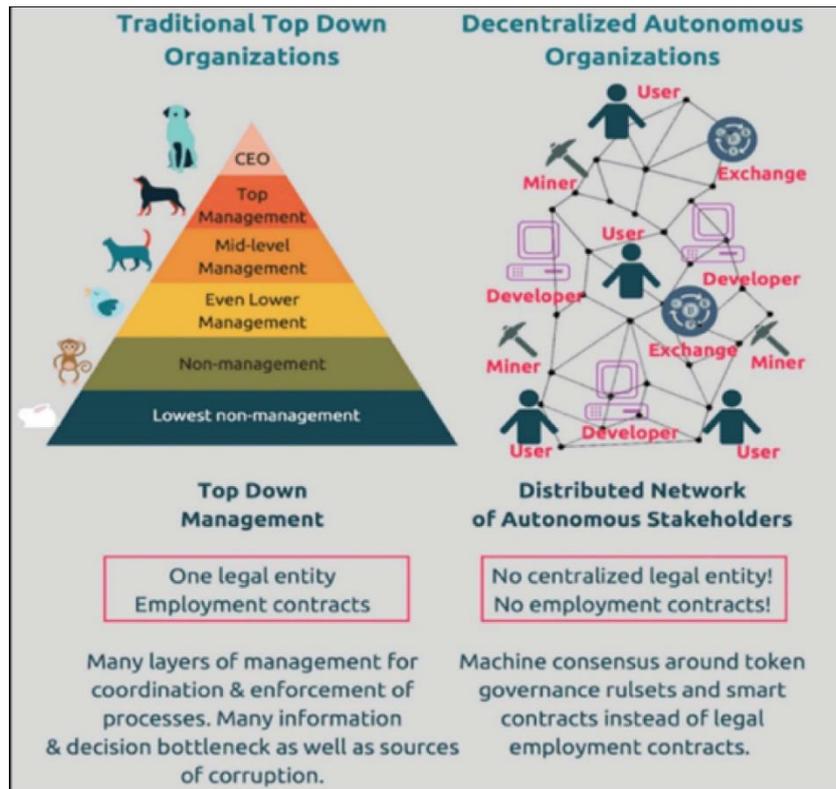


Figura 10 - Differenze tra una normale organizzazione e un'organizzazione decentralizzata.

Fonte: thedailyguardian.com

Un'organizzazione di questo tipo riesce quindi a mantenere la decentralizzazione e l'autonomia in quanto gli shareholders esercitano i propri diritti tramite votazioni che vengono indelebilmente registrate su blockchain e le decisioni vengono prese in autonomia dal codice sulla base delle indicazioni di voto, senza la necessità di tanti documenti e di una struttura gerarchizzata tipica di una normale società.

Come abbiamo visto l'ICO di Ethereum è durata 42 giorni ed è stata una delle più grandi della storia; durante i primi 14 giorni i soggetti interessati all'investimento potevano scambiare un bitcoin con 2000 ether (ether è il nome del token della blockchain di Ethereum), e il tasso di conversione è poi diminuito nei successivi 28 giorni per dare un vantaggio economico agli early adopters. Il meccanismo di consenso di Ethereum è basato

sul Proof of Work con un tempo di creazione del blocco di 10-20 secondi, anche se il network si sta lentamente modificando per adottare un meccanismo Proof of Stake (dove gli utenti dovranno detenere in stake almeno 32 ETH per diventare validatori)³³; inoltre il network ha anche deciso di implementare (a partire dal 2023) lo *sharding*³⁴, un processo attraverso il quale si suddivide orizzontalmente un database per ripartirne il carico e che risulta quindi un ottimo modo per permettere l'espansione mantenendo la decentralizzazione. L'uso combinato del meccanismo Proof of Stake e dello sharding dovrebbero rendere la blockchain migliaia di volte più scalabile rispetto alle prestazioni delle blockchain iniziali (Chiap et al, 2019).

Original Table

CUSTOMER ID	FIRST NAME	LAST NAME	FAVORITE COLOR
1	TAEKO	OHNUKI	BLUE
2	O.V.	WRIGHT	GREEN
3	SELDA	BAGCAN	PURPLE
4	JIM	PEPPER	AUBERGINE

Vertical Partitions

VP1			VP2	
CUSTOMER ID	FIRST NAME	LAST NAME	CUSTOMER ID	FAVORITE COLOR
1	TAEKO	OHNUKI	1	BLUE
2	O.V.	WRIGHT	2	GREEN
3	SELDA	BAGCAN	3	PURPLE
4	JIM	PEPPER	4	AUBERGINE

Horizontal Partitions

HP1				HP2			
CUSTOMER ID	FIRST NAME	LAST NAME	FAVORITE COLOR	CUSTOMER ID	FIRST NAME	LAST NAME	FAVORITE COLOR
1	TAEKO	OHNUKI	BLUE	3	SELDA	BAGCAN	PURPLE
2	O.V.	WRIGHT	GREEN	4	JIM	PEPPER	AUBERGINE

Figura 11 - Esempio di sharding. Fonte: digitalocean.com

Nella blockchain di Ethereum esistono due tipi di account: account normali e account associati ad uno smart contract; entrambi sono collegati ad un indirizzo, ma i secondi solitamente non sono controllati da una persona e contengono al loro interno un

³³ <https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/>

³⁴ <https://ethereum.org/it/upgrades/shard-chains/>

programma che si attiva nel momento in cui si riceve una transazione, mentre gli account normali non presentano differenze sostanziali con un account sulla blockchain di Bitcoin essendo possibile con essi inviare e ricevere transazioni.

La politica monetaria di Ethereum non prevede un numero prestabilito di monete in emissione e ciò è da molti considerato uno svantaggio perché non permette al token proprietario di avere caratteristiche deflattive ed essere quindi paragonato ad un asset che potrebbe diventare un bene rifugio come il bitcoin; tuttavia, ci sono molte discussioni in atto sul network e si pensa che nel futuro si potrebbe limitare o fissare un massimo all'emissione di Ether. Il token può essere suddiviso in wei (1 ETH corrisponde a 10^{18} wei), e questa unità di misura è molto utile quando parliamo di *gas*: con questo termine indichiamo un'unità di misura della quantità di calcolo necessaria a svolgere un'operazione sulla blockchain di Ethereum e ogni transazione è caratterizzata da prezzo del gas e dal limite di gas. Il prezzo del gas indica quanti wei è necessario pagare per un'unità di gas, mentre il limite indica il tetto massimo di gas che può essere consumato per una transazione. Dalla moltiplicazione di questi due fattori si ottiene il costo totale della transazione, che è un'importante fattore nel network poiché al momento, a differenza di Bitcoin, in Ethereum non si ha una dimensione fissa del blocco ma si ragiona in termini di limite del gas di un blocco; questo fattore viene usato per calcolare la remunerazione dei miners e per indicare il limite alla quantità di calcoli inseribili all'interno del blocco da aggiungere alla catena, risultando in questo modo utile a bloccare eventuali attacchi o errori di programmazione nei contratti che potrebbero sovraccaricare il network (Chiap et al, 2019).

Ethereum, come abbiamo detto, è al momento la blockchain più utilizzata per quanto riguarda lo sviluppo di applicazioni decentralizzate e l'utilizzo degli smart contract, ed è

proprio grazie all'uso massiccio di questi contratti che è anche la blockchain di riferimento per le Initial Coin Offerings. Dato che è piuttosto complesso scrivere del codice sicuro, sono stati definiti dei pattern da utilizzare qualora si voglia emettere un token destinato alla distribuzione; gli standard definiscono delle funzionalità all'interno di uno smart contract e il più conosciuto e utilizzato nelle ICOs è l'ERC 20 (acronimo di Ethereum Request for Comment)³⁵, ma ne esistono altri che vengono scelti sulla base delle caratteristiche che si vogliono attribuire (per gli NFT, ad esempio, viene spesso utilizzato lo standard ERC 721). Un token ERC 20 è uno smart contract che segue lo standard ERC 20 e quindi implementa almeno tutte le funzioni definite dal pattern (tra le principali troviamo la funzione che restituisce il numero totale di token in circolazione, la funzione che restituisce il saldo di un account e quella che permette di trasferire una certa quantità di token ad un indirizzo) (Gates, 2017).

1.2.5 PANORAMICA E ANDAMENTO DEL MERCATO

Le criptovalute, fin dalla comparsa del bitcoin, hanno riscosso un buon interesse negli investitori, interesse che è andato a crescere fino ad oggi, dove la tecnologia blockchain si è guadagnata un ruolo importante in alcuni ambiti della nostra società. Questi asset, come abbiamo accennato, sono (per la maggior parte) altamente speculativi e caratterizzati da una volatilità molto elevata: lo stesso bitcoin, che per caratteristiche e apprezzamento viene spesso utilizzato come benchmark dell'intero mercato e viene

³⁵ <https://academy.bit2me.com/it/che-cosa-%C3%A8-erc-20-token/>

percepito come la moneta più affidabile e sicura, ha avuto delle perdite di valore (i cosiddetti drawdown) di oltre l'80% in diversi periodi³⁶.

Fino al 2017, la capitalizzazione di mercato delle criptovalute è rimasta piuttosto limitata (intorno ai 15 miliardi di dollari in aggregato), con il bitcoin che ha mantenuto una capitalizzazione sempre superiore all'85% dell'intero mercato, per poi esplodere negli anni successivi, in concomitanza all'esplosione delle ICOs: nel 2018 la capitalizzazione è passata a valere quasi 800 miliardi in soli pochi mesi³⁷. In concomitanza a questo incremento di valore di mercato, bitcoin ha visto ridursi la sua dominance³⁸, arrivata ad essere di poco superiore al 30% durante il periodo di punta delle ICOs. Tra il 2018 e il 2020 si è poi avuto un periodo di incertezza nel mercato, caratterizzato anche dal fallimento di diversi progetti, e la capitalizzazione totale si è attestata abbastanza stabilmente tra i 200 e i 300 miliardi di dollari.

A fine 2020 il mercato ha ripreso a salire vertiginosamente, arrivando a toccare quasi i 3000 miliardi di dollari di capitalizzazione a fine 2021, salvo poi perdere quasi il 50% del valore nel giro di un paio di mesi (a inizio 2022 la capitalizzazione era di circa 1600 miliardi, con il bitcoin passato dagli oltre 60000\$ a moneta nel periodo di picco, a valere meno di 30000\$ al pezzo), a riprova dell'enorme volatilità di questi strumenti.

³⁶ <https://medium.com/galaxy-digital-research/contextualized-analysis-of-bitcoin-drawdowns-f4717ff8e3be>

³⁷ <https://coinmarketcap.com/charts/>

³⁸ Con il termine dominance si indica la misura della capitalizzazione di mercato di una criptovaluta rispetto alla capitalizzazione di mercato di tutte le restanti criptovalute.

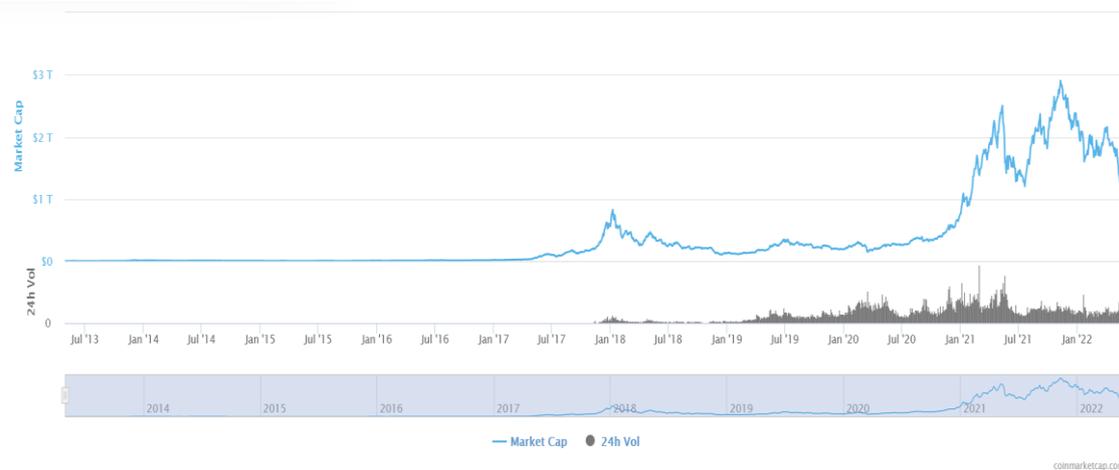


Figura 12 - Andamento della capitalizzazione di mercato delle criptovalute in aggregato. Fonte: coinmarketcap.com

Nel 2022 il mercato è stato molto movimentato e caratterizzato da elevata incertezza, come si può notare nell'immagine sovrastante; a inizio maggio il fallimento della blockchain Terra e il conseguente passaggio del token proprietario LUNA da 90\$ a 0\$, principalmente a causa della stablecoin algoritmica della piattaforma che aveva perso l'equivalenza³⁹ con il dollaro⁴⁰, ha causato panico tra gli investitori provocando un crollo della capitalizzazione dell'intero mercato di circa il 40%.

Al momento, bitcoin risulta ancora la criptovaluta più importante in termini di capitalizzazione di mercato, con una dominanza abbastanza stabile intorno al 40% da ormai più di un anno; ether ha guadagnato progressivamente terreno con il crescere della popolarità e dell'utilizzo della blockchain Ethereum, arrivando a detenere una quota di mercato pari a circa il 20%, e superando addirittura bitcoin per un brevissimo periodo di tempo a inizio 2018. Dopo le due monete di maggior risalto, nella top 5 odierna delle monete a maggior capitalizzazione troviamo due stablecoin, Tether e USD Coin (a

³⁹ <https://investire.biz/articoli/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-cos-il-peg-nella-defi>

⁴⁰ <https://it.cointelegraph.com/news/terra-peg-mechanism-in-doubt-as-ust-crashes-to-67-cents>

conferma dell'importanza delle stablecoin nel mercato) e BNB, il token proprietario di Binance, il più grande exchange al mondo, capitalizzato oltre 50 miliardi di dollari⁴¹ e con una quota di mercato di circa il 4%.



Figura 13 – Evoluzione delle quote di mercato delle varie criptovalute. Fonte: coinmarketcap.com

1.2.6 ULTERIORI CRITICHE E CENNI DI REGOLAMENTAZIONE

Le stesse caratteristiche viste e apprezzate fanno sorgere in capo ad alcuni delle critiche alle criptovalute⁴², in quanto la neutralità e la decentralizzazione possono favorirne l'utilizzo in attività illegali quali il riciclaggio di denaro proveniente da attività illecite, la compravendita di stupefacenti e di armi e il finanziamento al terrorismo; effettivamente gli scambi che avvengono in criptovaluta non sono direttamente collegati ad una persona fisica o giuridica perché gli indirizzi sono delle stringhe alfanumeriche, e ciò contribuisce a facilitare l'anonimato (se l'individuo prende le dovute precauzioni è quasi impossibile

⁴¹ <https://coinmarketcap.com/>

⁴² https://www.huffingtonpost.it/entry/terrorismo-riciclaggio-e-frodi-il-lato-oscuro-dei-bitcoin_it_61dde54be4b04b42ab8647c0/

risalire alla persona all'origine di una transazione). È da notare inoltre che in molti paesi gli operatori che offrono servizi di compravendita e scambio di valute non devono sottostare agli obblighi imposti dalle normative di antiriciclaggio (non in Italia, dove il legislatore si è recentemente adeguato alle direttive europee assoggettando così i “prestatori di servizi relativi all'utilizzo di valuta virtuale” alle disposizioni delle norme atte a contrastare il riciclaggio)⁴³. Di contro però è da sottolineare il fatto che qualsiasi transazione eseguita viene registrata sulla blockchain e lì vi rimane indelebilmente, fattore di non poco conto per chi svolge attività illecite, e che esse sono una piccola parte del totale delle operazioni che avvengono sulla catena.

Negli ultimi anni si è assistito a un forte incremento nell'utilizzo delle criptovalute e ciò ha spinto i paesi che ancora non ne possedevano a dotarsi di specifiche regolamentazioni, soprattutto in materia di antiriciclaggio e di protezione degli investitori. Nei paesi più avanzati si nota la presenza di leggi e regolamentazioni piuttosto permissive da un punto di vista di incentivo allo sviluppo della tecnologia, anche se diverse tra loro⁴⁴; ad esempio, il Giappone si è dotato di una legge regolatoria molto prima degli altri paesi e ciò ha permesso la nascita di diversi exchange regolamentati, situazione simile a quella verificatasi in Svizzera, dove linee guida tempestive hanno ridotto le incertezze legali e permesso a molte attività legate alle criptovalute di emergere. Nel Regno Unito dopo varie misure volte ad aiutare lo sviluppo delle valute virtuali si è deciso di focalizzarsi sulla protezione degli investitori, mentre negli Emirati Arabi Uniti si è decisa di attuare una politica favorevole alle criptovalute attraverso regolamentazioni precise ma non troppo ferree ed eliminando le imposte sui guadagni con le monete digitali (capital gain).

⁴³ https://www.diritto.it/valute-virtuali-e-normativa-antiriciclaggio/#_ftn5

⁴⁴ https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

In controtendenza si è mossa la Cina che di recente ha deciso di bandire gli exchange e il mining sul territorio nazionale, probabilmente vedendo nelle criptovalute una minaccia al controllo centrale che lo stato tenta di imporre sui cittadini (la nazione però, da anni sta studiando l'adozione su larga scala di una moneta digitale di stato, l'e-yuan).

CAPITOLO 2 – LE INITIAL COIN OFFERINGS

In questo capitolo verranno approfondite le dinamiche che spingono un'azienda a cercare fondi tramite l'emissione di token, operazione che prende il nome di *Initial Coin Offering (ICO)* e che negli ultimi anni ha riscosso grande successo. Il nome deriva dalle *Initial Public Offering* o *IPO*, termine con il quale si indica l'emissione di azioni acquistabili dal pubblico da parte di un'azienda fino a quel momento non quotata sul listino nel quale avviene l'offerta.

Le ICOs hanno guadagnato grande popolarità nel 2017 e hanno avuto un vero e proprio boom nel 2018; nel 2017 abbiamo assistito a oltre 500 ICOs che hanno globalmente raccolto oltre 7 miliardi di dollari, valori che hanno superato il migliaio di nuove emissioni per un totale di quasi 20 miliardi di dollari di fondi raccolti nel 2018. Per fare un paragone, nel 2013, anno in cui si è avuta la prima offerta di moneta virtuale, le operazioni di questo tipo erano state solo due e nel 2016 abbiamo assistito a 49 ICOs che hanno portato alla raccolta di 250 milioni di dollari, cifre non paragonabili in termini quantitativi agli anni successivi⁴⁵.

Al momento, il fenomeno delle ICOs risulta fortemente ridimensionato rispetto ai numeri di qualche anno fa, e la maggior parte dei progetti che usano questo metodo di finanziamento risultano molto specifici (spesso riguardano un aspetto caratteristico di una specifica blockchain) e in media richiedono una quantità di fondi inferiore ai progetti degli anni precedenti⁴⁶; ciò è anche dovuto al fatto che il corretto funzionamento e la fiducia degli utenti di una blockchain, per come è strutturata la tecnologia, è direttamente

⁴⁵ https://www.pwc.com/ee/et/publications/pub/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf

⁴⁶ <https://www.icolistingonline.com/>

proporzionale alla grandezza del network del quale essa gode, e ciò rende estremamente difficile la creazione da zero di nuove blockchain in grado di sostituire quelle precedenti, operazione che era invece molto ricercata nel periodo di boom delle ICOs e che richiede una quantità di fondi notevole.

Come riportato anche da PWC nel suo report annuale del 2022, riguardante le operazioni di fusione e acquisizione e ai metodi di finanziamento delle aziende facenti parte del mondo delle criptovalute⁴⁷, si nota sempre più una tendenza tra le aziende a inglobare le concorrenti più piccole, segno di un settore che si sta consolidando: nel 2021 le operazioni di fusione e acquisizione hanno raggiunto il valore di 55 miliardi, contro un miliardo dell'anno precedente, con le compagnie operanti nel settore del trading che si confermano le più attive per quanto riguarda l'operazione.

Per quanto concerne invece la raccolta di fondi equity, gli accordi siglati nel 2021 sono numericamente più del doppio rispetto a quelli del 2020, ma in aggregato sfiorano i 35 miliardi di dollari di raccolta, contro i 4,6 dell'anno precedente, con ancora le compagnie di trading in cima alla lista delle aziende più finanziate. Il 34% dei finanziatori sono venture capitalists e fondi che operano nel mercato delle crypto, seguiti dal 24% apportato dai venture capitalists tradizionali e dagli incubatori⁴⁸.

⁴⁷ <https://www.pwc.com/gx/en/financial-services/pdf/2021-full-year-global-crypto-ma-and-fundraising-report.pdf>

⁴⁸ <https://www.pwc.com/gx/en/financial-services/pdf/2021-full-year-global-crypto-ma-and-fundraising-report.pdf>

2.1 PIATTAFORME E TOKEN

Attualmente esistono numerose piattaforme utilizzabili per l'emissione di un token ed Ethereum è quella più utilizzata⁴⁹, ragione dovuta in gran parte all'enorme network del quale gode la blockchain e alla possibilità di esecuzione di smart contract e di dapps; tra le altre blockchain utilizzate per il processo vi sono da citare Stellar, Neo ed Eos, blockchain concettualmente simili a quella ideata da Vitalik Buterin, ma che faticano a rubare quote di mercato ad Ethereum.

Nell'ultimo periodo stiamo però assistendo ad un'inversione di tendenza rispetto all'utilizzo della blockchain per l'emissione di coin: l'interesse degli investitori sta spingendo sempre più le compagnie (soprattutto quelle che si occupano di servizi finanziari) ad approfondire la conoscenza della tecnologia e a creare strumenti di investimento diversi dalle "comuni" criptovalute, che vengono percepite da molti come un asset altamente speculativo ed enormemente rischioso, considerata anche la regolamentazione non sempre chiara e la scarsa protezione per gli investitori. In quest'ottica stanno guadagnando sempre maggiore importanza i security token, e anche in Italia molte aziende stanno studiando questo campo di applicazione; ad esempio, Cetif Advisory in collaborazione con Reply sta mettendo a punto una piattaforma DLT/blockchain per l'emissione di security token delle principali asset class alternative come Fondi d'Investimento, Real Estate o Private Equity⁵⁰. Questo processo è reso possibile grazie alla popolarità che stanno riscontrando i progetti in via di sviluppo e alla crescente fiducia e comprensione delle persone riguardo alla blockchain: il token non viene più visto come un qualcosa di astratto facente parte di una tecnologia perlopiù

⁴⁹ <https://icobench.com/stats>

⁵⁰ <https://www.reply.com/it/content/si-conclude-con-successo-la-prima-fase-della-sperimentazione-per-l-emissione-e-la-gestione-di-security-token>

sconosciuta, ma viene investigato, in quanto nuova opportunità di investimento, da chi comprende le potenzialità del processo di tokenizzazione, processo che consiste nel creare un asset digitale contenente una serie di informazioni in grado di conferire la proprietà di un bene specifico ad un determinato soggetto, il tutto godendo delle proprietà di una blockchain. Al momento l'utilizzo della tokenizzazione è ancora limitato, ma gode di un potenziale significativo in quanto può essere applicato ad un'infinità di beni ed è in grado di garantire numerosi vantaggi in termini di trasparenza, tracciabilità, efficienza e controllo (vantaggi derivati direttamente dall'utilizzo della tecnologia blockchain), ma anche di migliorare la rapidità delle transazioni e la liquidità del mercato attraverso l'uso di smart contract (operazione che permette anche l'eliminazione di eventuali intermediari). L'uso sempre più intenso della tecnologia e i vantaggi indicati potrebbero fornire la spinta necessaria a dare vita ad una rivoluzione in campo finanziario, settore nel quale l'innovazione gioca da sempre un ruolo fondamentale. Si pensi ad esempio a delle azioni di società di piccole e medie dimensioni: le informazioni sugli azionisti e sulle azioni vengono solitamente gestite autonomamente dalle parti interessate perché l'azienda non è quotata su un mercato, dando spesso adito ad errori ed alimentando asimmetrie informative; attraverso la tokenizzazione si potrebbe superare questo problema consentendo ad aziende ed azionisti di accedere ad un registro condiviso e immutabile (la stessa procedura si ritiene possa in futuro essere sempre più utilizzata dalle aziende per mettere sul mercato le azioni, attuando quella che sarebbe a tutti gli effetti una rivoluzione in campo finanziario)⁵¹, o più semplicemente si potrebbe dare la possibilità anche a piccole aziende di rendere liquidi degli asset in suo possesso senza per

⁵¹ <https://www.blockchain4innovation.it/esperti/tokenizzazione-degli-asset-scenari-e-sfide/>

forza dover passare da procedure gravose in termini di tempi e costi sostenibili solo dalle grandi imprese.

Abbiamo visto come l'interesse si stia spostando sempre più verso l'integrazione della tecnologia blockchain ai campi di applicazione reali, fenomeno recente e attualmente in evoluzione; ciò sta facendo guadagnare ai token sempre maggiore popolarità rispetto al passato. Nel capitolo precedente abbiamo diviso gli asset di nostro interesse presenti sulla blockchain in coin (o token di pagamento), utility token e security token, e questa distinzione sarà utile per distinguere tra le varie operazioni di emissione di token (Momtaz, 2020).

	Utility Tokens	Security Tokens
Essence	A tool for driving human behavior using incentives within a blockchain ecosystem.	An Investment contract that represents legal ownership of a physical or digital asset that has been verified on the blockchain.
Connection Between Token & Company	The token's value doesn't necessarily have a direct connection to the company's value and success.	The token represents true ownership of the company and is directly related to the growth of the company.
Scam Potential	Many scammers found this opportunity to raise money and exit without building the product they promised to develop.	Companies that release security tokens must go through significantly regulatory hurdles. This naturally reduces the potential for scams.
Regulations	There are still significant difficulties for creating true regulations for ICO's.	The company and the investors must meet the strict conditions of the SEC (The Howey Test).

Figura 14 - Utility Tokens vs Security Tokens. Fonte: medium.com

2.2 ICO, IEO E IDO

La dicitura Initial Coin Offering viene usata per indicare qualsiasi operazione di emissione di token su una blockchain, ma, dato che non tutte le emissioni presentano le stesse caratteristiche, si è iniziato a operare delle distinzioni all'interno di questo universo. Inizialmente l'operazione consisteva perlopiù nell'emissione di token di pagamento o di utility token direttamente da parte dell'azienda interessata, ma nell'ultimo anno si è assistito ad un progressivo aumento della gestione dell'emissione di utility token e di coin da parte di exchange e ad un incremento dell'emissione di security token, e si è iniziato a distinguere tra i fenomeni, considerando sia la diversità degli asset, sia la diversa regolamentazione alla quale devono sottostare. Le ICO sono così state in gran parte sostituite dalle IEO e dalle IDO⁵². Le *Initial Exchange Offering* e le *Initial Dex Offering* sono concettualmente quasi identiche alle ICO, ma in esse l'offerta di token al pubblico viene portata avanti da un exchange: l'impresa non si occupa più dell'emissione, che viene invece gestita dall'exchange al quale l'azienda paga una commissione (concettualmente il meccanismo è molto simile a quello di una IPO, operazione che, nella quasi totalità dei casi, prevede che una o più banche in sindacazione tra loro sottoscrivano le azioni della società ad un prezzo scontato per poi occuparsi della collocazione di esse agli investitori, aiutando in molti casi alla stabilizzazione del prezzo dell'azione dopo la quotazione)⁵³. La differenza tra i due processi risiede nel tipo di exchange che gestisce le quotazioni: nell'IEO l'exchange in questione è di tipo centralizzato (es. Binance), mentre nelle IDO ad occuparsi della distribuzione è un exchange decentralizzato; molto spesso

⁵² <https://it.cointelegraph.com/news/ieos-icos-stos-and-now-idos-how-to-raise-funds-for-crypto-in-2019>

⁵³ <https://corporatefinanceinstitute.com/resources/knowledge/deals/overallotment-greenshoe-option-ipo/>

comunque non viene data importanza alla distinzione e si identificano queste operazioni con il termine più generale di Initial Coin Offering.

	Initial Exchange Offering (IEO)	Initial Coin Offering (ICO)
Target	Exchange Users	Everyone
Counter-party	Exchange	Dev Team
Contribution	Exchange Account	Smart Contract
Administrator	Exchange	None
Project Assessment	Done by Exchange	None
Requirements for Launch	Yes	No
Vetting Buyers	KYC / AML	None / Third-parties
Marketing	Exchange & Project	Project only
Liquidity	Higher	Lower
Transparency	Higher	Lower
Protection	Higher	Lower

Figura 15 - Principali differenze tra ICO e IEO. Fonte: medium.com

Dopo aver identificato i metodi per l'emissione di currency e utility token, vi è ancora una distinzione da fare per quanto riguarda i security token; come abbiamo precedentemente detto, i security token sono una rappresentazione digitale di un prodotto di investimento registrata su blockchain, e come tale sono soggetti a delle regolamentazioni più stringenti. Un token può essere definito security token solo nel caso in cui il sottostante sia negoziabile e venga sottoposto a tokenizzazione; ad esempio, delle PMI pensano all'emissione di security token per rendere liquidi i propri asset normalmente illiquidi, ovvero per portare a termine delle operazioni di cartolarizzazione

in modo da riuscire ad accedere più facilmente ai mercati di capitali. Si possono distinguere cinque tipi di security token, di cui due ricoprono un ruolo preponderante: gli *equity token* (equiparabili alle azioni), e i *debt token* (assimilabili a obbligazioni).

Il fenomeno dell'emissione di security token viene definito STO (Security Token Offering) ed è un fenomeno recente ed in forte espansione, iniziato successivamente allo scoppio delle ICOs, che presenta però alcune differenze rilevanti rispetto ad esse; innanzitutto, le STOs sono soggette a regolamentazioni severe e necessitano di livelli elevati di trasparenza e di condivisione delle informazioni, dato che vengono equiparate a dei titoli e quindi ad essi viene applicata la giurisdizione riguardante i titoli, giurisdizione che attualmente in molte nazioni non presenta normative articolate applicabili agli utility token o ai token di pagamento; inoltre, la possibilità di prendere parte alle STOs solitamente non vengono offerte al pubblico ma solo ad investitori accreditati, un po' come accade nelle IPOs, e nella maggior parte dei casi l'emittente è un'azienda o una start-up già sviluppata ed in grado di effettuare le operazioni di divulgazione richieste dal mercato, mentre nelle ICOs si tratta solitamente di start-up in fase di sviluppo (Lambert et al, 2021).

2.3 MECCANISMO DELL'ICO

La prima ICO della storia non è stata quella di Ethereum, della quale abbiamo parlato nel capitolo precedente, bensì è stata lanciata nel 2013 da J. R. Willet per un progetto chiamato Mastercoin⁵⁴ e ha raccolto 600000\$ attraverso la distribuzione di Mastercoin token (veniva richiesto un bitcoin in cambio di 100 Mastercoin token); il progetto venne

⁵⁴ <https://academy.youngplatform.com/cryptoeconomia/ico-storia-cryptovalute/>

successivamente rinominato in Omni ed è tutt'ora ancora attivo, e sostanzialmente consiste in un protocollo di comunicazione basato sulla blockchain Bitcoin. Il token Omni ha raggiunto valori di oltre 100\$ nel 2018, ma al momento il suo prezzo è calato nettamente e si attesta intorno ai 4\$, con una capitalizzazione di mercato di poco superiore al milione di dollari⁵⁵.

Generalmente l'offerta di token da parte di un'azienda segue un procedimento ben definito, che si può raggruppare in tre macro-fasi: una prima fase di divulgazione e di pubblicità del progetto, una seconda fase di offerta dei token e, per concludere, una terza fase nella quale gli investitori ricevono i token richiesti e nella quale il token viene listato. La prima fase può essere suddivisa a sua volta in altri due momenti e riveste un ruolo di fondamentale importanza; nella fase iniziale l'azienda annuncia l'intenzione di portare avanti un determinato progetto, identifica gli investitori target, cercando di suscitare in loro curiosità, e pubblicizza la sua idea il più possibile attraverso tutti gli strumenti in proprio possesso, ovvero attraverso l'utilizzo di campagne di marketing via social network (con l'esplosione del fenomeno sono nati diversi siti che hanno il solo scopo di pubblicizzare ICO per renderle conosciute al pubblico) piuttosto che via mail o tramite la creazione di un blog e l'utilizzo di comunicati stampa⁵⁶; successivamente si passa alla stesura del *white paper*, documento informativo fondamentale per la buona riuscita dell'offerta di monete. Teoricamente il white paper dovrebbe avere carattere informativo riguardo ai rischi ed ai risultati previsti dall'investimento; nella pratica, essendo un documento non regolamentato (al contrario della maggior parte dei documenti informativi degli strumenti finanziari), esso risulta utilizzato principalmente utilizzato come uno

⁵⁵ <https://coinmarketcap.com/it/currencies/omni/>

⁵⁶ <https://cryptonomist.ch/blog/marketing/2020/04/25/strumenti-marketing-blockchain/>

strumento di marketing, di modo da sponsorizzare al meglio l'offerta e da attrarre il maggior numero di finanziatori. Come vedremo nel prossimo paragrafo, le informazioni e il livello di dettaglio del white paper sono elementi essenziali per la riuscita dell'ICO, in quanto si deve trovare il giusto compromesso tra la descrizione delle potenzialità dell'investimento e il livello di dettaglio di descrizione del progetto di modo da avere credibilità agli occhi degli investitori senza esasperarne il contenuto; con la pubblicazione del white paper si conclude la fase di pubblicità del progetto e si passa alla fase di creazione vera e propria dei token. La creazione può avvenire in proprio consultando le linee guida delle piattaforme e scrivendo il codice necessario o ci si può appoggiare a dei consulenti e a degli sviluppatori esperti di blockchain; in ogni caso al momento della creazione si devono definire alcuni parametri necessari al corretto svolgimento della procedura, quali il numero massimo di token vendibili, le valute accettate per il finanziamento (ether e bitcoin sono le più gettonate), il massimo numero di monete vendibili durante l'offerta iniziale (il cosiddetto *hard cap*)⁵⁷, il tempo di genesi di un blocco ed eventualmente il numero massimo di monete acquistabili da un unico soggetto, oltre ad una soglia minima di monete vendibili che se non raggiunta comporta il fallimento e la non prosecuzione dell'ICO (questo aspetto è discrezionale, come accade anche in alcune campagne di crowdfunding, ed è denominato *soft cap*)⁵⁸. Abbiamo detto che la grande maggioranza delle ICO prevede l'emissione sulla blockchain Ethereum e tra essi, più dell'80% dei token emessi sono del tipo ERC20, decisamente lo standard maggiormente adottato al momento. Il processo di una ICO svolta sulla blockchain di Ethereum è un processo rapido e snello: dopo la creazione del token è sufficiente creare un indirizzo che si occuperà di ricevere i fondi dagli investitori e scrivere uno smart

⁵⁷ <https://it.cointelegraph.com/explained/can-bitcoins-hard-cap-of-21-million-be-changed>

⁵⁸ <https://coinmarketcap.com/alexandria/glossary/soft-cap>

contract associato all'indirizzo (utilizzando un linguaggio di programmazione quale Solidity), ed esso si occuperà in automatico della distribuzione dei token ai finanziatori, in base a quanto hanno investito e al cambio tra il token emesso e la criptovaluta accettata come metodo di pagamento. (Catalini et al, 2018) (Howell et al, 2019) (Momtaz, 2020) (Ivashenko et al, 2018).

In accordo con quanto viene sostenuto da Momtaz, spesso assistiamo a delle vere e proprie emissioni di monete preventive alla vera ICO, chiamate appunto pre-ICO; nel campione analizzato dall'autore, quasi un'azienda su due tra quelle intenzionate all'emissione di token ha condotto una pre-ICO. Questa procedura è necessaria soprattutto per le piccole aziende o start-up non particolarmente sviluppate e che non dispongono di buoni flussi di cassa, in quanto consente di iniziare a raccogliere dei fondi che verranno utilizzati per coprire i costi dell'ICO dovuti, ad esempio, alla necessità di pubblicizzazione o all'assunzione di nuovi dipendenti; inoltre, un'operazione di questo tipo permette di estrapolare importanti informazioni dagli investitori riguardo il prezzo da utilizzare durante l'emissione e la previsione della domanda di token, aiutando così la società a decidere correttamente valore e offerta massima di monete (questo meccanismo ricorda il *book building* nelle IPO, metodo attraverso il quale l'emittente decide il prezzo sulla base dell'interesse manifestato dagli investitori nella fase di presentazione dell'emissione di azioni)⁵⁹.

Una volta creati i token si ha la vera e propria ICO, nella quale i soggetti interessati inviano denaro in cambio dei token; ogni ICO è caratterizzata da una durata variabile che può essere stabilita a priori ma anche non definita in quanto si prevede di continuare

⁵⁹ <https://www.borsaitaliana.it/borsa/glossario/bookbuilding.html>

l'emissione fino a quando non siano state vendute tutte le monete (per esempio l'ICO di BAT, acronimo di Basic Attention Token, token usato principalmente come merce di scambio tra creatori in un determinato ambiente di sviluppo, è durata circa 30 secondi⁶⁰, mentre l'ICO di EOS ha avuto la durata di quasi un anno⁶¹).

Come abbiamo detto, le ICO hanno avuto un boom nel 2018, per poi subire un ridimensionamento; attualmente le emissioni di criptovalute avvengono principalmente tramite l'offerta diretta da parte degli exchange attraverso IEO, ma, in accordo con la letteratura, l'essere listato da un exchange è sempre stato un punto cruciale nella sopravvivenza di un token, in quanto l'essere listato garantisce al token di poter essere liberamente scambiato tra tutti gli utenti attivi provvedendo a rendere il mercato molto più liquido; al contrario, qualora il token venga delistato dall'exchange ciò sancisce la fine del progetto dato che viene meno il poter commerciare la moneta liberamente e facilmente. Il fallimento del progetto è molto comune tra i progetti finanziati tramite ICO, a febbraio 2018 il 46% delle ICO svoltesi nel 2017 erano considerate fallite. (Momtaz, 2019).

2.4 IL WHITE PAPER

Buona parte delle informazioni necessarie agli investitori e sulle quali essi si basano per decidere della bontà o meno del progetto, sono rappresentate nel white paper che, come abbiamo accennato, è il documento fondamentale di una ICO, in quanto l'emissione di criptovalute non è soggetta alle regolamentazioni tipiche delle emissioni di titoli che

⁶⁰ <https://academy.bit2me.com/it/que-es-basic-attention-token-bat/>

⁶¹ <https://it.cointelegraph.com/news/eos-about-to-secure-a-record-4-bln-in-year-long-ico>

richiedono di produrre un'elevata quantità di documenti informativi molto specifici. Questo non è del tutto corretto per quanto riguarda le emissioni di security token che sono soggette a regolamentazioni più severe ed articolate anche qualora non conferiscano diritti di voto o dividendi; per gli utility token e i crypto token il documento è invece fondamentale, in quanto il mercato è caratterizzato da elevatissime asimmetrie informative e risulta estremamente difficile per un investitore privato capire e scegliere i progetti migliori: ci troviamo di fronte ad un mercato in continua evoluzione, caratterizzato da decentralizzazione e lacune nelle regolamentazioni e nel quale spesso esperti auto-nominati producono ratings non richiesti, con contributi monetari da parte delle aziende valutate non noti agli investitori. Un mercato di questo tipo è caratterizzato da seri problemi di informazione e dal rischio di un fallimento e si avvicina caratteristicamente ad un mercato Over The Counter (Floryask, 2022).

Il white paper ha quindi una doppia funzione esplicativa e di marketing e nonostante venga ritenuto essenziale per lo svolgimento di una ICO, legalmente non è obbligatorio e viene quindi emesso volontariamente dagli sviluppatori. Per quanto riguarda il lato marketing, oltre al paper, un fattore importantissimo di pubblicità per le ICO sono i social network (su tutti Twitter, Reddit e Telegram), nei quali gli appassionati si confrontano sulla base delle informazioni che hanno ricevuto e la discussione che si crea sull'argomento aumenta la visibilità del progetto e può aiutare a chiarirne alcuni aspetti, offrendo un ottimo effetto di segnalazione (Schuckes et al. 2020). Il white paper si presenta come una guida al progetto, più o meno articolata, e tipicamente include informazioni sull'obiettivo finale, sulle milestone essenziali da raggiungere, sui tempi previsti per lo sviluppo e per il raggiungimento delle milestone chiave e sulla composizione del team. Ci troviamo quindi davanti ad un documento che vuole ricalcare

il prospetto informativo di una IPO, includendo i tratti tipici di esso come il rendiconto finanziario o il business plan, anche se queste informazioni risultano difficili da valutare per un progetto su tecnologia blockchain. Nonostante questo, le informazioni necessitano di essere le più credibili possibile e gli emittenti hanno interesse che ciò sia così poiché il documento è la più importante fonte di informazioni per gli investitori e il punto di partenza per la SEC⁶² per eseguire l'*Howey test*, un test che determina se l'asset abbia le caratteristiche per essere equiparato ad un titolo e quindi se debba ricadere nella regolamentazione dei titoli⁶³.

HOWEY TEST FOR "INVESTMENT CONTRACT"

- **Investment of money**
- Includes an investment of goods and services. *Int'l Bhd. of Teamsters v. Daniel*, 439 U.S. 551,560 n.12 (1979)
- **In a "common enterprise"**
- Either horizontal commonality (where the investors' fortunes are interwoven) or vertical commonality (where there is a direct correlation between the success or failure of the promoter's efforts and the success or failure of the investment). *SEC v. Eurobond Exch., Ltd.*, 13F.3d 1334, 1339 (9th Cir. 1993)
- **With an "expectation of profits"**
- "Capital appreciation" and "participation in earnings" are examples, but a fixed rate of return also counts. *SEC v. Edwards*, 540 U.S. 389 (2004)
- **"Solely on the efforts of others"**

Figura 16 - Howey Test. Fonte: medium.com

Il white paper attraverso le informazioni diffuse fornisce agli investitori la segnalazione riguardo la bontà del progetto: dei white papers che forniscono alto contenuto di informazioni sono in grado di abbassare le asimmetrie informative e vengono visti di buon occhio dagli investitori, perché offrono un effetto di segnalazione sulla veridicità

⁶² Security and Exchange Commission, è l'ente federale statunitense preposto alla vigilanza della borsa, l'equivalente statunitense della Consob italiana.

⁶³ <https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>

del progetto, e perché molto difficilmente l'emittente di un progetto di scarsa qualità sarà in grado di generare un documento con un'elevata mole di informazioni specifiche; di contro, dei documenti ad alto contenuto informativo sono più difficili da produrre e molto più costosi, in quanto rivelare determinate informazioni sul progetto potrebbe essere controproducente perché esse diventerebbero fruibili anche dai concorrenti, nonostante abbiano un peso rilevante per gli investitori. È importante quindi capire (se si ha un buon progetto che potrebbe godere di un white paper ad alto contenuto informativo) il trade-off tra necessità di divulgazione e segretezza, di modo da spiegare abbastanza nel dettaglio il progetto agli investitori per far sì che essi si interessino e lo valutino positivamente ma senza rischiare di diffondere informazioni non conosciute e utilizzabili dai competitors (Floryask, 2022).

2.5 FATTORI DI SUCCESSO DI UNA ICO

La letteratura riguardo le ICOs sta continuando ad arricchirsi perché l'argomento è relativamente recente, e in un breve lasso di tempo ha raggiunto una dimensione e ha suscitato un interesse tali da convincere studiosi e ricercatori a dedicarsi all'argomento. Tra i lavori sviluppati, hanno una notevole importanza quelli che indagano i fattori di successo di questo metodo di finanziamento; in accordo con i lavori analizzati, i dati vengono inizialmente estrapolati da uno dei siti che si occupano di aggregazione degli stessi e di fornire statistiche delle diverse ICO (tra i più importanti troviamo icobench.com, icorating.com, icoalert.com, icotracker.net e icodrops.com) e successivamente vengono proposte dagli autori delle variabili da analizzare rispetto a quelle in loro possesso per trovare eventuali correlazioni. Per fare ciò, spesso vengono

usate delle funzioni di regressione non lineare come la logit o la probit⁶⁴, modelli nei quali la variabile dipendente (termine con il quale si indica la variabile da analizzare) viene trattata per semplificazione come una variabile che può assumere un range di valori limitato tra 0 e 1 e, tramite un programma di supporto al calcolo statistico come Stata, vengono fatte variare le variabili indipendenti (ovvero quelle conosciute dai ricercatori) per trovare eventuali correlazioni tra esse e la variabile dipendente, utilizzando il metodo della massima verosimiglianza degli stimatori per il calcolo dei coefficienti di correlazione.

In accordo con la letteratura, i fattori che influenzano il successo di una ICO sono molteplici; una ricerca rilevante da questo punto di vista è stata portata avanti da Campino, in un paper nel quale l'autore insieme al suo gruppo di ricerca, partendo dai risultati già presenti e portate alla luce da altri studi meno recenti, evidenzia i fattori di nostro interesse. Innanzitutto si pone l'accento sulle asimmetrie informative che permeano i progetti blockchain, tipiche dei mercati caratterizzati da alta intensità tecnologica, mercati nei quali, oltre ad un white paper tecnico contenente una buona quantità di informazioni, hanno un ottimo effetto di segnalazione la presenza di diritti di proprietà intellettuale quali i brevetti e un codice sorgente di ottima qualità, considerato che la grande maggioranza dei progetti blockchain necessita di un elevato livello di programmazione (spesso, per attuire le asimmetrie informative, gli sviluppatori del progetto decidono di pubblicare una parte o tutto il codice sorgente utilizzato, di modo da dare la possibilità di valutare a fondo il progetto a coloro che ne possiedano le competenze necessarie) (Campino et al, 2022) (Fisch, 2019).

⁶⁴ <https://www.econometrics-with-r.org/11-2-palr.html>

Oltre agli effetti di segnalazione che hanno il compito di ridurre le asimmetrie informative, si rilevano altri fattori di successo, ma prima di esaminarli si deve chiarire cosa si intenda per successo di una ICO: la letteratura non concorda su un'unica variabile in grado da sola di definire la buona riuscita del progetto o della campagna (tra l'altro è da sottolineare che nonostante normalmente non si faccia la distinzione, quando parliamo di "successo di una ICO" si intende la buona riuscita della campagna, in quanto il progetto potrebbe successivamente fallire per diversi motivi nonostante il finanziamento sia andato a buon fine), ma vengono definite più misure che, qualora si verificano, possono far considerare l'ICO di successo; tra esse, quelle che comunemente vengono indicate dalla letteratura sono il raggiungimento del soft cap o dell'hard cap e il fatto che dopo l'emissione il token riesca ad essere scambiato su un mercato secondario (ovvero che venga listato su un exchange che renda più liquido il mercato del token). Per quanto riguarda l'essere scambiato su un mercato secondario, questo fattore viene considerato una discriminante del successo in quanto viene considerato un elemento essenziale alla buona riuscita del progetto, senza il quale il token, una volta in mano ai finanziatori, avrebbe un valore molto basso; il raggiungimento o meno del soft cap e dell'hard cap invece vengono considerate all'unanimità misure di successo, in quanto una ICO che raggiunga il minimo importo necessario per iniziare lo sviluppo del progetto o che venga finanziata per l'intero importo richiesto viene unanimemente considerata di successo. In generale, il capitale raccolto durante una richiesta di finanziamento è la variabile preponderante per valutare la riuscita della campagna, anche se questa misura in realtà non è in grado di darci informazioni utili a valutare il progetto in sé (Ahmad et al., 2020) (Roosenboom et al., 2020).

Dopo questa dovuta precisazione, passiamo ad analizzare le variabili che influenzano il successo di una ICO. Quando si creano dei modelli regressivi per effettuare un'analisi econometrica si decide la variabile dipendente da utilizzare; nel caso di nostro interesse le variabili dipendenti sono le variabili trattate poco sopra, che si utilizzano per misurare il successo della campagna di finanziamento. Sono variabili binarie, e per verificare se le conclusioni proposte sono rilevanti, si dovrebbe costruire un modello econometrico per ogni variabile dipendente, contenente ogni volta le stesse variabili indipendenti, in modo da verificare se i risultati ottenuti nei diversi modelli sono tra loro consistenti e quindi poterne trarre delle conclusioni che siano statisticamente significative. Le variabili indipendenti sono molto numerose, e nel modello di nostro interesse possono essere raggruppate in quattro gruppi differenti: variabili di progetto (correlate alle caratteristiche stesse del progetto), variabili della campagna (collegate alle caratteristiche della campagna ICO), variabili dei social network (collegate all'utilizzo dei social durante la campagna) e variabili del team (correlate alle caratteristiche del nostro capitale umano). Tra le variabili indipendenti ricopre un ruolo fondamentale, come detto precedentemente, il whitepaper, i cui dettagli tecnici e la quantità crescente di informazioni riguardanti il sono correlati positivamente con il successo della campagna; anche la divulgazione della composizione del team influisce positivamente sulla raccolta ed è particolarmente importante quando la squadra è composta da un elevato numero di membri, anch'esso fattore importante in una ICO. Il prezzo del token risulta una variabile rilevante, in quanto un prezzo elevato viene percepito dagli investitori come un segnale di buona qualità del progetto, mentre token a basso prezzo sono maggiormente correlati a truffe. Il mercato delle ICO è correlato anche con il mercato delle criptovalute: i modelli confermano che un prezzo alto del bitcoin tende a sfavorire la buona riuscita della campagna, mentre un

alto prezzo di ether favorisce il successo della raccolta di fondi. Anche l'utilizzo di Twitter ricorrente durante la campagna è un fattore molto importante per puntare al successo, sia perché riduce le asimmetrie informative, sia perché tiene informati i potenziali investitori sullo sviluppo della stessa e del progetto (Campino et al, 2022).

Oltre agli elementi appena elencati, caratteristici di ogni progetto e influenzabili dal comportamento degli sviluppatori, troviamo dei fattori che possono influire nel successo di una ICO che non dipendono direttamente da come venga svolta la campagna, dalle caratteristiche del progetto o dal comportamento dei creatori, ma solo dalla nazione dove l'offerta di monete ha luogo. Come vedremo in un paragrafo successivo, le ICO non sono un metodo di finanziamento utilizzato globalmente in maniera uniforme, ma anzi sono tipiche di alcuni paesi, i quali sviluppano la quasi totalità dei progetti su blockchain, nonostante le criptovalute abbiano riscosso un forte interesse da parte degli investitori in buona parte del mondo. In accordo con le ricerche eseguite da (Ahmad et al., 2020), scopriamo, senza sorprenderci, che l'attività nel campo dell'emissione di token è fortemente correlata allo sviluppo finanziario del paese, che, in accordo con la letteratura, è a sua volta correlato con lo sviluppo economico e tecnologico della nazione. Dal punto di vista legislativo, non si trovano risultati statisticamente significativi che indichino un maggiore sviluppo del mercato delle ICO nei paesi con una legislazione che pone le sue radici nel common law rispetto a quelli che la pongono nel civil law (anche se i primi solitamente presentano un mercato più sviluppato perché garantiscono una maggiore protezione per gli investitori), ma si trovano forti segnali, confermati anche dal punto di vista statistico, tra lo sviluppo legislativo in materia di emissione di token e le ICO: esse avvengono maggiormente nei paesi in cui vi è in materia una regolamentazione legale

definita e dettagliata perché ciò favorisce lo sviluppo del mercato delle criptovalute dato che gli investitori e le aziende stesse sono maggiormente tutelati.

In ultimo, nella letteratura si è cercato se ci potessero essere anche dei fattori culturali in grado di influenzare il successo di una ICO; i risultati in questo senso non sono stati entusiasmanti, perché nei modelli econometrici presentati la maggioranza degli indici collegati a fattori culturali, utilizzati nel modello come variabili indipendenti, non sono risultati statisticamente significativi. Gli unici che hanno avuto rilevanza statistica sono l'indice di mascolinità (MAS⁶⁵), che misura in che grado nella società sono importanti i valori tipici della mascolinità, quali, ad esempio, l'assertività, la competitività e il successo e l'indice di prevenzione dell'incertezza (UAI⁶⁶), che indica la tolleranza della società all'incertezza e all'ambiguità. Un alto valore dell'indice MAS sottintende un tipo di società in cui i valori maschilini sono particolarmente importanti (non ha a che vedere con la parità di genere, ma solo con i valori che le persone reputano maggiormente significativi in quella determinata società), mentre un elevato valore dell'indice UAI indica una società in cui le persone percepiscono negativamente l'incertezza e quindi tendono a prendere decisioni meno rischiose e non sono particolarmente avvezze al cambiamento. Le ricerche suggeriscono che nelle società con un alto UAI le ICOs falliscono più facilmente (ciò è dovuto all'avversità al rischio delle persone), mentre nelle società con un elevato MAS le offerte di token hanno maggiore probabilità di successo, soprattutto per quanto riguarda il raggiungimento dell'hard cap (Ahmad et al., 2020).

⁶⁵ https://psychology.fandom.com/wiki/Masculinity_index

⁶⁶ <https://www.cqfluency.com/cqpedia/uncertainty-avoidance-index/>

Dopo aver analizzato qualche evidenza statistica, per concludere possiamo dire che non esiste una ricetta vincente da seguire, ma, in accordo anche con quanto sostenuto da Deloitte nel report “ICOs – The new IPOs?”⁶⁷, i fattori chiave di successo sono:

- ❖ La complementarità tra il business che si vuole sviluppare e la ICO, in quanto il progetto dovrebbe essere direttamente collegato alla blockchain e difficilmente sostituibile da una differente tecnologia;
- ❖ Costruire un team su misura per il progetto e con un’elevata preparazione in materia, fattore che viene reputato di grande interesse da parte degli investitori;
- ❖ Informare correttamente gli investitori, tramite un white paper il più tecnico e preciso possibile, definendo delle scadenze fattibili da rispettare e interagendo continuamente con il pubblico tramite blog e social;
- ❖ Proteggere i diritti degli investitori, importante soprattutto nelle prime fasi di vita del progetto e si può perseguire, ad esempio, dando incentivi agli *early investors* o mettendo i fondi raccolti in un wallet multi-signature per incrementare notevolmente la trasparenza;
- ❖ Considerare una piattaforma ICO per il lancio, in quanto la piattaforma assiste l’azienda in tutte le fasi e aumenta da subito la liquidità dell’investimento;
- ❖ Scegliere una nazione che presenti una regolamentazione favorevole.

2.6 SIMILITUDINI CON ALTRI METODI DI FINANZIAMENTO

In questo paragrafo cercheremo di fare un confronto tra le ICOs e gli altri metodi di finanziamento maggiormente utilizzati dalle aziende per richiedere fondi, e si tenterà di

⁶⁷ <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/ICOs-the-new-IPOs.pdf>

capire cosa spinga un imprenditore a scegliere un metodo di finanziamento innovativo come l'ICO piuttosto che una delle metodologie già affermatesi e consolidate nel tempo.

Negli anni sono state portate avanti numerose ricerche sulla finanza imprenditoriale che hanno tentato di spiegare tramite modelli matematici ed empiricamente come le imprese e le startup possano finanziarsi e quale metodo di finanziamento sia preferibile; se inizialmente i metodi per finanziarsi erano limitati, le opportunità si sono ampiamente allargate e ha quindi assunto un ruolo chiave capire le implicazioni di ogni metodologia di raccolta di fondi per scegliere quella più adatta al proprio progetto.

Di fondamentale importanza per i nostri ragionamenti è la conoscenza de “la teoria dell'ordine di scelta” sviluppata da Myers e Majluf nel 1984; questa teoria sostiene che le scelte di un'azienda sul come finanziarsi vengano prese nell'ottica di diminuire il costo del capitale associato alla fonte di finanziamento. In accordo con la teoria, le aziende non sono indifferenti rispetto a che fonte utilizzare per sostenere economicamente i loro progetti e, mediamente, la scelta ricadrebbe in primis su fonti di finanziamento interne, poi su un finanziamento a debito ed infine all'equity; questo perché asimmetrie informative e azzardo morale rendono il debito e l'equity più costosi per l'impresa rispetto al finanziamento tramite il flusso di cassa che riesce a generare. Il comportamento descritto dalla teoria è un comportamento “medio”, per cui non è detto che tutte le aziende attuino una scelta di questo tipo, soprattutto se le aziende in questione sono startup attive in settori altamente tecnologici, e non tiene adeguatamente conto dell'imprenditore, che, sempre nel caso di aziende di nuova costituzione, assume un ruolo di rilevanza fondamentale nell'influenzare le decisioni di sviluppo di un progetto e di finanziamento.

Tra i metodi di finanziamento maggiormente conosciuti e utilizzati, le ICOs presentano similitudini principalmente con le IPOs e con il crowdfunding. Altre tipologie di raccolta di fondi molto sfruttate dagli imprenditori come il venture capital o i business angels presentano meno tratti in comune con l'offerta di token, in quanto i venture capitalists sono degli investitori professionali che investono principalmente nell'equity delle compagnie, sono cioè dei professionisti che possono lavorare per conto dell'azienda che li ha assunti oppure essere indipendenti, e tipicamente investono grandi quantità di denaro in più tranches applicando contratti complessi, offrendo all'azienda finanziata servizi di supporto allo sviluppo del business con il fine ultimo di portare la società alla quotazione in borsa e quindi poter monetizzare l'investimento iniziale; i business angels invece sono individui con un elevato patrimonio personale, che investono principalmente in start-up non ancora sviluppatesi, applicano dei contratti non troppo complessi e non sempre inseguono come unico obiettivo quello di monetizzare l'investimento, ma potrebbero essere guidati non solo da motivazioni economiche ma anche filantropiche; molto spesso i business angels si riuniscono in gruppi per poter investire in più aziende e spartirsi il rischio e sempre per tale ragione è comune trovare società nelle quali co-investono business angles e venture capitalists.

Quando si parla di somiglianze tra metodi di finanziamento, possiamo notare analogie riguardo le caratteristiche dell'azienda, degli investitori e del patto che viene stretto tra finanziatori e finanziati. Passando ad analizzare le somiglianze tra le ICOs e gli altri metodi di finanziamento, si pensa subito alle IPOs, soprattutto per la similitudine a livello nominativo; l'offerta di azioni al pubblico in realtà, non condivide molte caratteristiche con l'offerta di monete, ma solo alcune di rilevante importanza: tra i tratti in comune si trova l'apertura all'investimento a tutti i tipi di investitori, ovvero la possibilità per un

vasto pubblico di partecipare alla raccolta, e l'elevata liquidità dell'investimento una volta che si è conclusa la distribuzione (in realtà, come abbiamo visto, questo non è sicuro per tutte le ICO perché non è detto che il token emesso venga listato); inoltre, lo strumento in emissione nelle due operazioni è molto differente, a meno che non si prendano in considerazione le sole STO che emettono security token. Le caratteristiche dell'azienda invece, sono molto differenti: solitamente chi vuole portare avanti un'ICO è un'azienda giovane oppure un'azienda in via di sviluppo che intende finanziare un progetto in ambito blockchain attraverso la raccolta di fondi (anche se un'azienda a qualsiasi grado di sviluppo può scegliere questo metodo), mentre chi decide di portare avanti un'IPO è un'azienda sviluppata e con solide basi, in grado di sostenere i costi elevati dell'operazione e che abbia intenzione ricevere una quantità molto alta di fondi (l'IPO maggiore di sempre⁶⁸ è quella della società Saudi Aramco del 2019, che ha raccolto quasi 30 miliardi di dollari se teniamo conto anche dell'opzione greenshoe⁶⁹). Anche dal punto di vista normativo le due operazioni differiscono fortemente dato che il prospetto per l'IPO è un documento fortemente regolamentato e l'intera operazione ha un grado di regolamentazione e complicatezza decisamente elevata, al contrario di cosa accade in una ICO che vede nel whitepaper (formalmente nemmeno obbligatorio) il documento informativo principale (Momtaz, 2020).

Prima di analizzare le somiglianze con il crowdfunding è necessario fare una precisazione su questo metodo di finanziamento, in quanto è una metodologia che viene applicata in diverse forme ed è quindi piuttosto importante avere presente i tipi di crowdfunding che vengono utilizzati maggiormente. Vengono definiti quattro tipi di crowdfunding:

⁶⁸ <https://www.firstonline.info/aramco-e-non-solo-le-10-ipo-piu-grandi-di-sempre-ce-unitaliana/>

⁶⁹ <https://www.borsaitaliana.it/notizie/sotto-la-lente/lagreenshoe.htm>

donation-based, lending-based, reward-based ed *equity-based*⁷⁰. I primi due tipi non presentano particolari punti in comune con le ICOs, in quanto il *donation-based* crowdfunding è un metodo di finanziamento principalmente per investitori con intenzioni filantropiche e il *lending-based* ha le sembianze di un'obbligazione o di un prestito, in quanto l'azienda chiede dei fondi alla folla con la promessa di restituzione del capitale più gli interessi (solitamente gli interessi sono più bassi rispetto a quelli che la società pagherebbe chiedendo un prestito alla banca). Di maggior interesse per lo scopo di questo elaborato sono invece le altre due tipologie; l'*equity* crowdfunding conferisce ai finanziatori dei diritti sui beni dell'azienda poiché investono nel capitale diventando soci, mentre nel *reward-based* i finanziatori ricevono un prodotto (molto spesso un prototipo di ciò che l'azienda intenderà sviluppare in futuro); dal punto di vista dello strumento in emissione è facile trovare analogie tra questo tipo di crowdfunding e le ICOs che prevedano l'emissione di utility token, mentre l'*equity-based* presenta maggiori analogie con le STOs. Il crowdfunding è uno strumento utilizzato principalmente dalle start-up ed è pensato per poter raggiungere un pubblico vasto: ciò ha un'importanza rilevante soprattutto nel crowdfunding a ricompensa, dove per l'azienda solitamente è fondamentale avere dei feedback sulla percezione che hanno gli investitori riguardo al prototipo di prodotto così da usarli per analisi di mercato, mentre ricopre un ruolo meno importante nell'*equity* crowdfunding, dove solitamente a partecipare con una quota d'investimento consistente sono degli imprenditori, e spesso l'operazione viene sponsorizzata e portata avanti da dei portali che si occupano quasi integralmente della campagna di marketing dell'azienda e della raccolta dell'investimento dal pubblico. Solitamente tramite il crowdfunding non vengono raccolte cifre enormi (principalmente

⁷⁰ <https://www.consob.it/web/investor-education/crowdfunding>

si punta ad una cifra nell'ordine del centinaio di migliaia di euro e raramente si arriva ad un milione), mentre le ICOs da questo punto di vista sono più variegate, partendo da raccolte molto limitate (poche migliaia di Euro), fino ad arrivare a dei miliardi per le operazioni maggiori, ed anche dal punto di vista normativo i due metodi di finanziamento presentano analogie poiché entrambi hanno un grado di regolamentazione non particolarmente elevato e quindi non necessitano di forme particolari di divulgazione delle informazioni (anche se, come abbiamo detto, maggiori informazioni fornite vengono viste dagli investitori di buon occhio), e non presentano elevati costi di transazione come nel caso delle IPO (Momtaz, 2020). In ultimo, si può notare una differenza nella liquidità dell'investimento (soprattutto in caso di IEO e IDO, nelle quali il token viene emesso direttamente su un exchange), in quanto gli importi investiti in un'azienda tramite crowdfunding sono difficilmente monetizzabili (in caso di equity crowdfunding per poter ottenere un'uscita la società dovrebbe essere acquisita da un'altra società oppure procedere alla quotazione su una borsa valori), poiché le aziende sono di recente costituzione e, oltre all'elevato tasso di fallimento che caratterizza le start-up, necessitano di periodi di tempo piuttosto elevati prima di risultare appetibili per l'acquisto da parte di una concorrente o di riuscire ad arrivare alla quotazione su un listino. Questo aspetto non è da sottovalutare, perché chi investe con il crowdfunding deve essere a conoscenza del fatto che, anche nella migliore delle ipotesi, monetizzare l'investimento richiede diversi anni (per questo motivo, in diverse nazioni tra cui l'Italia, che si è precocemente dotata di un'accurata regolamentazione in materia, il crowdfunding viene sostenuto da politiche di incentivi fiscali per gli investitori, di modo che chi voglia

investire in aziende di recente costituzione abbia un ritorno economico tangibile anche nel breve termine)⁷¹.

	Initial Coin Offerings	Reward Crowdfunding	Equity Crowdfunding	Venture Capital	Initial Public Offerings
Panel A: Start-up or Firm Characteristics					
Funding stage	Theoretically all stages	Before seed stage (prototype)	Early stage	Balanced-stage	After later stage
Issuance	Utility tokens, cryptocurrencies, or security tokens	Product (vouchers)	Equity-like instruments	Equity shares	Equity shares
Panel B: Investor Characteristics					
Investors	All types	Early adopters	Angel investors	Limited partners	Public
Motivation	Financial and non-financial	Financial and non-financial	Financial and non-financial	Financial	Financial
Panel C: Deal Characteristics					
Investment amounts	>\$100k	\$1k—\$150k	\$100k—\$2m	\$500k—\$10m	>\$10m
Transaction costs	Low	Low	Low	Medium	High
Information basis	Whitepaper	Project description	Business plan and pitch deck	Business plan and pitch deck	IPO prospectus
Degree of regulation	Low	Low	Low	Medium	High
Panel D: Post-Deal Characteristics					
Liquidity	High (if listed)	Low	Low	Low	High
Voting rights	Security tokens: yes; utility tokens and cryptocurrencies: no	No	No	Yes	Yes
Exit options	ICO, open market	IPO, acquisition	IPO, acquisition	IPO, acquisition	Open market

<https://doi.org/10.1371/journal.pone.0233018.t001>

Figura 17 - Differenze tra i metodi di finanziamento. Fonte: Momtaz, 2020.

Avendo dato un rapido sguardo alle classiche modalità di finanziamento in confronto alla più innovativa emissione di token, possiamo spiegare il perché questa nuova modalità abbia in poco tempo raggiunto una notevole popolarità. Innanzitutto, le ICOs sono operazioni versatili, ogni azienda più o meno sviluppata potrebbe decidere di effettuare un'emissione di questo tipo, mentre i metodi di finanziamento tradizionali sono complementari tra loro e tipici di determinati periodi di vita dell'azienda (crowdfunding per startup, venture capital per aziende che si stanno affermando e IPO per aziende di successo che possano facilmente scalare qualora riescano a reperire una grande quantità di fondi). Anche dal punto di vista degli investitori le ICOs presentano dei vantaggi

⁷¹https://www.crowdfundme.it/wpcontent/uploads/2021/04/CFM_Taxcoach_guida_agevolazioni_fiscali_Startup_PMI_2021.pdf

poiché, per come sono strutturate, possono prendervi parte tutti i tipi di investitori, mentre i metodi tradizionali anche da questo punto di vista sono pensati per investitori specifici e necessitano di un'elevata conoscenza del mercato e delle operazioni di finanziamento; inoltre gli investitori di ICOs operano in un mercato caratterizzato da una buona liquidità, caratteristica difficilmente riscontrabile negli altri metodi se non nell'emissione azionaria.

Per le startup però, il vantaggio migliore deriva dal fatto che le ICOs sono più veloci, meno problematiche e molto meno costose degli altri metodi di finanziamento e vengono spesso menzionate come uno dei metodi più efficienti per finanziare delle iniziative imprenditoriali (Schuckes et al. 2020); questo perché i costi di transazione sono quasi nulli, così come la regolamentazione obbligatoria (anche se negli ultimi anni molte nazioni si sono attivate per dotarsi di apposite leggi), che risulta paragonabile a quella di un'operazione di crowdfunding, nonostante tramite l'ICO si possano raccogliere anche capitali ingenti tipici di VC e IPO, che però sono operazioni soggette a costi di transazioni molto elevati e fortemente regolamentate (e in molti casi inefficienti, si pensi al caso di underpricing nelle quotazioni azionarie).

2.7 LE MAGGIORI ICOS DELLA STORIA

In questo paragrafo verranno brevemente descritte alcuni delle ICOs di maggior successo della storia in termini di capitale raccolto, con una breve spiegazione dei progetti che hanno contribuito a renderle così profittevoli.

Come è stato detto, le ICOs hanno vissuto un vero e proprio boom nel 2017, boom che ha raggiunto il suo apice nel 2018, anno che ha visto il numero delle emissioni aumentare notevolmente, passando da circa un migliaio a più di duemila, a fronte però di un non

eguale aumento dell'importo raccolto sia in termini assoluti che in termini relativi, passando da una media di quasi 25 milioni di dollari ad ICO, per un totale di 10 miliardi di dollari raccolti nel 2017, ad una media inferiore ai 12 milioni di dollari ad ICO per un totale di quasi 12 miliardi di dollari nel 2018⁷². A pesare notevolmente su questa statistica è però la più grande ICO mai avvenuta in termini di capitale investito, che ha raccolto 4,2 miliardi di dollari nell'arco di quasi un anno a partire dal 26 giugno 2017, quella di EOS, che ha venduto un miliardo di utility token omonimi alla piattaforma⁷³.

#	Name	Total raised amount (USD mn) ¹⁾	End of offering (month)	Focus	Industry	Country
1	EOS ²⁾	4'100	06/2018	Blockchain infrastructure for decentralized apps	BC infrastructure	 Cayman Islands
2	TELEGRAM	1'700	03/2018	Tokens to enhance messenger ecosystem	Social media	 British Virgin Islands
3	BITFINEX	1'000	05/2019	Tokens for fee discounts in the iFinex ecosystem	FinTech	 Hong Kong
4	TATATU	575	06/2018	Social entertainment on the Blockchain	Entertainment	 Cayman Islands
5	DRAGON	320	03/2018	Decentralized currency for casinos	Gambling	 British Virgin Islands
6	HUOBI TOKEN	300	02/2018	Token/ Coin for South Korean crypto exchange	FinTech	 Singapore
7	HDAC	258	12/2017	IOT platform backed by Hyundai BS&C	Internet of things	 Switzerland
8	FILECOIN	257	09/2017	Decentralized market for data storage	Data storage	 USA
9	TEZOS	232	07/2017	Blockchain infrastructure for decentralized apps	BC infrastructure	 Switzerland
10	KINESIS NEW	194	09/2019	Yield-bearing digital currency based on gold & silver	FinTech	 Cayman Islands
11	SIRIN LABS	158	12/2017	Secure open source consumer electronics	Consumer electronics	 Switzerland
12	BANCOR	153	06/2017	Enabling direct conversion between tokens	FinTech	 Switzerland
13	BANKERA	151	03/2018	Banking for the Blockchain era	FinTech	 Lithuania
14	POLKADOT	145	10/2017	Interoperability protocol across multiple Blockchains	BC infrastructure	 Switzerland
15	GCBIB	143	01/2019	Multi-asset digital wallet	FinTech	 United Arab Emirates

Figura 18 - Le maggiori ICOs della storia. Fonte: pwc.com

EOS è una piattaforma blockchain per lo sviluppo di applicazioni decentralizzate, con la possibilità e lo scopo di fornire agli utenti anche servizi di cloud storage e di server hosting⁷⁴; è stata sviluppata da una società denominata Block One e concettualmente è molto simile ad Ethereum e fonda i suoi principi sulla personalizzazione, sull'efficienza e sulla sicurezza⁷⁵, volendo differenziarsi dalla blockchain pensata da Buterin proprio in

⁷²<https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate>

⁷³ <https://icodrops.com/eos/>

⁷⁴ <https://www.criptoaluta.it/eos>

⁷⁵ <https://eos.io/>

termini di velocità e scalabilità. Per fare ciò, nella blockchain di Eos si utilizza un meccanismo di consenso denominato Delegated Proof of Stake (DPoS), un'evoluzione dell'algoritmo Proof of Stake descritto nel primo capitolo, che permette alla rete di disporre di un sistema di transazione molto efficiente, in grado di confermare una transazione in 0,25 secondi e di dare la certezza di irreversibilità della transazione in solo un secondo⁷⁶. Nonostante queste migliorie, EOS non ha ancora raggiunto un utilizzo su scala globale e attualmente il token ha un prezzo vicino ai 2\$, dopo aver toccato dei picchi di quasi 20\$ durante il periodo di ICO⁷⁷; questa straordinaria performance dell'operazione non è passata inosservata, tanto che una nuova ricerca sostiene che l'offerta iniziale di token EOS, che è stata richiesta dai finanziatori in grandi quantità fin da subito, sia stata manipolata tramite operazioni di wash trading effettuate da una ventina di account⁷⁸. La pratica del wash trading, considerata illegale nei classici exchange ma di difficile controllo nei crypto exchange, consiste sostanzialmente nell'effettuare un grande numero di buy e sell order al fine creare un volume fittizio e dare l'impressione che il bene in oggetto sia molto ricercato, aumentandone così il valore; se questa notizia non venisse smentita, il successo dell'ICO di EOS ne risulterebbe ridimensionata, nonostante rimanga una raccolta di fondi dai numeri stratosferici.

La seconda maggior ICO in termini di importo raccolto è stata lanciata da Telegram, l'ormai famoso social network fondato dai due fratelli russi Pavel e Nikolai Durov, nell'ambito del progetto denominato Telegram Open Network (TON), progetto che si preponeva l'obiettivo di creare una blockchain per lo sviluppo di applicazioni decentralizzate e per processare i pagamenti, promettendo una scalabilità tale da

⁷⁶ <https://academy.bit2me.com/it/que-es-eos-criptomonedas/>

⁷⁷ <https://coinmarketcap.com/currencies/eos/>

⁷⁸ <https://invezz.com/it/notizie/2021/09/03/21-account-pompato-eos-ico-attraverso-wash-trading/>

raggiungere le milioni di transazioni al secondo e poter così competere con le società di gestione dei pagamenti leader del mercato (Visa e Mastercard su tutte). L'ICO ha raccolto circa 1,7 miliardi di dollari tra investitori istituzionali e non, emettendo un utility token denominato Gram⁷⁹; tuttavia, poco dopo la conclusione della distribuzione del token, la SEC ha annunciato che la vendita effettuata costituiva un'offerta illecita di token, in quanto l'organismo di controllo statunitense considerava il Gram assimilabile ad un titolo azionario e i fondatori avevano svolto l'ICO senza rispettare le dovute regolamentazioni stabilite dalla SEC⁸⁰ per l'offerta di security token. L'organismo di controllo americano ha vinto la causa e ha quindi vietato la distribuzione di token Gram, non senza polemiche da parte dei fratelli Durov, obbligando inoltre i fondatori del progetto al risarcimento degli investitori per una cifra vicina ai 1,2 miliardi di dollari⁸¹. La compagnia ha deciso così di abbandonare il progetto, anche se recentemente Telegram si è di nuovo avvicinata alla tecnologia blockchain sostenendo lo sviluppo di The Open Network, un progetto simile a quello voluto inizialmente e dotato della propria criptovaluta, il Toncoin. Attualmente il Toncoin ha una capitalizzazione di circa 2 miliardi di dollari e la singola moneta vale circa 2\$⁸².

Dato l'apprezzamento a livello globale e il successo raggiunto dalla blockchain di Ethereum, sono nate sempre più blockchain con un progetto simile ad essa, o comunque aventi l'intento di creare una piattaforma globale per applicazioni decentralizzate, gestione di pagamenti e smart contract, facilmente scalabile di modo da poter essere utilizzata a livello globale; nonostante ciò, Ethereum rimane la piattaforma di gran lunga

⁷⁹ <https://decrypt.co/53950/the-10-biggest-icos-heres-where-the-money-went>

⁸⁰ <https://it.cointelegraph.com/news/breaking-us-sec-deems-17-billion-telegram-offering-illegal-orders-halt>

⁸¹ <https://it.cointelegraph.com/news/breaking-telegram-abandons-telegram-open-network-and-gram-tokens>

⁸² <https://coinmarketcap.com/it/currencies/toncoin/>

dominante per quanto riguarda le ICO e anche per lo sviluppo di applicazioni decentralizzate (NEO e Stellar, blockchain sulle quali è possibile portare avanti un'emissione di token e che durante il boom risultavano tra le più utilizzate dopo Ethereum avevano quote inferiori all'1%)⁸³. Tra le blockchain con questo obiettivo, oltre a quelle già citate in precedenza in questo paragrafo, Tezos, che si differenzia soprattutto per avere una governance "aperta" nella quale ogni partecipante può intervenire nelle decisioni⁸⁴, ha avuto un buon successo durante l'ICO, che ha portato il progetto a raccogliere poco più di 230 milioni di dollari nel luglio 2017, salvo poi dover restituire 25 milioni agli investitori essendo l'azienda stata accusata di aver emesso security token senza rispettare tutte le dovute regolamentazioni in materia⁸⁵. Tezos è quindi una blockchain open source che usa il Proof of Stake come algoritmo di consenso; il token nativo, denominato come la piattaforma e con ticker XTZ, ha tuttora una buona rilevanza a livello globale, essendo tra le migliori 50 monete per quanto riguarda la capitalizzazione di mercato che attualmente supera i 2 miliardi di dollari⁸⁶.

Un'altra ICO di dimensioni rilevanti e concettualmente interessante, dato il rilievo che ha acquisito il settore, è la ICO di Bitfinex, uno degli exchange centralizzati più importanti al mondo con oltre 2 miliardi di dollari di volume di trading giornaliero e avente listati 180 crypto token per un totale di 456 coppie di scambio⁸⁷. L'offerta iniziale è avvenuta tra il 4 e il 12 maggio 2019, e ha complessivamente raccolto un miliardo di dollari attraverso l'emissione di un miliardo di utility token denominati LEO, con l'obiettivo ultimo di sviluppare un'applicazione che renda il trading a portata di tutti, istantaneo e

⁸³<https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate>

⁸⁴<https://www.criptovalute24.com/tezos/>

⁸⁵<https://decrypt.co/40413/tezos-agrees-to-pay-25-million-in-damages-to-investors>

⁸⁶<https://coinmarketcap.com/it/currencies/tezos/>

⁸⁷<https://www.coingecko.com/en/exchanges>

senza commissioni; il token, come illustrato nel whitepaper⁸⁸, sarebbe al centro dell'ecosistema e permetterebbe agli utenti di avere benefici da progetti e prodotti futuri. Il token è stato apprezzato dagli investitori che hanno in questo modo investito nel progetto dell'exchange e hanno contribuito a farlo raggiungere la fama di cui gode tuttora, nonostante l'exchange abbia vissuto situazioni complicate, come un attacco hacker nel 2016 che portò i truffatori a trasferire su un account 120000 bitcoin, bitcoin recuperati (stranamente) a inizio 2022 quando si è riusciti a risalire agli artefici del furto⁸⁹. La credibilità dell'exchange ne ha risentito positivamente e ciò ha influenzato l'andamento del token LEO, il quale, nonostante stesse già ben performando rispetto al mercato, ha registrato un'impennata del prezzo dopo l'annuncio del recupero dei fondi. Attualmente LEO ha una capitalizzazione di mercato di oltre cinque miliardi di dollari, caratteristica che lo rende una delle criptovalute più importanti al mondo⁹⁰.

Abbiamo più volte detto quanto le ICO siano operazioni permeate da forti asimmetrie informative e azzardo morale e quanto sia facile per gli investitori imbattersi in truffe; ovviamente le truffe sono più comuni nei progetti piccoli e poco conosciuti, ma non mancano le eccezioni. Tra esse si può citare Dragon Coin, un'ICO lanciata da una società con sede a Macau nell'apice del boom delle offerte iniziali di monete nel marzo 2018, e che detiene la palma di quinta ICO più grande della storia. La Dragon Inc. disse di voler portare avanti questa ICO con l'obbiettivo di creare un sistema di pagamento per i casinò dell'asia orientale, e quindi il token Dragon Coin sarebbe stato una sorta di token per il gioco d'azzardo; l'operazione riscosse un ottimo successo tra gli investitori istituzionali

⁸⁸ <https://www.bitfinex.com/wp-2019-05.pdf>

⁸⁹ <https://it.cointelegraph.com/news/bitfinex-hack-recovery-spurs-crypto-community-responses>

⁹⁰ <https://coinmarketcap.com/currencies/unus-sed-leo/>

e non, riuscendo a raccogliere 320 milioni di dollari⁹¹. Tramite l'ICO l'azienda prometteva una rivoluzione nel mondo dei casinò, ma ben presto si scoprì che uno dei maggiori sostenitori del progetto era un gangster di Macau noto alle forze dell'ordine e che le partnership sponsorizzate e utilizzate per accrescere la credibilità dell'operazione erano fittizie, e, nonostante le smentite della società cinese, l'autorità thailandese contro i crimini (CSD) iniziò ad indagare. Gli investitori, momentaneamente ignari delle indagini, iniziarono a preoccuparsi quando videro non rispettate le promesse fatte in fase di marketing della campagna (soprattutto per quanto riguardava la costruzione di un casinò galleggiante da centinaia di milioni di dollari) e, nel giro di breve tempo, l'autorità thailandese arrestò delle persone vicine all'ICO con l'accusa di truffa⁹². Nel frattempo, il token riuscì ad essere quotato su un exchange, ma senza raggiungere buoni risultati, finendo poi per sparire dalla circolazione perché il progetto venne comunemente considerato fallito.

2.8 COLLOCAZIONE GEOGRAFICA

Le ICO non hanno avuto una diffusione uniforme a livello globale, ma anzi sono state molto concentrate in alcune nazioni e quasi passate inosservate in altre, con Stati Uniti, Singapore, Regno Unito e Russia in testa alle statistiche di emissione a livello quantitativo; a livello di importo aggregato raccolto si aggiungono a questa lista le Isole Vergini Britanniche e la Svizzera⁹³, nazioni nelle quali sono in vigore politiche fiscali particolarmente favorevoli alle aziende. Come abbiamo detto a inizio capitolo,

⁹¹ <https://decrypt.co/53950/the-10-biggest-icos-heres-where-the-money-went>

⁹² <https://fullycrypto.com/dragon-coin-the-floating-casino-ico-that-stole-24-million>

⁹³ <https://icobench.com/stats>

recentemente le aziende hanno spostato l'interesse maggiormente sull'emissione di security token, operazione che tecnicamente è molto simile ad una ICO ma che emette una versione digitale di un prodotto di investimento; essendo le STO simili alle ICO condividono con esse gran parte dei fattori di successo, anche se spesso ricadono nelle regolamentazioni dei titoli, meglio definite in ogni stato.

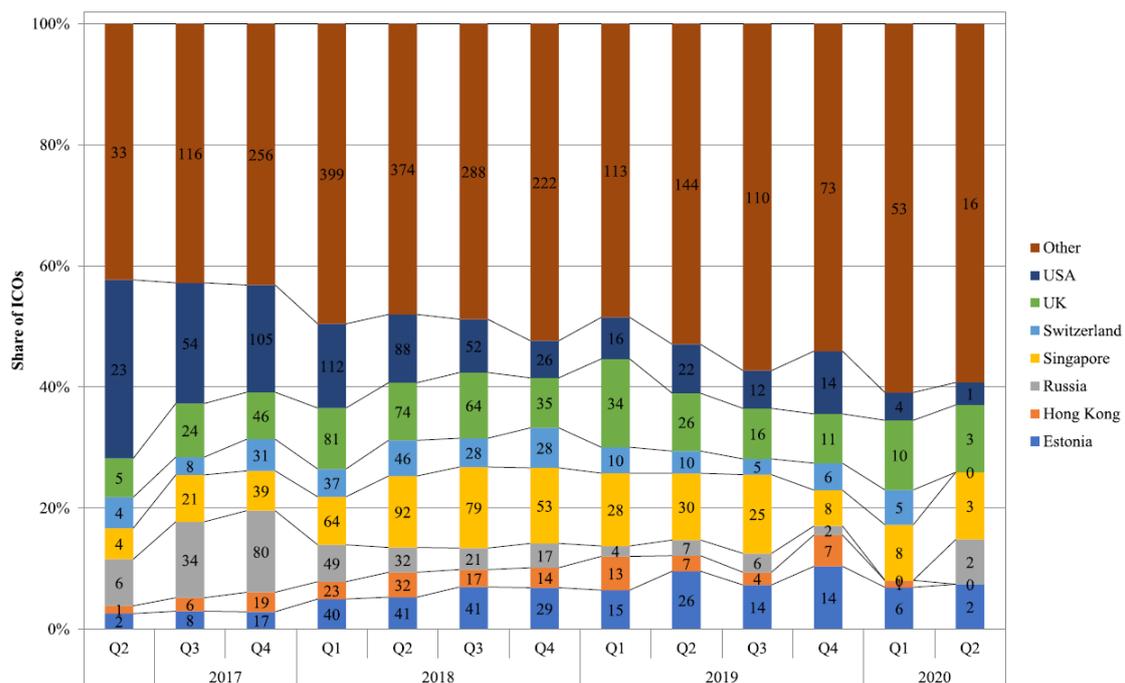


Figura 19 - Numero di ICOs nei maggiori stati. Fonte: Bellavitis et al, 2021.

Nella nostra analisi dei fattori di successo ci siamo soffermati maggiormente sulle parti tecniche del progetto che lo potrebbero rendere vincente rispetto ad un progetto concorrente, senza indagare approfonditamente la dispersione geografica delle ICO dovuta allo sviluppo dello stato. Huang e Vismara nel 2019, ci forniscono un grosso aiuto per comprendere le ragioni della collocazione geografica delle ICO, poiché hanno tentato di analizzare i fattori di dispersione geografica, notando che esse non erano globalmente diffuse allo stesso modo; per fare ciò hanno sviluppato un modello di

regressione lineare utilizzando come variabile dipendente il numero di ICOs verificatesi nella nazione e come variabili indipendenti quattro diverse variabili: in primis, una variabile riguardante un indice di sviluppo finanziario del paese, con particolare riguardo allo sviluppo bancario, allo sviluppo del mercato dell'equity e alla diffusione del Venture Capital e del Private Equity; la seconda variabile riguarda un indice sullo sviluppo del settore delle telecomunicazioni in termini di conoscenza, infrastrutture e intensità di utilizzo; la terza variabile riguarda la regolamentazione delle ICO: è una variabile *dummy* (può assumere solo i valori 0 e 1) che viene settata a 1 nelle nazioni che presentano regolamentazioni aperte o liberali verso le criptovalute e a 0 negli stati che le hanno bandite o che non si sono ancora dotati di nessun tipo di regolamentazione.

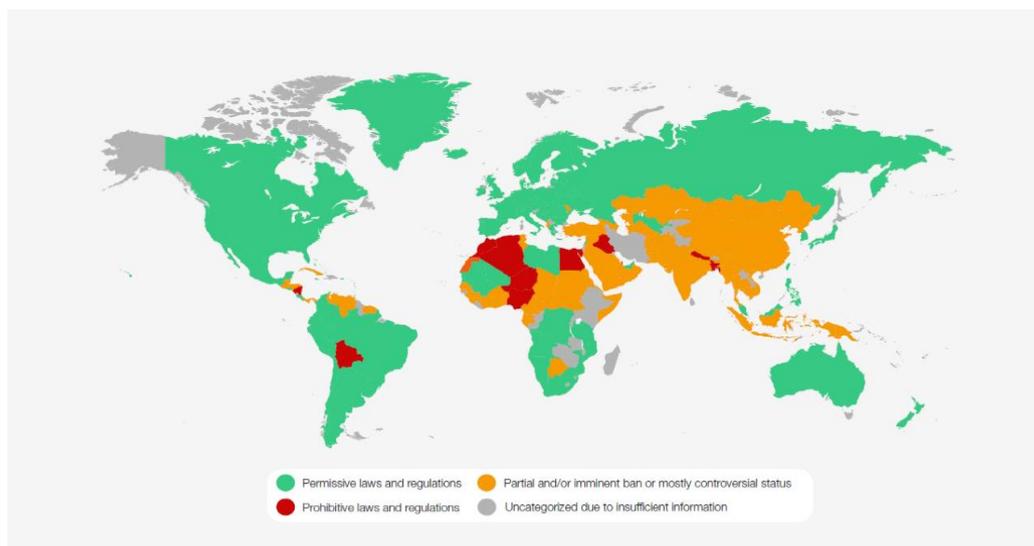


Figura 20 - Regolamentazione delle criptovalute nel mondo. Fonte: World Economic Forum.

L'ultima variabile mira ad indagare l'importanza delle piattaforme online per la raccolta di fondi, con particolare interesse alle piattaforme di crowdfunding, che, come abbiamo detto, sono operazioni che presentano numerose analogie con le ICOs. Oltre a queste quattro variabili principali è presente una variabile di controllo che racchiude delle

variabili in grado di influenzare le raccolte di fondi, come il PIL pro capite, il livello e la densità di popolazione e la percentuale di persone avente educazione universitaria.

$$\begin{aligned} \text{No.of ICOs} = & \alpha + \beta_1 \times \text{Financial Development Index} \\ & + \beta_2 \times \text{ICT Market Development} \\ & + \beta_3 \times \text{ICO Regulation} \\ & + \beta_4 \times \text{Crowdfunding Platforms} \\ & + \gamma \times \text{Controls} + \varepsilon \end{aligned}$$

Figura 21 - Equazione modello di regressione lineare. Fonte: Huang et al, 2020.

Per lo sviluppo del modello è stato usato un campione di poco inferiore alle 1000 ICOs e si è notato che in sole cinque nazioni avviene oltre il 50% delle operazioni di emissione di token; con l'eccezione della Russia, tutte le maggiori nazioni per numero di ICOs presentano performance migliori in praticamente tutte le variabili analizzate, sia in quelle principali che in quelle di controllo. In particolare, questi stati hanno in comune un mercato delle telecomunicazioni sviluppato e un indice dello sviluppo finanziario elevato, oltre ad avere una regolamentazione ben definita e diverse piattaforme online che si occupano di crowdfunding.

Le ipotesi sviluppate dagli autori vengono successivamente messe in discussione rispetto alle normative fiscali in vigore nei paesi, ma anche aggiungendo questi parametri i risultati ottenuti precedentemente rimangono significativi; dai test effettuati risulta non trascurabile anche la variabile rappresentante il carico fiscale delle nazioni, dato che appaiono evidenze statistiche sul fatto che le ICOs siano attratte da migliori condizioni in termini di tassazione.

La nazione nella quale avvengono la maggior parte delle ICOs sono gli Stati Uniti, seguiti da Singapore, Russia, Regno Unito, Estonia e Svizzera, anche se spesso le società

emittenti hanno sede in una nazione differente da quella in cui avviene l'emissione di token; in generale, in accordo con i dati forniti da ICObench, l'America settentrionale è il continente più attivo per quanto riguarda questo tipo di operazioni, mentre l'America meridionale e l'Africa sono i meno attivi e ricoprono un ruolo marginale. In Asia, la Cina giocava un ruolo fondamentale nel panorama delle criptovalute, ma i limiti imposti dalle regolamentazioni hanno fatto crollare la popolarità di questo strumento. Per quanto riguarda l'Europa lo scenario è molto vasto, in quanto sono presenti alcune delle nazioni con il mercato delle ICOs tra i più sviluppati (Regno Unito e Svizzera su tutte, ma anche Germania e Paesi Bassi presentano un discreto numero di operazioni) assieme ad alcune nazioni che, nonostante abbiano dei parametri che sembrano favorevoli ad uno sviluppo della tecnologia, non si sono avvicinate a questo mondo, come ad esempio i paesi nordici (complice probabilmente una pressione fiscale molto elevata in capo alle aziende).

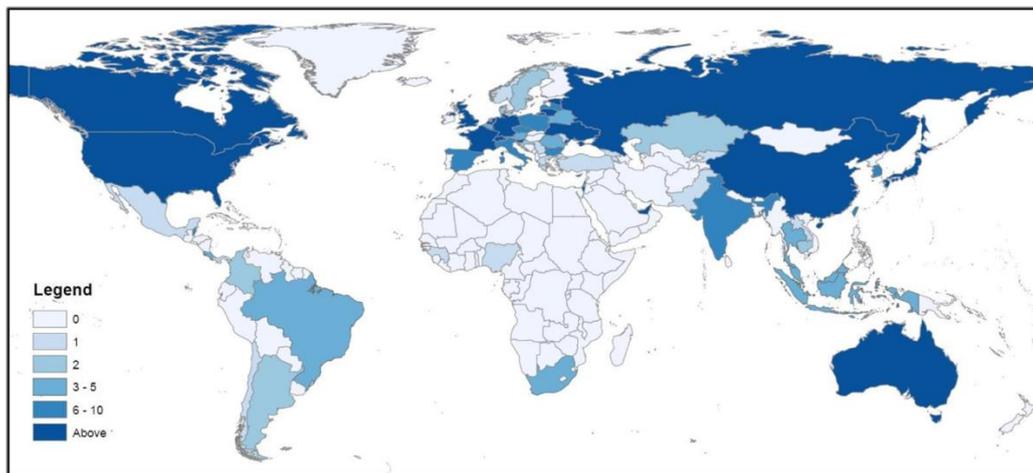


Figura 22 - Mappa ICOs nel mondo. Fonte: Huang et al, 2020.

Anche l'Italia non presenta un mercato delle ICOs sviluppato e l'operazione ricopre un ruolo marginale rispetto ai metodi di finanziamento tradizionali, complice la mancanza per molto tempo di una regolamentazione ben definita.

Per quanto riguarda l'allocazione settoriale, in accordo con il report⁹⁴ del 2022 pubblicato dal Politecnico di Milano assieme a molte società partner, i progetti in ambito blockchain e database distribuiti nel mondo appartengono per il 38% all'area finance e per il 17% all'area amministrativa, con le amministrazioni pubbliche che ancora non l'hanno fatto che si stanno attivando per implementare la tecnologia nei loro sistemi; per quanto riguarda invece i processi coinvolti, i più rilevanti sono quelli riguardanti la gestione dei pagamenti, la gestione dei dati e la gestione della catena produttiva, tutti processi molto rilevanti nell'ambito di gestione di un'azienda e di corporate finance.

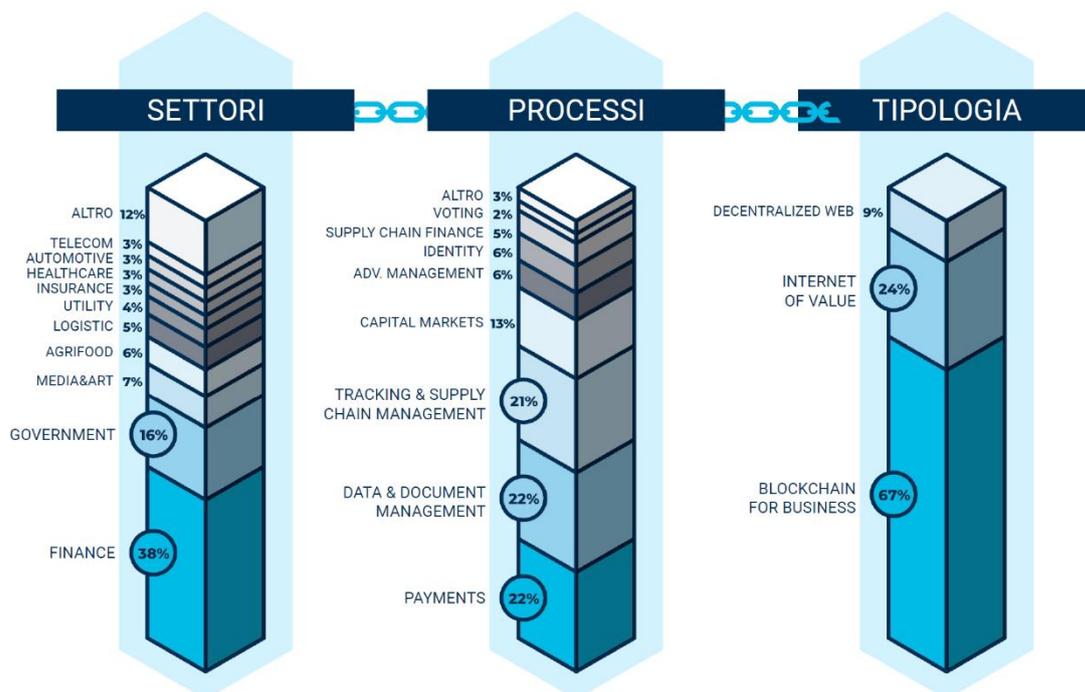


Figura 23 - Progetti blockchain per settore. Fonte: Osservatorio Blockchain e Distributed Ledgers del Politecnico di Milano.

⁹⁴ <https://blog.osservatori.net/hubfs/Report%20-%20Blockchain%20&%20Distributed%20Ledger--2022-.pdf>

2.9 CENNI DI REGOLAMENTAZIONE

Parlando di regolamentazione in uno stato, innanzitutto si deve avere presente che nello sviluppo sono coinvolte più autorità, non solo quelle nazionali ma anche quelle sovranazionali, come può essere l'Unione Europea per l'Italia. Solitamente l'autorità sovranazionale si occupa di condividere informazioni e di definire le *best practices*, senza intervenire direttamente se non per tentare di armonizzare le regolamentazioni presenti; l'autorità nazionale è quella che definisce nel dettaglio la legislazione e non è un'autorità unica, bensì è composta da più autorità che lavorano separatamente e che tentano di perseguire diversi obiettivi (governo, autorità di controllo finanziario, banca centrale).

In questo scenario, ci deve essere un regolatore che per primo pone l'accento sul prodotto o servizio che secondo lui necessita di regolamentazione: uno studio dell'università di Cambridge⁹⁵ su un campione di 40 diverse giurisdizioni, ha sottolineato che l'autorità che per prima ha emesso un comunicato ufficiale riguardo le criptovalute nel 40% dei casi è la banca centrale, mentre nel 17% dei casi è l'autorità addetta alla supervisione finanziaria (in Italia questa autorità è la CONSOB); inoltre, in 30 delle giurisdizioni analizzate, il primo comunicato ufficiale è arrivato nel 2013, a sottolineare l'importanza che alcune autorità hanno dato al mondo delle criptovalute già agli albori della tecnologia. Anche per quanto riguarda la terminologia utilizzata le diverse giurisdizioni non sono concordi tra loro e ciò porta ad utilizzare diversi termini per definire la stessa cosa (ad esempio quello che abbiamo definito security token è anche denominato asset token, investment token o equity token).

⁹⁵<https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf>

Nel regolamentare, i legislatori possono utilizzare diversi approcci, come viene anche sostenuto dal documento del World Economic Forum riguardo la regolamentazione delle criptovalute nel mondo⁹⁶: si può avere un approccio del tipo “aspettiamo e vediamo”, oppure un approccio basato su una partnership tra il pubblico e il privato, che prevede di regolamentare sulla base delle decisioni che vengono prese nelle discussioni tra i regolamentatori e il settore privato, con un occhio di riguardo alla crescita del business e alla formazione del settore, o ancora un approccio comprensivo o restrittivo, dove il legislatore decide autonomamente le regolamentazioni ed esse influenzeranno positivamente o negativamente lo sviluppo del mercato nascente.

In base all’approccio dei regolatori si può decidere di adattare leggi esistenti ed estenderle al mondo delle valute digitali (decisione efficace soprattutto in un approccio attendista per non lasciare un vuoto di regolamentazione), oppure creare un nuovo set di regole che verranno applicate alla nuova tecnologia o a dei sottoinsiemi di essa; quest’ultimo approccio segue il concetto di “equivalenza funzionale”, con il fine di applicare un insieme di regole già definite ad un determinato prodotto: nel caso in nostro esame, l’approccio tenta di capire se i diversi token possano essere ricondotti a dei prodotti finanziari già regolamentati per tentare di estendere la regolamentazione esistente senza dover partire a crearne una da zero (De Filippi et al., 2019). Le somiglianze tra i token e altri investimenti sono presenti, come abbiamo visto in questo capitolo, e ciò ha fatto sì che i legislatori di molti paesi abbiano esteso regolamentazioni tipiche di titoli finanziari e IPO alle operazioni di emissione di security token, o la legislazione di operazioni di reward-based crowdfunding alle ICOs che prevedono l’emissione di utility token.

⁹⁶ https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

Quasi tutti i regolatori hanno quindi dato una definizione di “valuta digitale” spiegando cosa intendano e cosa si possa assimilare alla definizione fornita, andando a mettere dei paletti più o meno ferrei; ad oggi, la grande maggioranza degli stati ha regolamentato le criptovalute o si è dotato di un’apposita legislazione, soprattutto riguardo la distribuzione delle monete virtuali (quindi le ICOs) e l’attività degli exchange. Gli approcci dei legislatori sono stati diversi e più o meno permissivi, ma la tecnologia è in rapida evoluzione e al momento stanno emergendo nuovi rischi e la necessità di gestione da un punto di vista legislativo di questi rischi. Non è compito di questo elaborato andare ad indagare nel dettaglio le regolamentazioni dei vari paesi poiché la trattazione risulterebbe particolarmente gravosa e non essenziale per l’obiettivo, ma, oltre a farci un’idea delle principali regole vigenti nei paesi più attivi dal punto di vista delle ICOs, è interessante indagare quali saranno le prossime sfide dei regolamentatori, che devono svolgere un lavoro tutt’altro che facile: quando si ha a che fare con una nuova tecnologia, oltre alla difficoltà di comprensione si deve prestare attenzione al grado di regolamentazione, come viene evidenziato anche dal WEF⁹⁷, poiché se si attua una regolamentazione eccessivamente stringente si rischia di soffocare sul nascere il processo innovativo della tecnologia stessa, mentre se si impongono regole eccessivamente permissive si espongono maggiormente gli investitori ad eventuali truffe e si favorisce la nascita di progetti poco trasparenti; è quindi importante che i legislatori attuino delle regolamentazioni precise perché l’ambiente esterno giova del fatto di avere una certezza legale, che viene ben vista dagli investitori e dal mercato, ma senza calcare troppo la mano perché un’eccessiva regolamentazione ottiene l’effetto contrario (Ahern, 2021).

⁹⁷ https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

Per avere un quadro più completo della situazione e qualche esempio, diamo una rapida occhiata ad alcune regolamentazioni rilevanti e tra loro contrastanti, dei paesi attivi dal punto di vista dell'emissione di token, nel particolare Regno Unito, Svizzera, India e Cina.

Nel Regno Unito i regolatori si sono mossi precocemente per dotarsi di una regolamentazione e ciò ha ridotto l'incertezza e ha posto le basi per lo sviluppo del mercato delle criptovalute; nel 2019 l'autorità britannica FCA (Financial Conduct Authority) ha sviluppato un regime regolatorio applicabile a tutti i tipi di token dopo aver effettuato una categorizzazione tra loro; nel 2018 ci si è dotati di una legge (Her Majesty's Revenue and Customs) che ha stabilito le linee guida per quanto riguarda la tassazione del capital gain applicabile alle criptovalute. Il Regno Unito ha poi attuato diverse iniziative volte a promuovere l'implementazione e l'adozione della tecnologia blockchain da parte delle imprese (Bellavitis et al, 2020).

Situazione simile a quella britannica dal punto di vista della precocità dell'emissione di linee guida in grado di creare terreno fertile per la nascita del mercato criptovalute si è verificata in Svizzera, una delle prime nazioni in assoluto ad attuare una regolamentazione per le criptovalute, già nel 2014 (Bellavitis et al, 2020); nel 2020 il legislatore ha diramato un atto che espande la regolamentazione della blockchain e delle DLT già abbondantemente sviluppata e definita. Per quanto riguarda la tassazione, l'autorità Svizzera ha deciso di non voler tassare i guadagni dei privati generati tramite criptovalute (soluzione molto gradita agli investitori), e da febbraio 2021 nel cantone di Zurigo è accettato il pagamento delle tasse attraverso le criptovalute⁹⁸.

⁹⁸ https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

In India e in Cina la situazione è stata differente rispetto a Regno Unito e Svizzera; in India nel 2018 la Reserve Bank of India (RBI) ha proibito alle persone di commerciare criptovalute, e la situazione è rimasta tale fino a marzo 2020, quando un ordine della Corte Suprema ha abolito la regola. Le restrizioni e l'assenza di regolamentazione hanno creato un terreno ostile per lo sviluppo della blockchain, anche se nel 2021 il governo ha manifestato l'interesse di dotarsi di apposite leggi a riguardo. Anche dal punto di vista fiscale non sono state sviluppate leggi o linee guida⁹⁹.

La Cina rappresenta invece un caso particolare, perché si è dotata precocemente di regolamentazioni che hanno permesso alle criptovalute di raggiungere una fama notevole, salvo poi ritrattare e applicare grandi restrizioni alla tecnologia. Al momento le criptovalute non sono bandite ma sono appunto soggette a notevoli restrizioni, mentre l'attività di mining e gli exchange sono considerati illegali. Il focus della Cina riguardo la tecnologia è principalmente legato allo sviluppo da parte della banca centrale della moneta digitale di stato, progetto che viene fortemente sostenuto perché permetterebbe di attuare un controllo centralizzato anche sui pagamenti.

In ultimo, diamo uno sguardo alla situazione in Italia. Nel nostro paese, l'autorità che si è espressa ed ha posto attenzione sul tema è stata la CONSOB; l'autorità ritiene che il fenomeno sia di sua competenza perché paragona i token a strumenti finanziari dato che presentano molte analogie con diversi prodotti finanziari¹⁰⁰. La CONSOB è attenta alla tutela degli acquirenti dei token e vorrebbe creare per le ICOs e per le STOs dei portali simili a quelli di equity crowdfunding, dove gli investitori possano interagire con gli emittenti cercando di ridurre le asimmetrie informative e vedendosi garantito un buon

⁹⁹ https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

¹⁰⁰ https://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/12117302-78b0-4e6e-80c4-d3af7db0fdac

grado di protezione, senza dover creare un insieme di regole rigide¹⁰¹. Il legislatore italiano a fine 2018 ha introdotto le definizioni di DLT e smart contract e ha riconosciuto il valore giuridico delle certificazioni emesse tramite tecnologia blockchain. Complice una direttiva dell'Unione Europea, si è poi posto l'accento sulle operazioni di STO, in quanto risultano rilevanti nel continente poiché permettono alle imprese, anche di dimensioni ridotte, di rendere liquidi degli asset in proprio possesso tramite il processo di tokenizzazione; per rendere la tecnologia maggiormente utilizzabile dalle aziende il legislatore europeo ha deciso di permettere alle piccole e medie imprese (PMI¹⁰²) di emettere security token attraverso l'utilizzo di un prospetto semplificato, che risulta meno gravoso in termini di costi se paragonato ai documenti da produrre in media per un'operazione di questo tipo¹⁰³.

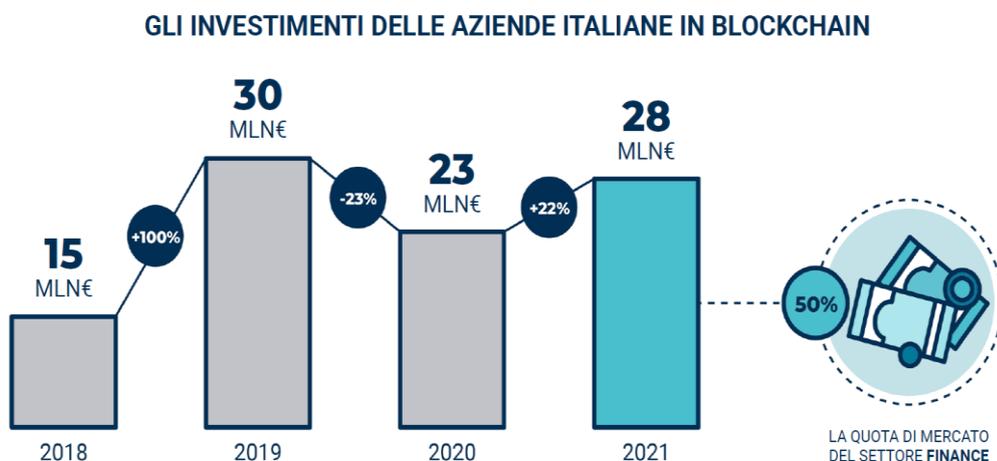


Figura 24 - Investimenti delle aziende italiane in ambito blockchain. Fonte: Osservatorio Blockchain e Distributed Ledgers del Politecnico di Milano.

¹⁰¹<https://tayros.bg/index.php/2022/03/15/la-regolamentazione-di-security-token-offering-sto-ico-blockchain-e-smart-contract-in-italia-lapproccio-consob/>

¹⁰² Con il termine PMI il legislatore europeo identifica delle aziende aventi meno di 250 dipendenti e un fatturato annuo inferiore ai 50 milioni di euro, oppure un attivo in bilancio inferiore ai 43 milioni di euro.

¹⁰³https://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/12117302-78b0-4e6e-80c4-d3af7db0fdac

Da quanto viene detto nella trattazione dell'argomento, potrebbe emergere che ormai quasi tutti i paesi abbiano definito delle regolamentazioni alle criptovalute, e ciò è vero, ma la tecnologia e le possibilità derivanti da essa sono in evoluzione rapida e costante; per questo motivo ci troviamo spesso in una situazione in cui è stata creata una regolamentazione, partendo da zero oppure attraverso l'estensione di una già esistente, ma che essa si trovi a regolare solo una parte dell'universo che circonda la blockchain. Abbiamo detto che nel 2013 le autorità nazionali hanno iniziato ad usare il termine criptovaluta in alcuni comunicati ufficiali, ma solo qualche anno dopo la maggior parte delle nazioni si è dotata di apposite regolamentazioni riguardo le criptovalute, mentre sono ancora più recenti quelle riguardo le ICOs. In questo scenario e nell'ottica di salvaguardare gli investitori senza soffocare l'innovazione, i legislatori devono attivarsi per regolare dei fenomeni sempre più permeanti in ambito blockchain.

Parlando di ICOs, ad esempio, ci può venire in mente un'operazione chiamata airdrop¹⁰⁴, operazione che ha guadagnato recentemente popolarità e che spesso non presenta regolamentazioni; l'operazione consiste nella distribuzione di token da parte di un'azienda a utenti attuali o potenziali, soprattutto per finalità di marketing e di ampliamento della rete, caratteristica essenziale di ogni blockchain. In generale tutto il mondo della finanza decentralizzata (DeFi)¹⁰⁵, termine con il quale si indica la finanza senza bisogno di intermediazione sviluppatasi grazie alla tecnologia blockchain (soprattutto grazie all'utilizzo di smart contract e oracoli), ha avuto un boom incredibile ed attualmente risulta scarsamente regolamentato e potenzialmente pericoloso per un utente non correttamente informato sui rischi e sulle operazioni che sta svolgendo, e ciò

¹⁰⁴ <https://academy.binance.com/it/articles/what-is-a-crypto-airdrop>

¹⁰⁵ <https://www.ilsole24ore.com/art/defi-come-funziona-finanza-pret-a-porter-basata-blockchain-AEJ3rj9>

rappresenta una sfida notevole per tutti i regolamentatori. Ormai la finanza decentralizzata ha creato un mondo finanziario parallelo a quello reale e nel quale è possibile effettuare delle operazioni analoghe a quelle finanziarie tradizionali, grazie all'utilizzo di smart contract e stablecoin ancorate al prezzo delle maggiori valute fiat; è infatti possibile effettuare operazioni di staking su molti exchange (operazioni simili a prestiti agli exchange per i quali ci viene corrisposto un interesse, interesse che è spesso molto maggiore di quello utilizzato in quel momento nel mondo reale suscitando in capo a molti perplessità rilevanti riguardo la sostenibilità dell'operazione stessa), piuttosto che operazioni di utilizzo delle criptovalute come collaterale per ottenere prestiti in valuta fiat o in stablecoin.

La finanza decentralizzata è un mondo innovativo, vasto e in molti casi affascinante e necessiterebbe di un'attenta analisi per essere approfondita, ma ciò non è il proposito di questo paragrafo. In accordo con la letteratura, la FinTech (abbreviazione inglese di "finanza tecnologica") sta avendo un impatto notevole in molti settori, da quello dei pagamenti, agli investimenti, a quello della finanza tradizionale, presentando diverse nuove sfide agli attori presenti nel mercato e agli stessi regolamentatori, che dovranno ingegnarsi per porre dei limiti allo sviluppo senza frenare l'innovazione (Ahern, 2021).

CAPITOLO 3 – LE STABLECOIN

Dopo aver esposto una panoramica generale del funzionamento della tecnologia blockchain e aver indagato come le aziende abbiano usato la tecnologia per finanziarsi, in questo ultimo capitolo si vogliono analizzare un paio di aspetti della tecnologia che vengono da me ritenuti particolarmente interessanti: il ruolo delle stablecoin all'interno del mercato delle criptovalute e le ripercussioni che esse possono avere sull'economia reale, e le cosiddette “monete digitali delle banche centrali” (in inglese definite CBDC, *Central Bank Digital Currency*), ovvero quelle criptovalute che le banche centrali di tutto il mondo stanno studiando di inserire sul mercato per creare una moneta virtuale emessa da un'istituzione monetaria, a tutti gli effetti equiparabile alla valuta fiat della quale la stessa banca centrale decide la politica monetaria. Di fatto le monete digitali delle banche centrali sono delle stablecoin, in quanto hanno un valore fisso uguale a quello della valuta fiat alla quale corrispondono.

3.1 STABLECOIN

Per iniziare il nostro discorso partiamo ad analizzare le stablecoin emesse da aziende private, che al momento sono già presenti in grande quantità nel mercato delle criptovalute, tentando di capire come mai da qualche anno a questa parte questo tipo di moneta abbia avuto così tanta fortuna.

3.1.1 TIPI DI STABLECOIN

Per capire l'importanza e l'utilità delle stablecoin nel mondo delle criptovalute, per prima cosa bisogna operare una distinzione tra di esse, in quanto non tutte le monete presentano le stesse caratteristiche. La distinzione fondamentale è tra stablecoin "collateralized", ovvero ancorate ad un asset preesistente, oppure stablecoin algoritmiche. Tra le stablecoin aventi un collaterale è possibile effettuare un'ulteriore distinzione, principalmente con riguardo al sottostante che sostiene la moneta: si possono così avere monete ancorate ad una valuta fiat (queste sono la porzione più grande del mercato e la maggior parte sono agganciate al dollaro americano, esempi sono Tether e USD Coin), piuttosto che ad una commodity come l'oro (ad esempio Pax Dollar), o a delle criptovalute (Dai) (Kristoufek, 2022); le stablecoin algoritmiche invece, non presentano un altro asset come sottostante, ma mirano a mantenere il peg¹⁰⁶ con la valuta fiat attraverso degli algoritmi che essenzialmente incentivano l'offerta (emettendo token) quando il prezzo sale sopra al peg, portando di nuovo la stablecoin al valore desiderato, o, al contrario, incrementano la domanda (bruciando token) se il prezzo scende sotto al peg¹⁰⁷.

¹⁰⁶ Con il termine peg si intende un tasso di cambio fisso; nel caso in esame indica il tasso di cambio tra la criptovaluta e la valuta fiat.

¹⁰⁷<https://www.coindesk.com/tech/2021/12/16/how-stablecoins-merge-traditional-and-decentralized-finance/>

101 Blockchains | AN OVERVIEW OF STABLECOINS

WHAT IS A **STABLECOIN**?

Stablecoin is a type of cryptocurrency that always holds a stable price. These type of cryptocurrencies are created to take on the unstable crypto market scenario and ensure a stable ground for all.

Thus, stablecoins are crucial for crypto investors, exchanges and the overall crypto market.



DIFFERENT TYPES OF STABLECOINS

Icon	Type	WHAT IT MEANS	POPULAR PROJECTS
	Fiat-Backed	These are backed up by fiat money and one of the common forms of stablecoin. In simple term, it's somewhat a digital form of fiat money.	 TrueUSD  tether  GEMINI
	Commodity-Backed	This type of coin is backed up by commodities such as Gas, Gold, Valuable Metals, etc. Here, all these commodities will always have a stable value on the network.	 DIGIX  ietherbase.com
	Cryptocurrency-Backed	Cryptocurrencies back up this type of stablecoin. Usually, these coins are backed up by a mix of different cryptocurrencies, instead of a single crypto. This structure prevents any volatility risks.	 MAKER  SYNTHETIX
	Seigniorage-Style/ Non-collateralized	This category of coins is a bit different. They don't have any assets to back them up, rather they use an algorithm to burn or add crypto to stabilize the value.	 CARBON  KOWALA

Figura 25 - I diversi tipi di stablecoin. Fonte: 101blockchains.com

Le stablecoin algoritmiche sono spesso state il bersaglio di numerose critiche, in quanto non posseggono la stabilità intrinseca che si cerca da questo tipo di asset: molto spesso una stablecoin algoritmica mantiene l'equivalenza con la valuta fiat grazie ad un altro token presente sulla piattaforma, che viene creato o distrutto (un meccanismo chiamato mint/burn) a seconda della necessità e dipende quindi molto dal valore di esso.

3.1.2 IL CASO TERRA-LUNA E LE RIPERCUSSIONI SUL MERCATO

Recentemente si è dimostrata la fondatezza di alcune di queste critiche; a inizio maggio 2022, la stablecoin della blockchain Terra¹⁰⁸, denominata Terra USD (UST), che in quel periodo era la stablecoin algoritmica più capitalizzata sul mercato con oltre 18 miliardi di dollari di capitalizzazione¹⁰⁹, ha perso l'equivalenza con il dollaro, fermandosi a 0,80\$ prima di capitolare fino all'attuale valore di pochi centesimi. Questa blockchain è nata come un sistema di stablecoin per facilitare pagamenti, ma di fatto è diventata rilevante come ecosistema nel mondo della DeFi¹¹⁰. In questo ecosistema, oltre alla stablecoin era presente il token proprietario, denominato LUNA ed essenziale per l'esistenza di Terra USD, in quanto facente parte di un meccanismo che prende il nome di signoraggio¹¹¹; sostanzialmente l'operazione consiste nel dare la possibilità a tutti i partecipanti della blockchain e detentori di token LUNA di agire in due diversi modi a seconda dello scenario di mercato: se UST ha valore maggiore di un dollaro, il possessore di LUNA può coniare UST al valore di un dollaro, "bruciando" LUNA (ovvero scambiando il token LUNA, che verrà distrutto, con una quantità di token UST) e rivenderli immediatamente sul mercato; questa operazione permette all'utente di avere un minimo guadagno (conio a 1\$ e rivendo ad un prezzo sensibilmente superiore), e aumenta l'offerta di UST (diminuendone il prezzo), mentre diminuisce l'offerta di LUNA (che di conseguenza vedrà il suo prezzo aumentare, con felicità di chi compie questa operazione). Nel caso in cui UST si trovi sotto al dollaro, si ha invece la possibilità di compiere l'azione inversa: il detentore di UST può scambiare il token con dei token LUNA al valore teorico di un

¹⁰⁸ <https://www.terra.money/>

¹⁰⁹ <https://coinmarketcap.com/currencies/terrausd/>

¹¹⁰ <https://cryptoeccetera.com/cose-terra-luna-guida-a-terra-money/>

¹¹¹ <https://cryptoeccetera.com/cose-terra-luna-guida-a-terra-money/>

dollaro e così facendo ottiene un guadagno avendo comprato LUNA “in sconto”, e la stablecoin, a seguito di questa riduzione dell’offerta, subisce un aumento del prezzo, e può così ritornare all’equivalenza con il dollaro.

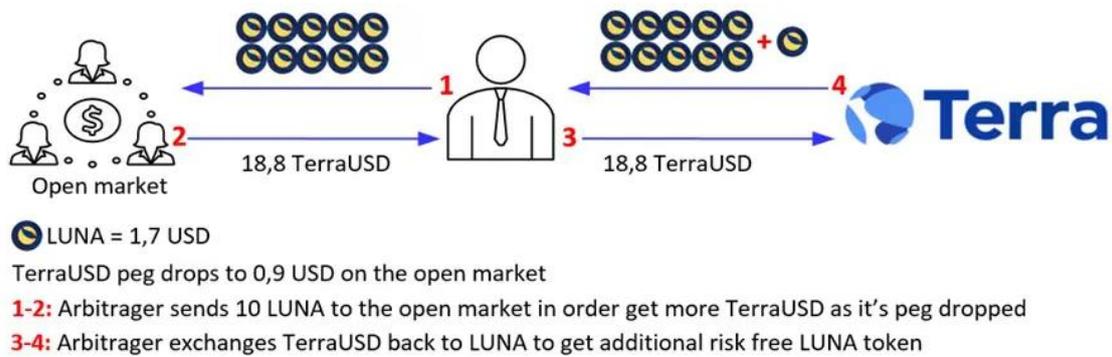


Figura 26 - Arbitraggio Terra USD - Luna. Fonte: coinbureau.com

Questo meccanismo incentiva quindi gli utenti a queste operazioni di compravendita di token, poiché permette di avere un guadagno semplice derivato da operazioni di arbitraggio volte a mantenere la stabilità di UST, ma può rivelarsi molto pericoloso in caso di movimenti bruschi di mercato, come di fatto accaduto alla stablecoin a partire dallo scorso 9 maggio. Alcuni prelievi di grosse entità (qualche centinaio di milione di dollari) hanno fatto perdere a UST l’equivalenza con il dollaro in modo abbastanza deciso; se in uno scenario di minime variazioni il meccanismo di mint/burn ha dimostrato di funzionare correttamente, così non è stato in uno scenario di forti variazioni: innanzitutto, il panico generato dalla perdita di valore di una stablecoin ha spinto molti possessori alla vendita, spaventati da una possibile ulteriore perdita di valore della moneta; inoltre, per come è stato concepito l’algoritmo, per tentare di far riguadagnare il peg alla stablecoin si è iniziato a produrre enormi quantità di LUNA, causando un crollo anche del token proprietario della blockchain, senza però riuscire a riportare l’UST

all'equivalenza con il dollaro¹¹². La Luna Foundation Guard¹¹³, organizzazione no profit nata con l'obiettivo di mantenere il peg della stablecoin Terra USD e quindi il corretto funzionamento della blockchain Terra, vista la mancanza di equivalenza tra UST e la moneta americana, ha provveduto a vendere tutti i bitcoin in suo possesso (70000 unità) per cercare di raggiungere nuovamente l'equivalenza con il dollaro, ma nemmeno ciò ha avuto successo vista la mancanza di fiducia crescente venuta a crearsi nell'ecosistema¹¹⁴, anzi, al contrario, la vendita ha contribuito a far diminuire anche il prezzo di bitcoin e a trascinare in basso l'intero mercato delle criptovalute, come accennato nel precedente capitolo. Il token LUNA è arrivato così a perdere l'intero valore, e Terra USD attualmente vale un paio di centesimi; Terra Foundation sta comunque tentando di salvare l'ecosistema (cosa che appare però quasi impossibile), attraverso l'iniezione di nuovi capitali (che faticano molto ad arrivare, dato che la quasi totalità degli investitori è convinta dell'imminente fallimento del progetto) e attraverso il rimborso parziale dei suoi precedenti investitori: dopo la votazione di governance positiva¹¹⁵, ha infatti trasferito tramite airdrop ai precedenti possessori di LUNA e di UST una nuova moneta denominata LUNA 2.0. L'operazione non ha sortito l'effetto sperato: dal rilascio del token, avvenuto il 28 maggio, in soli due giorni il valore di LUNA 2.0 ha subito un crollo di oltre il 70%¹¹⁶, dovuto soprattutto al fatto che gli investitori abbiano in gran parte liquidato immediatamente l'investimento per rientrare, anche solo parzialmente, delle perdite ricevute dal possesso dei token crollati di valore. La situazione rimane comunque

¹¹²https://www.hwupgrade.it/news/web/terra-luna-e-la-stablecoin-algoritmica-ust-ecco-cosa-e-successo_107113.html

¹¹³ <https://medium.com/alessandro-omega/formazione-del-luna-foundation-guard-lfg-14eba11481bd>

¹¹⁴ <https://it.cointelegraph.com/news/kwontitative-easing-btc-price-hits-43k-in-ust-as-terra-empties-2-2b-bitcoin-bag>

¹¹⁵ <https://it.cointelegraph.com/news/do-kwon-proposes-terra-hard-fork-to-save-ecosystem>

¹¹⁶ <https://it.cointelegraph.com/news/investors-dumping-on-terra-as-luna-2-tanks-70-in-two-days>

complessa, e, nonostante i tentativi, appare difficile che la blockchain Terra possa riguadagnare la fiducia da parte del pubblico o iniezioni di denaro sufficienti a salvare l'ecosistema da un fallimento praticamente certo.

A risentire dell'avvenimento è stato tutto il mercato delle criptovalute, comprese le stablecoin: il panico causato dal crollo di Terra USD ha scatenato una vendita importante di Tether, che ha perso di conseguenza l'equivalenza con il dollaro, anche se solo momentaneamente¹¹⁷; la società emittitrice di USDT infatti, ha dovuto in qualche giorno restituire circa 7 miliardi di dollari ai suoi investitori¹¹⁸, e ciò è stato possibile liquidando dei buoni del tesoro americano, asset che l'azienda detiene a riserva come sottostante della moneta. Il prezzo di Tether è quindi ritornato in breve tempo in pareggio con il dollaro, aiutando a calmare l'eccessiva paura presente sul mercato dopo gli avvenimenti di Terra USD. In generale il mercato delle criptovalute sta comunque faticando molto a riprendersi; a metà giugno 2022, possiamo notare che tutte le maggiori monete abbiano perso gran parte del loro valore, e si iniziano a vedere delle criticità tra le piattaforme che forniscono servizi nel mondo delle criptovalute: giusto per citare un esempio, Celsius, una piattaforma CeFi (Centralized Finance, si distingue dalla DeFi principalmente per una maggiore facilità di utilizzo, ma nel contempo è necessario porre fiducia nel sistema poiché è centralizzato ed esiste quindi un'autorità centrale di controllo alla quale gli utenti devono fare affidamento), ha stoppato tutti i prelievi e i trasferimenti di criptovalute tra gli account a causa di "condizioni di mercato estreme", con l'intento di stabilizzare la liquidità dell'exchange per evitare un possibile default sulle obbligazioni assunte¹¹⁹.

¹¹⁷ <https://www.wallstreetitalia.com/usdt-il-panico-mette-in-crisi-il-peg-di-tether/>

¹¹⁸ https://www.repubblica.it/economia/affari-e-finanza/2022/05/30/news/il_buco_da_40_miliardi_di_luna_apre_nuove_crepe_nelle_stablecoin-351440635/

¹¹⁹ <https://www.protocol.com/bulletins/crypto-firm-celsius-stops-withdrawals>

Dopo aver visto quanto accaduto, risulta certamente più comprensibile capire il rischio intrinseco di una stablecoin “classica” rispetto alla più innovativa algoritmica: nonostante (a livello teorico) un algoritmo di mint/burn sia efficace a mantenere il peg di una stablecoin, in momenti di pessimismo e di paura sui mercati e di fronte a fattori esogeni inaspettati (come può essere un prelievo molto oneroso da un protocollo, ovvero ciò che è accaduto a Terra), l’algoritmo può contribuire ad affondare l’ecosistema, in quanto per i detentori dei token non risulta un incentivo abbastanza elevato la conversione della stablecoin nel token della piattaforma perché l’operazione, se continuativa, contribuisce ad abbassare notevolmente il valore del token proprietario, spingendo quindi gli investitori verso la liquidazione totale dell’investimento. Al contrario, se il valore di una stablecoin è sostenuto da un equivalente in denaro depositato come sottostante e di facile liquidazione, nel momento di un grosso richiamo di fondi è possibile vendere il collaterale per soddisfare le richieste dei creditori, senza provocare il crollo della valuta digitale. Questa operazione non è però esente dallo scatenare effetti collaterali sui mercati finanziari, come approfondiremo successivamente nel paragrafo.

3.1.3 L’UTILIZZO DELLE STABLECOIN NEL MERCATO DELLE CRIPTOVALUTE

Le stablecoin sono nate principalmente per ovviare ad un grosso problema di bitcoin e delle criptovalute in generale, quello della volatilità, che fa sì che questa criptovaluta non possa essere un’alternativa valida ad una valuta fiat (Hoang et al, 2020). Se rivolgiamo il nostro sguardo agli exchange, si intuisce la necessità che essi abbiano di effettuare transazioni on-chain tra di loro senza essere esposti al rischio di cambio derivante dalla

volatilità delle criptovalute “tradizionali” (Kristoufek, 2021); inoltre, essi possono riscontrare difficoltà ad ottenere le licenze bancarie necessarie a permettere ai clienti di usare moneta a corso legale per comprare direttamente criptovalute, mentre risulta più facile ottenere licenze per operare sul mercato attraverso l’utilizzo delle stablecoin (Griffin et al, 2019).

La popolarità delle stablecoin è andata in crescendo dalla prima moneta emessa, con i maggiori player del mercato delle criptovalute che hanno mostrato fin da subito un interesse crescente in questo asset; attualmente USDT e USDC sono secondi solo a bitcoin ed Ethereum in quanto a capitalizzazione di mercato, ma per quanto riguarda i volumi scambiati giornalmente Tether movimentava il doppio del capitale rispetto a bitcoin, che risulta la seconda criptovaluta in termini di volume giornaliero¹²⁰.

# ▲	Name	Price	24h %	7d %	Market Cap ⓘ	Volume(24h) ⓘ	Circulating Supply ⓘ
☆ 1	 Bitcoin BTC	\$18,883.87	▼ 8.34%	▼ 33.65%	\$359,727,821,755	\$28,553,283,508 1,513,731 BTC	19,070,700 BTC
☆ 2	 Ethereum ETH	\$982.83	▼ 8.88%	▼ 35.97%	\$119,204,386,038	\$14,162,768,908 14,402,161 ETH	121,219,286 ETH
☆ 3	 Tether USDT	\$0.9988	▼ 0.01%	▼ 0.03%	\$68,146,179,134	\$43,682,762,256 43,737,130,930 USDT	68,230,995,597 USDT
☆ 4	 USD Coin USDC	\$1.00	▲ 0.01%	▲ 0.03%	\$55,311,039,357	\$4,972,008,977 4,970,859,354 USDC	55,298,250,396 USDC

Figura 27 - Volumi di scambio di Tether e USD Coin in confronto a Bitcoin ed Ethereum. Fonte: coinmarketcap.com

Recentemente le stablecoin hanno guadagnato ulteriore popolarità grazie all’importanza che viene data ad esse da parte degli exchange e delle piattaforme per la DeFi; proprio l’utilizzo nei progetti DeFi ha contribuito ad aumentare l’apprezzamento di queste monete, ed alcuni exchange permettono tra l’altro lo staking delle stablecoin proponendo

¹²⁰ <https://coinmarketcap.com/>

ritorni altissimi sull'investimento (ad esempio crypto.com, uno degli exchange che più ha fatto parlare di sé nell'ultimo periodo, soprattutto per l'uso massiccio della pubblicità, propone attualmente il rendimento del 10% annuo su Tether e USD Coin¹²¹, rendimento che fino a poco tempo fa era superiore, ma che l'azienda ha deciso di ridurre). Questo fatto fa storcere il naso a molti, poiché ci si interroga sulla reale tenuta del sistema e sulla sostenibilità del progetto, in quanto teoricamente una stablecoin dovrebbe mantenere l'equivalenza con la valuta fiat alla quale è ancorata e di conseguenza essere un asset assimilabile ad essa, ma guardando il rendimento di mercato di un'obbligazione statunitense a 10 anni si può notare che esso sia del 3% (l'anno scorso era dell'1,5%), una notevole differenza rispetto al 10% annuo offerto per un asset che dovrebbe essere simile. Un rendimento così alto riflette una rischiosità intrinseca dell'asset maggiore, dovuta principalmente a due fattori: la liquidità dell'investimento e il rischio emittente. Quando si analizza un'obbligazione standard, che è uno strumento finanziario che presenta alcune analogie con lo staking sulle piattaforme DeFi, i rischi principali in cui si incorre sono di tre tipi: rischio di tasso di cambio, rischio emittente e rischio liquidità; se si confrontano due obbligazioni, nell'analisi si può trascurare il rischio di tasso di interesse (ammesso che gli strumenti abbiano la stessa durata) e concentrarsi sugli altri due aspetti. Nell'analisi dello staking, sicuramente pesa il fatto di non poter ritirare l'investimento prima della scadenza (esso presenterà quindi una liquidità nulla), anche se l'orizzonte temporale è relativamente limitato (solitamente qualche mese); si presenta però un rischio emittente decisamente maggiore, poiché l'investitore dispone di garanzie molto ridotte e, di fronte a situazioni di mercato particolarmente concitate, potrebbe andare incontro ad una perdita totale del capitale. In ogni caso i dubbi sulla sicurezza dell'operazione e sulla

¹²¹ <https://crypto.com/eea/earn>

rischiosità delle compagnie che propongono progetti DeFi rimangono, poiché per garantire un rendimento così alto sulle stablecoin l'azienda è obbligata ad avere un rischio operativo intrinseco del business piuttosto elevato.

Nonostante la crescente importanza di questo asset nel mondo delle criptovalute, le ricerche sul tema hanno riscosso meno successo rispetto a quelle sugli altri token, le quali hanno avuto un boom nel 2017, con lo scoppio delle ICOs; i lavori riguardanti le stablecoin si sono concentrati perlopiù sulla loro capitalizzazione di mercato, che viene utilizzata come metro di misura dell'affluenza dei capitali nel mercato delle criptovalute, dato che la capitalizzazione delle principale stablecoin è aumentata di oltre 200 volte dal lancio e data l'enorme importanza che ricoprono nelle operazioni di trading (nei più grandi exchange, i volumi più alti non si registrano tra coppie di criptovalute, bensì tra una stablecoin e una criptovaluta) (Kristoufek, 2022).

3.1.4 CRITICHE ALLE STABLECOIN

Oltre ai numerosi vantaggi per gli exchange e all'apprezzamento da parte del pubblico (dovuto principalmente all'abbassamento delle commissioni e all'incremento della facilità d'investimento), le stablecoin sono anche oggetto di alcune critiche; in primis, la letteratura ha evidenziato come queste monete possano svolgere un ruolo chiave nell'incrementare le valutazioni delle altre criptovalute durante dei periodi di bolla speculativa (come quello del 2017). A favore di questa tesi vi è l'ipotesi intuitiva che sostiene che un asset che contribuisce a facilitare la raccolta e l'inserimento di capitali nel mercato amplifichi l'effetto di crescita dei prezzi che si ha durante una bolla; le ricerche tuttavia, non sono concordi nell'accettare o meno questa ipotesi: Wei (2018) ad esempio,

sostiene che non vi siano segnali che indichino i prezzi di bitcoin siano manipolati tramite l'uso delle stablecoin, e Kristoufek (2022), autore di una delle ultime ricerche in materia, è concorde nell'affermare che le stablecoin non amplifichino i prezzi durante una bolla. Al contrario Griffin et al (2019), nella loro ricerca trovano evidenze sul fatto che i prezzi di bitcoin vengano continuamente manipolati attraverso l'uso di Tether.

Un altro effetto del quale vengono "accusate" le stablecoin è quello di aumentare la volatilità del mercato, in quanto rendono più facile la compravendita di token; a supporto di questa ipotesi vi è la forte correlazione positiva tra i volumi di scambio delle stablecoin e la volatilità di bitcoin (Hoang et al, 2020) e alcune evidenze che, dati alla mano, indicano che le stablecoin siano spesso usate direttamente per comprare criptovalute, e aumenti del volume di esse causino degli aumenti del volume di trading tra le criptovalute (Ante et al, 2021).

A proposito di volatilità, si può aprire una parentesi interessante in quanto teoricamente (o per lo meno è ciò che si vorrebbe), le stablecoin dovrebbero avere una bassissima volatilità. Alcune ricerche hanno però evidenziato il contrario: ad una frequenza di 5 minuti si nota come le stablecoin siano invece instabili e mostrino una correlazione con l'andamento di bitcoin, sia in termini di ritorni che in termini di volatilità (evidenze che vengono meno nel caso di osservazioni di periodo più ampio) (Hoang et al, 2020). Anche guardando alle stablecoin sostenute dall'oro durante il periodo di pandemia da COVID-19, si nota anche in questo caso come la volatilità rimanga paragonabile a quella di bitcoin, nonostante esse siano state create appositamente per ridurre ulteriormente le fluttuazioni della moneta (Jalan et al, 2021).

Avendo sempre riguardo al rischio di volatilità, si possono aggiungere alcune ulteriori precisazioni basate anche sulla tecnologia delle stablecoin; abbiamo visto come le più innovative algoritmiche presentino dei rischi intrinseci maggiori, dato che il prezzo viene mantenuto costante attraverso algoritmi che si basano su smart-contract e attraverso incentivi economici per i partecipanti alla piattaforma, e ciò ci viene confermato da Bullmann et al. (2019) in un paper della Banca Centrale Europea, nel quale gli autori mettono in relazione l'innovatività della stablecoin in confronto alla loro volatilità. La stablecoin più sicura e meno esposta al rischio di volatilità è la moneta virtuale, intesa come moneta digitale emessa da una banca centrale, la quale è sostanzialmente equivalente ad una valuta fiat; tra le stablecoin sostenute da un collaterale invece, è possibile notare delle differenze, a seconda del tipo di collaterale utilizzato e del fatto che esso sia off-chain (un collaterale classico, detenuto da una parte terza che funge da garante), o on-chain (in questo caso il collaterale è un asset registrato su blockchain). Le stablecoin con collaterale on-chain presentano un potenziale innovativo maggiore, ma anche maggiori rischi, poiché la loro volatilità dipende anche dalla volatilità del sottostante, la quale può essere elevata nel caso in cui l'asset a collaterale on-chain sia una criptovaluta; al contrario, quelle off-chain, presentano un grado innovativo inferiore, ma anche minore esposizione alla volatilità, dato che tipicamente il sottostante è un sottostante "reale" e quindi meno volatile degli asset presenti su tecnologia blockchain. Nonostante ciò, si possono trovare differenze nella rischiosità anche tra le stablecoin off-chain, dato che i sottostanti possono essere di diversi tipi; se pensiamo, ad esempio, ad una moneta digitale che ha come riserva denaro contante e buoni del tesoro a breve termine, ci rendiamo conto di come essa possa ritenersi "sicura", in quanto gli asset detenuti sono estremamente liquidi e, anche in caso di grossi richiami della stablecoin, è

plausibile che si riesca a liquidare il sottostante in breve tempo e senza perdite di valore significative. Al contrario, alcuni tipi di sottostante considerati tipicamente liquidi, in determinate condizioni di mercato potrebbero diventare illiquidi, concorrendo ad incrementare notevolmente il rischio di default della stablecoin; ad esempio, un tipico collaterale utilizzato sono i commercial paper, che sono degli strumenti di debito a breve termine utilizzati dalle aziende per finanziare delle passività a breve termine¹²². Di norma questo strumento è altamente liquido, ma dei fattori esogeni sul mercato potrebbero trasformarlo in un asset illiquido con tutte le criticità del caso (Eichengreen et al, 2021). La composizione del sottostante è quindi una componente fondamentale da valutare per avere un'idea della stabilità di una stablecoin. Se analizziamo Tether, scopriamo che l'azienda emettitrice della moneta inizialmente non aveva rivelato il sottostante, ma l'interesse sempre crescente degli investitori nel minimizzare i rischi di investimento su prodotti basati su tecnologia blockchain ha obbligato l'azienda a rivelare il collaterale a sostegno di USDT. Fino a non molto tempo fa, Tether possedeva il 50% del valore posto a riserva in commercial paper, ma l'azienda ha deciso di ridurre l'esposizione su questo asset ed aumentare quella in Treasury americani¹²³; al momento, il sottostante di Tether è composto da circa il 50% di Treasury a breve termine e dal 25% di commercial paper¹²⁴.

3.1.5 RISCHI PER I MERCATI FINANZIARI

Questa composizione del sottostante fa sorgere in capo a molti analisti una preoccupazione riguardo al trasferimento della volatilità tra il mercato delle criptovalute

¹²² <https://www.investopedia.com/terms/c/commercialpaper.asp>

¹²³ <https://www.bloomberg.com/news/articles/2022-05-19/tether-declares-fall-in-commercial-paper-increase-in-treasuries>

¹²⁴ <https://tether.to/en/transparency/#reports>

e i mercati finanziari tradizionali. Storicamente, il mercato delle criptovalute è popolato da investitori meno esperti ed è caratterizzato da una volatilità molto alta; tuttavia, questo mercato non ha mai avuto una particolare influenza verso i mercati finanziari, soprattutto per il coinvolgimento limitato di risorse se paragonato ai mercati tradizionali. Molti analisti sono preoccupati dal fatto che un periodo di particolare incertezza sul mercato delle criptovalute, che potrebbe essere dovuto anche a degli attacchi da parte di grossi investitori istituzionali che mirano a destabilizzare alcune stablecoin a fini speculativi, possa far perdere momentaneamente la fiducia che gli investitori ripongono nell'asset causando vendite di grande volume, ed obbligando le aziende emittitrici delle stablecoin a liquidare grandi quantità di asset "reali". Al momento, i volumi scambiati e i valori di capitalizzazione delle stablecoin sono irrilevanti rispetto ai volumi che si registrano nelle borse tradizionali, per cui il problema non è particolarmente rilevante, ma potrebbe diventarlo in un futuro: per far fronte ai richiami di Tether richiesti dagli investitori dopo il panico provocato dal crollo di LUNA, l'azienda ha liquidato alcuni miliardi di Treasury a breve termine; se i volumi di scambio e la capitalizzazione diventassero più rilevanti, una liquidazione di massa di obbligazioni di Stato a breve termine porterebbe una rilevante volatilità nei mercati finanziari, con conseguenze che potrebbero impattare anche la solidità di molte aziende e i tassi d'interesse del mercato.

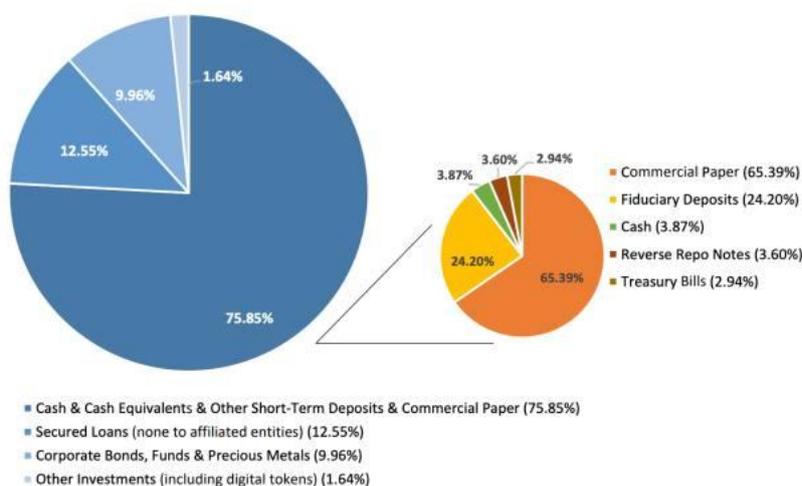


Figura 28 - Composizione del sottostante di Tether al 21 marzo 2021. Fonte: beincrypto.com

Anche la Banca Centrale Europea è concorde nell'affermare che, per il momento, le stablecoin portino dei rischi limitati alla stabilità finanziaria dell'area Euro, ma vista la rapidità con la quale stanno crescendo urge la necessità di sviluppare una regolamentazione efficace.

3.2 CENTRAL BANK DIGITAL CURRENCY

La valuta digitale emessa da una Banca Centrale (o Central Bank Digital Currency, CBDC) è un tipo di stablecoin, in quanto possiede tutte le caratteristiche di una criptovaluta ancorata al valore di un asset reale, ma, al contrario delle stablecoin emesse da aziende private, essa è emessa da un'istituzione finanziaria, e quindi dovrebbe avere un grado di sicurezza maggiore e dare maggiori diritti in capo ai possessori.

3.2.1 CONTESTO STORICO E IMPORTANZA PER LE BANCHE CENTRALI

Come viene evidenziato dalla Banca Centrale Europea, durante la storia il denaro e i tipi di pagamento si sono costantemente evoluti; negli ultimi anni si è avuto un incremento dei pagamenti digitali effettuati nei negozi e dei pagamenti online, e ciò ha contribuito a trasformare sempre più il nostro portafoglio da un oggetto fisico ad un oggetto virtuale presente su dei dispositivi elettronici. Questo cambiamento, unito alla nascita delle monete digitali, fa sorgere dei ragionamenti riguardo la necessità o meno da parte delle banche centrali di emettere delle versioni digitali delle valute fiat, di modo da continuare a mantenere un ruolo centrale nel sistema dei pagamenti e di preservare la sovranità monetaria¹²⁵.

La sovranità monetaria è una caratteristica essenziale del sistema capitalistico; con questa espressione si intende il diritto da parte di un soggetto giuridico di emettere moneta e di controllarla attraverso la scelta della sua politica monetaria. Ciò fa sì che vi sia un'istituzione centrale alla quale fare riferimento e nella quale porre fiducia per il corretto funzionamento del sistema monetario. Grazie a questa garanzia dello stato, i soggetti che fanno parte della società possono effettuare scambi di valore tra di loro, senza per forza dover porre fiducia uno nell'altro, dato che il bene oggetto di scambio ha valore di per sé perché garantito da un'istituzione centrale, ed è proprio questa possibilità di convertire denaro scambiato "tra privati" in denaro "pubblico" sicuro che garantisce il funzionamento e la fiducia nel sistema. Se così non fosse, i privati, prima di effettuare uno scambio tra di loro, dovrebbero controllare continuamente la validità e la credibilità dell'emittente della moneta, fatto che comprometterebbe il corretto funzionamento del

¹²⁵ https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220218_1~938e881b13.en.html

sistema di pagamento. Nella storia possiamo notare esempi di questo tipo: se prendiamo ad esempio il diciannovesimo secolo, notiamo che vi erano un discreto numero di banche che emettevano la propria moneta, la quale era però soggetta a fluttuazioni di prezzo e instabilità. La preoccupazione delle banche centrali è quella che, in un momento come questo in cui i pagamenti digitali stanno crescendo a dismisura, le banconote possano perdere la loro funzione di riferimento di valore, minando l'integrità del sistema monetario. In un contesto simile, si capisce il perché le banche centrali di tutto il mondo si stiano interrogando sulla necessità dell'emissione di valute digitali.

Alcuni sostengono che, qualora giustamente regolamentate, le stablecoin potrebbero rendere le CBDCs superflue, ma questo potrebbe non essere vero, dato che la fiducia nelle stablecoin si basa sulla loro capacità di essere scambiate con valute fiat; anche rendere disponibile ai privati emittitori di stablecoin di investire gli asset in depositi risk-free presso la banca centrale potrebbe essere un'idea, ma questo sarebbe equivalente ad un'emissione di moneta e potrebbe quindi danneggiare la sovranità monetaria, oltre ad avere un impatto sulle politiche monetarie e sui tassi di interesse reali presenti sul mercato¹²⁶.

Un altro rischio da non sottovalutare, è quello dell'effetto di sostituzione che si potrebbe creare nei confronti della propria moneta qualora un altro stato decidesse di emettere la sua moneta digitale: diversi modelli mostrano che la fruibilità della moneta digitale e il conseguente abbassamento dei costi delle transazioni aumentano le quote di questo tipo di moneta nei pagamenti globali e ciò potrebbe portare a problemi sia sull'economia della nazione (soprattutto nel caso di nazioni caratterizzate da monete ed economie deboli), sia

¹²⁶ https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220218_1~938e881b13.en.html

a delle difficoltà intrinseche per lo stato nel tutelare i suoi cittadini, in quanto l'adozione su larga scala di una moneta digitale straniera porterebbe a molti problemi di controllo, dovuti al fatto che le transazioni effettuate siano basate su tecnologie difficili da supervisionare perché dislocate all'estero e di proprietà di un altro stato, creando problemi sia di protezione dei cittadini, sia di carenza di informazioni necessarie ad ostacolare attività criminali quali il riciclaggio di denaro.

3.2.2 DIVERSI TIPI DI CBDC

Le CBDCs, come accade in tutti i tipi di token che si analizzano, non sono di un unico tipo; possiamo infatti operare una distinzione in base all'utilizzo per la quale viene emessa la moneta, definendo così le retail (al dettaglio) CBDC e le wholesale (all'ingrosso) CBDC. La differenza tra i due tipi risiede principalmente nel fatto che le retail sono una versione digitale della valuta a corso legale in grado di sostituire le banconote, mentre le wholesale sono designate solo per essere usate per effettuare transazioni tra istituzioni finanziarie, sia all'interno dello stato che per pagamenti internazionali. Le CBDCs al dettaglio risultano decisamente più interessanti per la nostra ricerca, in quanto sono uno strumento universale che potrebbe coinvolgere potenzialmente tutti i cittadini ed essere utilizzato in sostituzione al denaro contante. Le monete digitali emesse dalla banca centrale "al dettaglio", sono ulteriormente suddivisibili tra "direct retail" e "indirect retail", in base a quale istituzione finanziaria abbia a bilancio l'asset e detenga un record di tutte le transazioni; nel modello diretto questo ruolo è ricoperto solamente dalla banca centrale, mentre nel modello indiretto sono presenti degli intermediari (solitamente delle

banche commerciali) che si interfacciano con la banca centrale e a cui gli utilizzatori possono fare riferimento.

3.2.3 BENEFICI DELL'ADOZIONE DI UNA MONETA DIGITALE

Dopo aver rapidamente spiegato il perché in questo momento storico sia essenziale interrogarsi e discutere dell'adozione di una moneta digitale e dei rischi che potrebbero verificarsi qualora le istituzioni finanziarie non reagiscano rapidamente ai cambiamenti, possiamo anche prevedere gli eventuali benefici dei quali gioverebbero i cittadini derivanti dall'emissione e dall'utilizzo di una moneta di stato digitale. Come viene evidenziato sempre dalla BCE, questi benefici potrebbero essere molteplici, in primis riguardo alla privacy dei cittadini stessi. Se l'offerta di moneta avvenisse da parte un'istituzione pubblica, si potrebbe ovviare a tutti quei problemi di privacy e confidenzialità dei dati, dati che invece le aziende private hanno interesse ad ottenere perché risultano facilmente monetizzabili. Questo aspetto è quello più tenuto in considerazione dai cittadini; infatti, un sondaggio svolto nel 2020 dalla BCE¹²⁷, ha evidenziato come i cittadini considerino l'aspetto della privacy come il più importante per l'adozione di un euro digitale (con il 43% degli intervistati a sostegno di questa posizione), seguito dalla sicurezza dei pagamenti (ritenuta la caratteristica principale dal 18% del campione).

Un altro beneficio che si potrebbe apprezzare è quello dell'inclusione finanziaria; sebbene ciò dipenda da molti fattori, in primis dall'educazione finanziaria, si può notare che il costo dei servizi finanziari gioca un ruolo importante riguardo questo aspetto. Un euro

¹²⁷ https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210414_1~e76b855b5c.en.html

digitale sarebbe in grado di ridurre i costi di transazione nel mercato dei pagamenti, mercato che nel mondo è dominato da poche aziende di dimensioni rilevanti: nell'Unione Europea si stima che l'1,4% del PIL sia speso per i servizi di pagamento, e negli Stati Uniti questa quota è addirittura maggiore¹²⁸, contribuendo all'esclusione dai pagamenti digitali delle parti di popolazione che percepiscono redditi bassi. Questa ipotesi è confermata da uno studio riguardante l'attitudine al tipo di pagamento nell'area euro, nel quale viene evidenziato come la preferenza per i contanti sia significativamente più alta tra chi percepisce un reddito inferiore ai 1000€ mensili (solo il 36% della popolazione dichiara di preferire un metodo di pagamento con carta o comunque cashless, contro il 61% di preferenze per questi metodi espresse tra chi percepisce più di 2500€ mensili)¹²⁹.

L'adozione di una moneta digitale potrebbe portare numerosi cambiamenti per quanto riguarda i pagamenti anche a livello globale tra diverse nazioni, considerato che, attualmente, un bonifico internazionale ha delle commissioni notevoli (anche oltre 50 dollari) e dei tempi di esecuzione elevati. Molti paesi stanno sperimentando soluzioni di pagamento istantaneo e stanno provando a connettere i loro sistemi per effettuare pagamenti tra gli stati (Tailandia e Singapore, ad esempio, hanno collegato i loro due sistemi di pagamento istantaneo nel 2021, anche se è da notare che questi due strumenti non implicano l'utilizzo della tecnologia blockchain, ma sono organizzati attraverso una rete di banche, tra cui quella centrale). Tuttavia, sempre più istituzioni stanno sperimentando tecnologie DLT (la stessa banca centrale di Singapore sta considerando di aggiungere funzionalità basate su questa tecnologia nel suo sistema di pagamento

¹²⁸<https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/accelerating%20winds%20of%20change%20in%20global%20payments/2020-mckinsey-global-payments-report-vf.pdf>

¹²⁹<https://www.ecb.europa.eu/press/key/date/2021/html/ecb.sp210615~05b32c4e55.en.html>

istantaneo), tra cui anche la *Society for Worldwide Interbank Financial Communication* (SWIFT), attraverso la quale vengono effettuati la maggior parte dei bonifici internazionali; anche delle compagnie di gestione dei pagamenti quali Mastercard e Visa stanno analizzando questi metodi e stanno approfondendo la possibilità di effettuare transazioni utilizzando le stablecoin, con MasterCard che ha annunciato a metà 2021 una partnership con Circle, la principale società emittente di USD Coin (Einchengreen, 2021). Circle, tra l'altro, a metà giugno ha lanciato sul mercato la sua stablecoin ancorata al prezzo dell'euro e completamente collaterizzata, denominata Euro Coin¹³⁰.

3.2.4 ULTERIORI RISCHI DELL'ADOZIONE DI UNA MONETA DIGITALE

In questo contesto possiamo apprezzare come diverse società private stiano provando a fare ciò che si potrebbe fare tramite l'utilizzo delle monete emesse dalla banca centrale, accelerando il processo decisionale delle banche stesse. Le istituzioni centrali stanno analizzando i costi e i benefici di un'eventuale adozione della tecnologia e delle sue applicazioni, con particolare riguardo ad eventi potenzialmente distruttivi che potrebbero verificarsi passando ad un sistema di pagamento digitale: se è vero che i benefici potrebbero essere molteplici, come abbiamo visto precedentemente nel paragrafo, un down del sistema elettronico potrebbe avere conseguenze gravissime, poiché se venissero bloccati i pagamenti la popolazione non avrebbe modo di effettuare transazioni nemmeno per i beni essenziali; così come potrebbe essere molto grave un eventuale attacco hacker andato a buon fine, e visto che i grandi exchange sono spesso le vittime predilette, è lecito aspettarsi un trattamento simile nei confronti delle CBDCs, visti gli enormi volumi che

¹³⁰ <https://cointelegraph.com/news/circle-launches-euro-backed-stablecoin-euroc>

esse avrebbero e le difficoltà delle istituzioni nel controllare un sistema di tale portata. Infine, si potrebbero aggiungere degli ulteriori costi “nascosti” per le banche commerciali: con lo sviluppo di una moneta digitale emessa direttamente dalla banca centrale e direttamente fruibile dagli utenti, qualora i tassi d’interesse applicati ai conti correnti dalle banche siano bassi o comunque assimilabili a quelli della banca centrale (come accade in questo momento storico), gli individui potrebbero logicamente preferire il deposito di fondi nell’istituzione centrale, in quanto intrinsecamente più sicura, o, nel caso in cui sopraggiungano difficoltà economiche per una banca commerciale, i correntisti avrebbero interesse a spostare tutti i loro fondi nella banca centrale (Einchengreen, 2021). Questi problemi sono tutt’altro che banali, e spiegano il perché le banche centrali di tutto il mondo siano caute sull’argomento e si stiano interrogando sulle regolamentazioni da attuare per sfruttare a pieno la tecnologia senza causare delle crisi di grosse dimensioni, che potrebbero facilmente avvenire qualora si verificasse una delle situazioni appena descritte; inoltre, vi è la necessità di intervenire piuttosto rapidamente, poiché l’emissione continua di stablecoin private potrebbe portare ad un incremento dei rischi finanziari e della volatilità dei mercati e, ammesso che queste monete digitali vengano sempre più utilizzate a discapito dei contanti, trovare il giusto equilibrio tra l’emissione pubblica e privata risulta fondamentale, perché il solo utilizzo massiccio delle stablecoin private potrebbe minare la stabilità del sistema finanziario qualora esse dovessero perdere l’equivalenza con la valuta fiat. Anche i regolamentatori dovranno seguire da vicino questo cambiamento, in quanto il regime regolatorio risulterà fondamentale per l’adozione della tecnologia e dovrà progredire sulla base della popolarità e dell’utilizzo che si farà di questo strumento, di modo da sostenerne lo

sviluppo garantendo un buon livello di sicurezza per i cittadini e per la tenuta del sistema monetario (Bolt, 2022).

3.2.5 IMPATTO DELLE CBDC SUL CONTESTO ECONOMICO

La letteratura recente si sta arricchendo di studi che hanno l'obiettivo di tentare di spiegare meglio o di prevedere gli impatti che potrebbe avere l'emissione di una CBDC sull'economia di uno stato, con l'obiettivo di aiutare l'arduo processo decisionale delle banche e di dare una visione globale ai regolamentatori; a tal proposito, Chen et al (2022) hanno redatto un articolo che si propone di dare una spiegazione riguardo all'ipotetico impatto di una moneta digitale sull'inflazione e sulla stabilità finanziaria. Per misurare questo impatto, gli autori si sono basati sulla storia economica e su come i diversi fattori abbiano contribuito nel tempo a dei cambiamenti nel contesto economico, in particolare analizzando la crescita dell'innovazione in campo finanziario, di cui le CBDC sono un ottimo esempio. Gli autori hanno usato la regola di McCallum, regola che, nella politica monetaria, esprime un valore obiettivo per la base monetaria delle banche centrali, usando come parametro, tra gli altri, anche una misura della "velocità" della moneta, intesa come una misura di quanto spesso un'unità di moneta venga utilizzata per comprare un bene in un determinato periodo di tempo, e in generale degli indicatori riguardo la crescita monetaria. Questo parametro di misura della velocità risulta importante nel contesto di nostro interesse poiché l'emissione di una moneta digitale comporterebbe un forte aumento dello stesso. A giudicare dai risultati ottenuti utilizzando sia con la regola di McCallum, sia analizzando degli eventi assimilabili all'emissione di una moneta digitale accaduti in diversi periodi storici, gli autori non trovano evidenze sul fatto che

l'emissione farebbe necessariamente aumentare l'inflazione, anche se permangono dei dubbi sull'impatto delle monete sulla stabilità finanziaria e sulla veridicità delle informazioni ottenute basandosi sui dati di quanto è accaduto nella storia, essendo questo nuovo strumento potenzialmente differente da quanto apprezzato in periodi precedenti.

Un'altra ricerca molto recente ed interessante sul tema, ci viene fornita da Castren et al (2022); nel paper, gli autori descrivono uno scenario in cui una banca centrale decida di emettere la sua moneta, provocando uno shock iniziale sul mercato, che sostanzialmente consiste nel passaggio dei depositi delle famiglie e delle aziende dalle banche commerciali alla banca centrale. Come abbiamo infatti già accennato precedentemente, la possibilità da parte di tutti di investire in depositi presso la banca centrale potrebbe causare dei problemi di scarsità di depositi nelle banche commerciali, o provocare una corsa agli sportelli qualora una di queste banche si trovasse in condizioni di difficoltà.

Per sviluppare la loro ricerca, gli autori immaginano di inserire una moneta digitale nel contesto macroeconomico, che viene qui inteso come un insieme di collegamenti bilaterali tra i principali settori istituzionali; così facendo definiscono dieci settori principali, tra i quali troviamo, ad esempio, le famiglie, i fondi d'investimento, le banche centrali, le banche commerciali e il resto del mondo. Basandosi su dati aggregati della zona Euro, si ipotizza che l'iniziale lancio della moneta digitale al tempo $t=0$ crei un prelievo del 20% dei depositi posseduti dalle famiglie e dalle aziende dalle banche commerciali dove essi sono detenuti; successivamente, al tempo $t=1$, si ha il reinvestimento dei suddetti fondi presso la banca centrale, per finanziare l'acquisto della moneta digitale. Infine, al tempo $t=2$, abbiamo questo cambiamento nei bilanci delle banche, e si possono presentare alternativamente quattro scenari (scelti dagli autori e che

non ricoprono esaustivamente tutte le possibili combinazioni, ma servono per dare un quadro complessivo abbastanza esauriente):

- ❖ Scenario 1: la banca centrale deposita nuovamente i fondi ricevuti presso le banche commerciali, diminuendo le sue passività;
- ❖ Scenario 2: le banche commerciali vendono obbligazioni (asset) alla banca centrale che le acquista (diminuendo così le sue passività, nel mentre aumentano quelle delle banche commerciali);
- ❖ Scenario 3: le banche commerciali riscattano dei prestiti per contrastare la riduzione delle passività, costringendo i settori che vedono mancare il finanziamento bancario ad emettere direttamente delle obbligazioni, le quali verranno acquistate dalla banca centrale per diminuire le passività;
- ❖ Scenario 4: le banche commerciali emettono delle obbligazioni con l'intento di contrastare la diminuzione delle proprie passività; la banca centrale acquista le obbligazioni emesse.

Come risultato di tutte queste operazioni, lo stato patrimoniale della banca centrale si espande, mentre quello delle banche commerciali rimane uguale (negli scenari 1 e 4), oppure diminuisce (negli scenari 2 e 3). Ogni scenario comporta delle conseguenze per tutta la struttura macroeconomica analizzata: se guardiamo alla carenza di finanziamento, solo il primo scenario garantisce che non ci siano carenze dei finanziamenti e ciò accade solo qualora la banca centrale depositi tutti i fondi ricevuti dalle banche commerciali; il quarto scenario, nonostante sia simile da un punto di vista di risultati a bilancio, potrebbe causare difficoltà a finanziarsi per i piccoli istituti che non possiedono abbastanza garanzie o per gli istituti più rischiosi, perché le obbligazioni presentano maggiori costi per banche in difficoltà economica, dato che per raccogliere capitali dovranno pagare ai

finanziatori tassi di interesse maggiori. Se analizziamo gli scenari 2 e 3 sotto questo punto di vista, ci accorgiamo che in questi casi le banche commerciali trasferiscono questa carenza di finanziamento ad altri settori, creando potenzialmente dei seri scompensi nei finanziamenti all'aumentare della quantità di obbligazioni vendute o di prestiti richiamati; inoltre, si deve tener presente che molte imprese, qualora non possano ottenere finanziamenti dalle banche, non sono in grado di accedere liberamente al mercato del credito, e anche quelle in grado di farlo sono molto influenzate dalle condizioni macroeconomiche presenti. In ultimo, ma non meno importante, vi è da segnalare il fatto che il mercato delle obbligazioni europeo è decisamente meno sviluppato di quello americano e solitamente l'emissione di obbligazioni avviene da parte di grandi aziende che sono però presenti in numero limitato.

Dopo esserci soffermati sulla carenza dei finanziamenti, è interessante anche approfondire come l'emissione di una moneta digitale della banca centrale possa influenzare e condizionare la struttura macroeconomica; per fare ciò, ci viene sempre in aiuto la ricerca effettuata da Castren et al (2022), dove gli autori identificano dieci settori istituzionali e li immaginano come dei nodi che interagiscono tra loro nel contesto macroeconomico della società. Per analizzare il cambiamento di ogni settore nel sistema, viene introdotta una misura di centralità, misura che aiuta a quantificare le variazioni che avvengono nella struttura e che sono scatenate dall'emissione della CBDC, quantificando la posizione di un dato nodo nella rete e fornendoci spunti utili alla nostra analisi in base alla variazione da prima a dopo l'emissione (in passato questa variabile è stata utilizzata, ad esempio, per analizzare gli effetti della crisi globale del mercato interbancario). Quantificando quindi quanto un nodo risulti "vicino" agli altri presenti nella rete e di quanto si sposti dopo l'emissione della moneta, si possono trarre indicazioni

sull'importanza relativa di ogni settore. Per fare ciò prendiamo in analisi il primo scenario, che è quello più semplice da un punto di vista di fattori economici in gioco e dal punto di vista delle banche commerciali. Simulando lo shock iniziale attraverso lo spostamento dei depositi dalle banche commerciali a quella centrale, possiamo notare che, ad avvenuta emissione della moneta digitale (al tempo $t=1$), la centralità della banca centrale aumenta notevolmente, a discapito di quella delle banche commerciali che subisce invece un decremento; successivamente, al tempo $t=2$, la banca centrale restituisce i fondi alle banche commerciali, ma si può notare che la misura della centralità non torna ai valori premissione: il settore delle banche commerciali, anche nello scenario a lui più favorevole, non mantiene la stessa centralità nel sistema. Di conseguenza, possiamo affermare che l'emissione di una moneta digitale della banca centrale, anche nello scenario più conservativo possibile, cambia l'importanza relativa dei vari settori istituzionali all'interno del sistema; ovviamente questo effetto è tanto più accentuato quanto più alto è il trasferimento iniziale di fondi dalle banche commerciali a quella centrale.

La stessa analisi può essere effettuata se immaginiamo che la moneta digitale non sia emessa da una banca centrale ma sia una classica stablecoin, emessa da un'azienda privata. In tal caso, possiamo sempre prevedere che si verificherà uno degli scenari descritti, ma la sostanziale differenza è che qui i fondi non si spostano dalle banche commerciali verso quella centrale, ma si spostano verso l'azienda emittitrice, portando quindi il settore di cui l'azienda fa parte ad accrescere la propria centralità nel sistema. Inoltre, va considerato il fatto che l'azienda privata potrebbe non avere gli incentivi ad effettuare un ribilanciamento dei fondi ricevuti nello stesso modo della banca centrale: ad esempio, nel primo scenario, non è detto che qualora l'azienda decidesse di restituire i

depositi alle banche li distribuisca tra esse proporzionalmente ai prelievi subiti inizialmente. Di contro, essendo un'azienda privata, se essa decidesse di ribilanciare i suoi conti solamente attraverso l'acquisto di titoli poco rischiosi ed assimilabili a denaro (quali, ad esempio, bond governativi a breve termine), questi titoli salirebbero di prezzo, mentre scenderebbero quelli delle aziende, contribuendo ad aumentare la volatilità del mercato. Negli scenari analizzati precedentemente, essendo l'attore principale la banca centrale, si assume che agisca a sostegno delle banche commerciali, in un'ottica di salvaguardia dell'intero sistema e degli interessi della collettività; questo non è scontato accada qualora l'emittente sia un'azienda, a meno che non la si obblighi adottando delle adeguate regolamentazioni in materia.

3.2.6 LA SITUAZIONE ATTUALE NEL MONDO

Le banche centrali di tutto il mondo si stanno quindi interrogando se sia necessario o meno emettere una moneta digitale, anche se al momento poche di queste istituzioni hanno provveduto a rilasciarne ufficialmente. Da questo punto di vista, l'Asia sta accelerando i discorsi rispetto al resto del mondo: il primo esperimento per collegare CBDCs basate su tecnologia blockchain è avvenuto tra Thailandia e Hong Kong a fine 2021; la divisione della banca che si occupa di coordinare gli sforzi in materia di innovazione (Bank for International Settlements Innovation Hub) ha sede a Singapore e la Cina sta seriamente analizzando l'emissione della propria valuta digitale, candidandosi ad essere la prima grande nazione ad emettere una valuta digitale (Eichengreen et al, 2021).

In ultimo, è interessante analizzare quali sono le banche centrali che hanno già provveduto a lanciare una moneta digitale, e per farlo ci viene in aiuto un report di PWC¹³¹ uscito nel mese di aprile 2022 che tratta appunto delle CBDCs nel mondo. Il report distingue tra CBDCs “al dettaglio” e “all’ingrosso”; tra le wholesale (che, ricordiamo, sono le monete emesse per essere utilizzate per effettuare transazioni tra istituzioni finanziarie), quelle più sviluppate sono il sopracitato progetto congiunto tra Thailandia e Hong Kong, che ha l’intento di continuare lo sviluppo di un prototipo proof-of-concept che faciliti pagamenti internazionali istantanei basati su tecnologia DLT e che ha recentemente coinvolto anche la banca centrale degli Emirati Arabi Uniti e una divisione specifica della People’s Bank cinese e il progetto denominato “Dunbar”, portato avanti dalla Monetary Authority of Singapore (MAS) in collaborazione con altre banche centrali, con l’intento di permettere alle banche commerciali di effettuare transazioni tra di loro utilizzando CBDCs delle rispettive nazioni, eliminando gli intermediari e riducendo i tempi e i costi delle transazioni oltre confine.

Tra le altre nazioni, nelle Americhe il Canada sta approfondendo le ricerche e portando avanti collaborazioni internazionali in materia, anche se al momento non ha ancora definito un piano per il rilascio della sua valuta digitale; in Europa la Francia ha lanciato nove differenti esperimenti per analizzare il rapporto tra rischi e benefici di un’implementazione di una wholesale CBDC e la Banque de France è convinta che l’utilizzo di questa moneta basata su tecnologia blockchain potrebbe avere efficacia nell’accelerare gli accordi di sicurezza per le transazioni internazionali tra diverse valute.

¹³¹ <https://www.pwc.com/gx/en/news-room/press-releases/2022/pwc-cbdc-global-index-2022.html>

Per quanto concerne invece le retail CBDCs, la nazione con uno dei progetti più sviluppati risulta la Nigeria; nell'ottobre 2021 è stata la prima nazione africana ad emettere una CBDC, chiamata eNaira. La Central Bank of Nigeria ha lanciato la moneta digitale per migliorare l'ecosistema di pagamento esistente ed aumentare l'inclusione finanziaria, una problematica di non poco conto per il paese africano. La valuta digitale è stata concepita con un approccio ibrido (un misto tra direct retail e indirect retail); dal lancio della valuta sono stati creati 700000 wallet digitali e sono state effettuate più di 35000 transazioni, di cui oltre il 90% sono transazioni effettuate tra persone e aziende o viceversa (dati aggiornati a dicembre 2021). La Nigeria non è stata però la prima nazione ad emettere la propria valuta digitale: il primato spetta infatti alle Bahamas con il loro Sand Dollar; l'obiettivo di questo progetto è quello di migliorare l'efficienza del sistema di pagamento attraverso il miglioramento della sicurezza e della velocità delle transazioni, aumentando allo stesso tempo l'inclusione finanziaria. Tutti i residenti hanno accesso al proprio portafoglio digitale tramite un'applicazione da installare sul proprio dispositivo mobile oppure tramite una carta fisica di pagamento.

Nel 2020, la Cina continentale è stata la prima grande economia mondiale a lanciare un progetto pilota riguardo le CBDCs. La People's Bank of China ha stretto accordi con molte banche commerciali possedute da altri stati e con compagnie di telecomunicazione al fine di testare i progetti nell'ambito di interesse e a marzo 2022 i piloti risultano attivi in 12 città, tra le quali Pechino e Shanghai. Anche il Digital Yuan (nome con cui si identifica la valuta digitale cinese) è pensato come una retail CBDC "ibrida": la banca centrale emette la stablecoin e la trasferisce direttamente alle banche commerciali le quali si occupano della distribuzione al pubblico. Dalla partenza dei progetti sono già stati creati oltre 260 milioni di portafogli digitali, con oltre 13 miliardi di dollari di transazioni

effettuate e una platea sperimentale sempre più vasta: durante i giochi olimpici invernali del 2022 è stata data la possibilità di acquistare e utilizzare il Digital Yuan anche ai turisti presenti, e in quei giorni sono state registrate transazioni per oltre 300000 dollari al giorno.

Per quanto riguarda l'Asia, altre nazioni ad aver iniziato lo sviluppo e dei test sulle monete digitali emesse dalla banca centrale sono la Thailandia e la Corea del Sud; nelle Americhe troviamo invece la Jamaica (che ha annunciato ufficialmente che lancerà la sua moneta digitale nel corso dell'anno) e i Caraibi Orientali. La Nigeria fa eccezione nel continente africano, in quanto non vi sono altre nazioni che siano pronte a lanciare la propria valuta digitale.

Se volgiamo invece il nostro sguardo al continente europeo, tra le nazioni che più stanno vagliando l'ipotesi di dotarsi di una CBDC troviamo l'Ucraina e la Svezia. Per quanto riguarda la prima, nel dicembre 2021 il Ministro per la Transizione Digitale aveva annunciato delle partnership con dei settori privati per iniziare i test per una moneta elettronica di stato basata su tecnologia blockchain e chiamata e-hryvnia; la situazione ha probabilmente subito uno stallo dovuto allo scoppio del conflitto con la vicina Russia. In Svezia invece, si sta analizzando la possibilità di emettere la propria moneta digitale per rimpiazzare Swish, un'applicazione per pagamenti digitali sviluppata da sei banche svedesi. Nel 2022 la Riksbank (che aveva iniziato il progetto pilota per l'e-krona già nel 2017) sta continuando ad investigare il bisogno e gli effetti di una moneta digitale sull'economia svedese; l'obiettivo di questa nuova moneta sarebbe quello di incrementare la sicurezza e l'efficienza delle transazioni elettroniche che nella nazione occupano già una posizione dominante (solo il 10% delle transazioni in Svezia avviene per contanti).

Per concludere, è giusto citare un paio di altri progetti in ambito CBDC, in quanto risultano rilevanti in termini di dimensione nonostante siano ancora in fase embrionale. Le nazioni a cui guardiamo in questo caso sono gli Stati Uniti d'America e l'Unione Europea (intesa come l'agglomerato degli stati che ne fanno parte e che adottano la moneta unica). Negli Stati Uniti d'America nel marzo 2022 è stato rilasciato un ordine esecutivo che esprime il volere di investigare approfonditamente il design e lo sviluppo di una moneta digitale di stato con la massima urgenza, elencando anche i molti benefit che questa scelta potrebbe portare. Al momento non è stata presa alcuna decisione ufficiale, ma l'ordine esecutivo impone a regolatori e autorità di rilasciare un report congiunto sui potenziali impatti della moneta entro e non oltre 180 giorni.

Nell'Unione Europea la BCE ha iniziato nell'ottobre 2021 un'investigazione riguardo un euro digitale, avvalendosi di numerosi professionisti provenienti dall'industria dei pagamenti; al momento anche l'UE non ha previsto ufficialmente il lancio della valuta digitale, ma, entro la fine del 2023, è previsto il lancio di una seconda fase di sperimentazione della durata di tre anni, che prevede lo sviluppo e il test delle soluzioni tecnologiche essenziali per l'emissione dell'euro digitale.

Come si è potuto capire, la situazione è in continuo divenire e una molteplicità di nazioni sta seriamente analizzando i costi, i benefici e i rischi dovuti all'utilizzo di questa nuova tecnologia. L'Asia sta investendo pesantemente nella tecnologia, ma, in accordo con quanto detto da Eichengreen (2021), permangono ancora molte incertezze riguardo le stablecoin, e nonostante le aziende private emittenti stiano cercando di aumentare la protezione nei confronti dei consumatori (in un futuro, le aziende saranno obbligate a detenere il 100% del valore della moneta a collaterale?), rimangono dubbi riguardo la stabilità del sistema e i vuoti normativi che le autorità per la supervisione finanziaria

dovranno tentare di colmare. Inoltre, si dovrà capire se veramente le CBDCs potranno essere la soluzione cercata in ambito finanziario, risultando efficaci nel ridurre i costi e nel velocizzare i pagamenti rispetto alle tecnologie presenti e non basate sulla blockchain e incrementando l'interoperabilità tra sistemi di diverse nazioni aventi diverse valute.

Al momento non sappiamo se questa tecnologia porterà la rivoluzione che potenzialmente potrebbe, ma, a giudicare dal comportamento e dall'attitudine delle diverse nazioni verso la tecnologia (Cina in primis), la sensazione è che non ci vorrà troppo tempo per scoprirlo.

CONCLUSIONE

La tecnologia blockchain ha gettato le basi per quella che potrebbe essere una vera rivoluzione in molti settori industriali, in primis nel settore finanziario, che è quello di maggior interesse di questo scritto. Abbiamo accennato a come la tecnologia abbia già subito diversi cambiamenti dalla sua nascita (su tutti, si pensi ai meccanismi di consenso e alla loro efficienza) e di come tutte le applicazioni stiano progredendo velocemente, anche quelle che non vengono trattate esplicitamente in questa sede ma che sono essenziali come supporto a diversi processi industriali (soprattutto in ambito gestione della supply chain e transizione verso l'IoT).

Dopo aver offerto una panoramica sul funzionamento della tecnologia ed aver analizzato quelle che al momento sono le due blockchain più grandi e utilizzate (Bitcoin ed Ethereum), nel secondo capitolo si è parlato di ICOs, facendo riferimento soprattutto ai fattori che hanno contribuito a rendere popolare questa operazione e alle differenze che si presentano rispetto agli altri metodi di finanziamento. Dall'analisi è emerso che questa operazione è stata particolarmente apprezzata in quanto ha avuto costi di finanziamento significativamente inferiori a tutte le altre metodologie di raccolta di fondi e maggiore semplicità; infatti, l'emissione di un token è un'operazione semplice per un programmatore, e, nel momento del boom del 2018, le regolamentazioni all'operazione erano pressoché inesistenti, così come i documenti obbligatori, semplificando notevolmente la richiesta di finanziamento da parte degli imprenditori. L'unico documento quasi sempre prodotto dalle aziende per approcciarsi a questa operazione è il white paper, che non viene però emesso per assolvere ad obblighi legali, quanto piuttosto per convincere gli investitori della bontà del progetto e svolgere una funzione di marketing. Difatti, il marketing si è mostrato una parte essenziale della campagna, in

quanto si è visto che le discussioni riguardo l'ICO sui social network e un white paper specifico e ben strutturato siano due elementi fondamentali per raggiungere il successo cercato in termini di fondi. Si è notato anche come questa operazione non abbia preso piede ovunque allo stesso modo, ma si sia localizzata soprattutto in quei paesi dove la tecnologia blockchain ha avuto più risalto fin dagli albori e dove si potevano trovare delle regolamentazioni (non particolarmente articolate), perché gli investitori possedevano un grado di protezione più alto (anche se si è visto che, per un investitore, il rischio di essere truffato partecipando ad una ICO è nettamente maggiore rispetto a tutti gli altri metodi di finanziamento, e ciò è dovuto in primis alla mancanza di regolamentazioni stringenti e alle forti asimmetrie informative presenti in un mercato a così alto contenuto tecnologico).

Nell'ultimo capitolo si è inizialmente fatto un focus sulle stablecoin, analizzando il ruolo fondamentale che esse svolgano nella raccolta di capitali nel mercato delle criptovalute e nelle operazioni di trasferimento di valore tra gli exchange; nell'approfondire questo tipo di asset è emerso come ci sia una differenza di rischiosità tra le varie stablecoin, e come avvenimenti avversi in un prodotto percepito come relativamente sicuro dagli investitori possano scatenare il panico sul mercato. A tal proposito sono state fatte considerazioni anche riguardo alla volatilità che potrebbe essere trasferita ai mercati finanziari, poiché queste monete sono emesse da aziende private e, nella maggior parte dei casi, hanno a collaterale degli asset "reali" negoziati su una borsa valori e quindi, in caso di un ulteriore aumento dei volumi di scambio e degli investimenti in questo prodotto e qualora si verificasse un evento estremo potrebbero esserci serie ripercussioni anche sull'economia reale. Di fatto, i regolamentatori si stanno accorgendo di questi rischi, anche grazie agli ultimi movimenti concitati nel mercato delle criptovalute, e stanno studiando delle soluzioni di intervento.

In ultimo, si è volto lo sguardo alle Central Bank Digital Currency, un particolare tipo di stablecoin caratterizzato dal fatto di essere emesso da una banca centrale, e di essere quindi sostanzialmente equivalente ad una valuta fiat. Questo tipo di moneta digitale è una delle applicazioni che, a mio avviso, risulta più interessante e che potrebbe maggiormente condizionare la vita di tutti i cittadini già nel breve periodo; infatti, alcune nazioni con economie di dimensioni poco rilevanti, hanno già provveduto a rilasciare questo tipo di asset con ottimi risultati, sia in termini di efficienza dei pagamenti che di inclusione finanziaria. È vero che al momento nessuna grande nazione ha ufficialmente adottato una valuta digitale emessa da una banca centrale, ma la Cina ha fatto partire un progetto pilota in diverse città e gli Stati Uniti e l'Unione Europea stanno valutando i costi e i benefici derivanti dall'adozioni di queste monete e i danni che una mancata emissione potrebbe comportare al sistema economico qualora le società di gestione dei pagamenti decidessero comunque di utilizzare la tecnologia attraverso l'uso di stablecoin emesse da aziende private. Nell'elaborato si è cercato di spiegare, attraverso l'analisi di alcune ricerche scientifiche molto recenti, l'impatto che queste monete digitali potrebbero avere sulla struttura macroeconomica di uno stato e dei vantaggi che potrebbero avere i cittadini dall'utilizzo della tecnologia, soprattutto in termini di sicurezza, di contrasto all'illegalità e di inclusione finanziaria, considerato che, per la popolazione avente redditi bassi, non è scontato l'accesso ai sistemi di pagamento digitale presenti al momento sul mercato. Inoltre, i cittadini e gli stessi stati potrebbero avere dei vantaggi monetari e di efficienza nei pagamenti internazionali, considerato che al momento essi sono caratterizzati da commissioni sostanziose e da tempi di esecuzione molto elevati se paragonati ai pagamenti istantanei.

A mio parere, questo strumento verrà utilizzato in un futuro abbastanza prossimo, in quanto le banche centrali, per conservare la sovranità monetaria e minimizzare l'effetto sostituzione, saranno praticamente obbligate a rilasciare questo asset, soprattutto nel caso in cui una potenza economica come la Cina decidesse di adottare una CBDC come valuta a corso legale.

In ogni caso i rischi derivanti dall'adozione di un sistema di pagamento totalmente digitale basato su tecnologia blockchain non sono nulli, ed eventuali anomalie devono essere analizzate in anticipo per evitare di andare in contro a crisi sistemiche che porterebbero sicuramente molti danni all'economia reale. I benefici al momento sembrano comunque prevalere sulle criticità, e per vedere se sarà effettivamente così e se si andrà verso una gestione dei pagamenti nazionali e internazionali utilizzando le CBDCs e la tecnologia blockchain non ci resta che attendere le decisioni delle banche centrali maggiori al mondo, che saranno chiamate a pronunciarsi su un tema che potrebbe portare, in non troppo tempo, ad una rivoluzione in ambito finanziario, condizionando la vita di tutti i cittadini.

BIBLIOGRAFIA

Ahern D. (2021), *Regulatory Lag, Regulatory Friction and Regulatory Transition as FinTech Disenablers: Calibrating an EU Response to the Regulatory Sandbox Phenomenon*, *European Business Organization Law Review*, 22:395–432.

Ahmad M.F., Kowalewski O., Pisany P. (2020), *What determines initial coin offering success: a cross-country study*, *IÉSEG working paper series 2020*.

Ante L., Fiedler I., Strehle E. (2021), *The impact of transparent money flows: Effects of stablecoin transfers on the returns and trading volume of Bitcoin*, *Technological Forecasting and Social Change*, 170.

Balani N., Hathi R., *Enterprise Blockchain A Definitive Handbook*, a. 2017, ISBN 1973336871.

Bellavitis C., Fisch C., Wiklund J. (2021), *A comprehensive review of the global development of initial coin offerings (ICOs) and their regulation*, *Journal of Business Insights*, 15.

Bolt W., Lubbersen V., Wierst P., (2022), *Getting the Balance Right: Crypto, Stablecoin and CBDC*, *De Nederlandsche Bank Working Paper No. 736*.

Bullmann D., Klemm J., Pinna A. (2019), *In search for stability in crypto-assets: are stablecoins the solution?*, *ECB Occas Paper Series 230*, 1–53.

Campino J., Brochado A., Rosa A. (2022), *Initial coin offerings (ICOs): Why do they succeed?*, *Financial Innovation*, 8:17.

Carboni D., *Dagli Smart Contract alle ICO*, a. 2017, ISBN 1976775027.

Castren O., Kavonius I. K., Rancan M., (2022), *Digital currencies in financial networks*, *Journal of Financial Stability*, 60.

Catalini C., Gans J.S. (2018), *Initial Coin Offerings and the Value of Crypto Tokens*, *National Bureau of Economic Research, Working Paper No. 24418*.

Chen H., Siklos P. L., (2022), *Central bank digital currency: A review and some macro-financial implications*, *Journal of Financial Stability*, 60.

Chiap G., Ranalli J., Bianchi R., *Blockchain – tecnologia e applicazioni per il business*. *Ulrico Hoepli Editore, a. 2019*.

De Filippi P., Collomb A., Sok K. (2019), *Blockchain Technology and Financial Regulation: A Risk-Based Approach to the Regulation of ICOs*, *European Journal of Risk Regulation*, *Cambridge University Press*.

Eichengreen B., Viswanath-Natraj G. (2021), *Stablecoins and Central Bank Digital Currencies: Policy and Regulatory Challenges*, *Asian Economic Papers*, 21, 1.

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

Florysiak D., Schandlbauer A. (2022), *Experts or charlatans? ICO analysts and white paper informativeness*, *Journal of Banking and Finance*, 139.

Gates M., *Ethereum*, *Wise Fox Publishing, a. 2017*.

Griffin J. M., Shams A. (2019), *Is Bitcoin Really Untethered?*, *The Journal of Finance*, 85, 4.

Gupta M., *Blockchain for the Enterprise*, *a. 2018, ASIN B07B2PR63V*.

Hoang L. T., Baur D. G. (2020), *How stable are stablecoin?*, *SSRN Electronic Journal*.

Howell S.T., Niessner M., Yermack D. (2019), *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, *The Review of Financial Studies*, v 33, n 9.

Huang W., Meoli M., Vismara S. (2019), *The geography of initial coin offerings*, *Small Business Economy*, 55:77-102.

Ivashchenko, A., Polishchuk, Ye., & Britchenko, I. (2018), *Implementation of ICO European best practices by SMEs*, *Economic Annals-XXI*, 169(1-2), 67-71.

Jaggi H., Jha R., *Blockchain Scalability Interoperability Bane-to-Boon*, a. 2021, ASIN B08XB5LQ2N.

Jalan A., Matkovskyy R., Yarovaya L. (2021), *“Shiny” crypto assets: A systemic look at gold-backed cryptocurrencies during the COVID-19 pandemic*, *International Review of Financial Analysis*, 78.

Kristoufek L. (2021), *Tethered, or Untethered? On the interplay between stablecoins and major cryptoassets*, *Finance Research Letters*, 43.

Kristoufek L. (2022), *On the role of stablecoins in cryptoasset pricing dynamics*, *Financial Innovation*, 8, 27.

Lambert T., Liebau D., Roosenboom P. (2021), *Security Token Offering*, *Small Business Economy*.

Momtaz P.P. (2019), *Token Sales and Initial Coin Offerings: Introduction*, *The Journal of Alternative Investments*, 21, 7–12.

Momtaz P.P. (2020), *Initial Coin Offerings*, *PLoS ONE* 15.

Roosenboom P., Kolk T.V., Jong A.D. (2020), *What determines success in initial coin offerings?. Venture Capital*

Schuckes M., Gutmann T. (2020), *Why do startups pursue initial coin offerings (ICOs)? The role of economic drivers and social identity on funding choice*, *Small Business Economy*, 57, 1027-1052.

Takashima I., *Ethereum – The Ultimate Guide to the World*, a. 2017, ASIN B07651GQ2W.

Taylor T.J., *Criptovalute: La guida completa per guadagnare con la moneta digitale*, a. 2021, ASIN B08ZYBZ5HK.

SITOGRAFIA

<https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>

<https://it.cointelegraph.com/news/ethereum-s-vitalik-buterin-blasts-centralized-crypto-exchanges-i-hope-they-burn-in-hell>

<https://www.hedgewithcrypto.com/cryptocurrency-exchange-hacks/>

<https://bebeez.it/fintech/e-crypto-com-il-re-degli-sponsor-dello-sport-ecco-la-mappa-delle-maggior-sponsorship-crypto-nel-settore/>

<https://academy.bit2me.com/it/51-attacco-bitcoin/>

<https://bitinfocharts.com/comparison/bitcoin-hashrate.html#3y>

<https://www.treccani.it/enciclopedia/ fiat-money/>

<https://www.ilsole24ore.com/art/bitcoin-el-salvador-prim-o-paese-ad-adottarlo-come-valuta-legale-AExYt8g>

<https://www.wisdomtree.eu/it-it/blog/2021-07-06/ethereum-a-deconstruction-of-crypto-supply>

<https://tether.to/en/transparency/#reports>

<https://coinmarketcap.com/currencies/tether/>

<https://coinmarketcap.com/currencies/bitcoin/>

<https://www.ilsole24ore.com/art/i-bitcoin-emessi-sono-90percento-totale-circa-20percento-e-sparito-sempre-AETWwp4>

<https://www.ilsole24ore.com/art/bitcoin-sara-l-oro-digitale-prospettive-e-limiti-ADERWWOB>

<https://it.cointelegraph.com/news/unconfirmed-transactions-on-bitcoin-network-at-highest-level-since-2017>

<https://www-statista-com.ezproxy.biblio.polito.it/statistics/1200477/bitcoin-mining-by-country/>

<https://www-statista-com.ezproxy.biblio.polito.it/statistics/731416/market-share-of-mining-pools/>

<https://www.ilsole24ore.com/art/kazakhstan-proteste-spaventano-miners-criptovalute-AEnwAX6>

https://www.repubblica.it/esteri/2021/07/22/news/cina_usa_texas_minatori_miniere_bitcoin_migrazione_fuga_bitmain_bit_mining_criptovalute-311328018/

<https://lab24.ilsole24ore.com/green-generation/bitcoin-brucia-l-energia-un-intero-paese-ecco-quanto-e-perche-consuma.php#>

<https://www-statista-com.ezproxy.biblio.polito.it/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/>

<https://academy.youngplatform.com/criptovalute/ethereum-ico/#5>

<https://ethereum.org/it/dapps/#what-are-dapps>

<https://www.open.online/2021/01/11/usa-amazon-parler-offline/>

<https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/>

<https://ethereum.org/it/upgrades/shard-chains/>

<https://academy.bit2me.com/it/che-cosa-%C3%A8-erc-20-token/>

https://www.huffingtonpost.it/entry/terrorismo-riciclaggio-e-frodi-il-lato-oscuro-dei-bitcoin_it_61dde54be4b04b42ab8647c0/

https://www.diritto.it/valute-virtuali-e-normativa-antiriciclaggio/#_ftn5

https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

<https://coinmarketcap.com/charts/>

<https://medium.com/galaxy-digital-research/contextualized-analysis-of-bitcoin-drawdowns-f4717ff8e3be>

<https://investire.biz/articoli/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-cos-il-peg-nella-defi>

<https://it.cointelegraph.com/news/terra-peg-mechanism-in-doubt-as-ust-crashes-to-67-cents>

<https://coinmarketcap.com/>

https://www.pwc.com/ee/et/publications/pub/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf

<https://icobench.com/stats>

<https://www.reply.com/it/content/si-conclude-con-successo-la-prima-fase-della-sperimentazione-per-l-emissione-e-la-gestione-di-security-token>

<https://www.blockchain4innovation.it/esperti/tokenizzazione-degli-asset-scenari-e-sfide/>

<https://it.cointelegraph.com/news/ieos-icos-stos-and-now-idos-how-to-raise-funds-for-crypto-in-2019>

<https://corporatefinanceinstitute.com/resources/knowledge/deals/overallotment-greenshoe-option-ipo/>

<https://academy.youngplatform.com/criptoconomia/ico-storia-criptoalute/>

<https://coinmarketcap.com/it/currencies/omni/>

<https://cryptonomist.ch/blog/marketing/2020/04/25/strumenti-marketing-blockchain/>

<https://it.cointelegraph.com/explained/can-bitcoins-hard-cap-of-21-million-be-changed>

<https://coinmarketcap.com/alexandria/glossary/soft-cap>

<https://academy.bit2me.com/it/que-es-basic-attention-token-bat/>

<https://it.cointelegraph.com/news/eos-about-to-secure-a-record-4-bln-in-year-long-ico>

<https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets>

<https://www.econometrics-with-r.org/11-2-palr.html>

https://psychology.fandom.com/wiki/Masculinity_index

<https://www.cqfluency.com/cqpedia/uncertainty-avoidance-index/>

<https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/ICOs-the-new-IPOs.pdf>

<https://www.firstonline.info/aramco-e-non-solo-le-10-ipo-piu-grandi-di-sempre-ce-unitaliana/>

<https://www.borsaitaliana.it/notizie/sotto-la-lente/lagreenshoe.htm>

<https://www.consob.it/web/investor-education/crowdfunding>

https://www.crowdfundme.it/wpcontent/uploads/2021/04/CFM_Taxcoach_guida_agevo_lazioni_fiscali_Startup_PMI_2021.pdf

<https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate>

<https://icodrops.com/eos/>

<https://www.criptoaluta.it/eos>

<https://eos.io/>

<https://academy.bit2me.com/it/que-es-eos-criptomoneda/>

<https://coinmarketcap.com/currencies/eos/>

<https://invezz.com/it/notizie/2021/09/03/21-account-pompato-eos-ico-attraverso-wash-trading/>

<https://decrypt.co/53950/the-10-biggest-icos-heres-where-the-money-went>

<https://it.cointelegraph.com/news/breaking-us-sec-deems-17-billion-telegram-offering-illegal-orders-halt>

<https://it.cointelegraph.com/news/breaking-telegram-abandons-telegram-open-network-and-gram-tokens>

<https://coinmarketcap.com/it/currencies/toncoin/>

<https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate>

<https://www.criptoaluta24.com/tezos/>

<https://decrypt.co/40413/tezos-agrees-to-pay-25-million-in-damages-to-investors>

<https://coinmarketcap.com/it/currencies/tezos/>

<https://www.coingecko.com/en/exchanges>

<https://it.cointelegraph.com/news/bitfinex-hack-recovery-spurs-crypto-community-responses>

<https://coinmarketcap.com/currencies/unus-sed-leo/>

<https://fullycrypto.com/dragon-coin-the-floating-casino-ico-that-stole-24-million>

<https://icobench.com/stats>

<https://blog.osservatori.net/hubfs/Report%20-%20Blockchain%20&%20Distributed%20Ledger--2022-.pdf>

<https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf>

https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

<https://www.bitfinex.com/wp-2019-05.pdf>

https://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/12117302-78b0-4e6e-80c4-d3af7db0fdae

<https://tayros.bg/index.php/2022/03/15/la-regolamentazione-di-security-token-offering-sto-ico-blockchain-e-smart-contract-in-italia-lapproccio-consob/>

https://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/12117302-78b0-4e6e-80c4-d3af7db0fdae

https://www.researchgate.net/publication/329096171_Token_Sales_and_Initial_Coin_Offerings_Introduction

<https://www.borsaitaliana.it/borsa/glossario/bookbuilding.html>

<https://www.coindesk.com/tech/2021/12/16/how-stablecoins-merge-traditional-and-decentralized-finance/>

<https://www.terra.money/>

<https://coinmarketcap.com/currencies/terrausd/>

<https://cryptoeccetera.com/cose-terra-luna-guida-a-terra-money/>

https://www.hwupgrade.it/news/web/terra-luna-e-la-stablecoin-algoritmica-ust-ecco-cosa-e-successo_107113.html

<https://medium.com/alessandro-omega/formazione-del-luna-foundation-guard-lfg-14eba11481bd>

<https://it.cointelegraph.com/news/kwontitative-easing-btc-price-hits-43k-in-ust-as-terra-empties-2-2b-bitcoin-bag>

<https://it.cointelegraph.com/news/do-kwon-proposes-terra-hard-fork-to-save-ecosystem>

<https://it.cointelegraph.com/news/investors-dumping-on-terra-as-luna-2-tanks-70-in-two-days>

<https://www.wallstreetitalia.com/usdt-il-panico-mette-in-crisi-il-peg-di-tether/>

https://www.repubblica.it/economia/affari-e-finanza/2022/05/30/news/il_buco_da_40_miliardi_di_luna_apre_nuove_crepe_nelle_stablecoin-351440635/

<https://www.protocol.com/bulletins/crypto-firm-celsius-stops-withdrawals>

<https://coinmarketcap.com/>

<https://crypto.com/eea/earn>

<https://www.investopedia.com/terms/c/commercialpaper.asp>

<https://www.bloomberg.com/news/articles/2022-05-19/tether-declares-fall-in-commercial-paper-increase-in-treasuries>

<https://tether.to/en/transparency/#reports>

https://www.hwupgrade.it/news/web/terra-luna-e-la-stablecoin-algoritmica-ust-ecco-cosa-e-successo_107113.html

<https://medium.com/alessandro-omega/formazione-del-luna-foundation-guard-lfg-14eba11481bd>

<https://it.cointelegraph.com/news/kwontitative-easing-btc-price-hits-43k-in-ust-as-terra-empties-2-2b-bitcoin-bag>

<https://it.cointelegraph.com/news/do-kwon-proposes-terra-hard-fork-to-save-ecosystem>

<https://it.cointelegraph.com/news/investors-dumping-on-terra-as-luna-2-tanks-70-in-two-days>

<https://www.wallstreetitalia.com/usdt-il-panico-mette-in-crisi-il-peg-di-tether/>

https://www.repubblica.it/economia/affari-e-finanza/2022/05/30/news/il_buco_da_40_miliardi_di_luna_apre_nuove_crepe_nelle_stablecoin-351440635/

<https://www.protocol.com/bulletins/crypto-firm-celsius-stops-withdrawals>

<https://coinmarketcap.com/>

<https://crypto.com/eea/earn>

<https://www.investopedia.com/terms/c/commercialpaper.asp>

<https://www.bloomberg.com/news/articles/2022-05-19/tether-declares-fall-in-commercial-paper-increase-in-treasuries>

<https://tether.to/en/transparency/#reports>

FONTI FIGURE

Figura 1: <https://www.criptoinvestire.com/come-funziona-la-crittografia-nelle-blockchain.html>

Figura 2: <https://it.cointelegraph.com/news/bitcoin-network-now-8-times-more-powerful-than-it-was-at-20k-price>

Figura 3: <https://blog.bitnovo.com/it/cose-lo-staking-di-criptoalute/>

Figura 4: <https://subscription.packtpub.com/book/big-data-&-business-intelligence/9781788473040/8/ch08lv11sec53/token-versus-coin>

Figura 5: <https://coinmarketcap.com/currencies/bitcoin/>

Figura 6: <https://www.tuttocrypto.it/trilemma/>

Figura 7: <https://academy.bit2me.com/it/tipi-di-blocchi-in-blockchain/>

Figura 8: <https://zipmex.com/learn/what-is-lightning-network/>

Figura 9: <https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P>

Figura 10: <https://theguardian.com/decentralized-autonomous-organizations-daos-regulating-through-company-laws/>

Figura 11: <https://www.digitalocean.com/community/tutorials/understanding-database-sharding>

Figura 12: <https://coinmarketcap.com/charts/>

Figura 13: <https://coinmarketcap.com/charts/>

Figura 14: <https://constkogan.medium.com/the-howey-test-the-fine-line-between-a-security-token-and-a-utility-token-2e28194b0cdf>

Figura 15: <https://medium.com/okex-blog/ieo-vs-ico-what-are-the-differences-f0a700bb9a5c>

Figura 16: <https://constkogan.medium.com/the-howey-test-the-fine-line-between-a-security-token-and-a-utility-token-2e28194b0cdf>

Figura 17: <https://doi.org/10.1371/journal.pone.0233018.t001>

Figura 18:

https://www.pwc.com/ee/et/publications/pub/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf

Figura 19: <https://doi.org/10.1016/j.jbvi.2020.e00213>

Figura 20:

https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf

Figura 21: <https://doi.org/10.1007/s11187-019-00135-y>

Figura 22: <https://doi.org/10.1007/s11187-019-00135-y>

Figura 23: <https://blog.osservatori.net/hubfs/Report%20-%20Blockchain%20&%20Distributed%20Ledger--2022-.pdf>

Figura 24: <https://blog.osservatori.net/hubfs/Report%20-%20Blockchain%20&%20Distributed%20Ledger--2022-.pdf>

Figura 25: <https://101blockchains.com/stablecoins/>

Figura 26: <https://www.coinbureau.com/review/terra-luna/>

Figura 27: <https://coinmarketcap.com/>

Figura 28: <https://beincrypto.com/tether-mints-three-billion-usdt-past-two-weeks/>

