TESI DI LAUREA TRIENNALE IN ECONOMIA E MANAGEMENT

CATTEDRA DI FINANZA AZIENDALE

Blockchain e Venture Capital

Come i Venture Capital possono sfruttare la blockchain per dare slancio all'innovazione

RELATORE:

Prof. Roberto Mazzei

CANDIDATO:

Giovanni Sammartino

Matricola: 259571

Anno Accademico: 2022/2023

ABSTRACT

Come si può aumentare ed incentivare lo slancio innovativo sfruttando le nuove tecnologie?

In questo elaborato, suddiviso in quattro capitoli, vengono analizzati e studiati sia gli attori che si occupano comunemente di agevolare ed incentivare il processo innovativo, sia le nuove tecnologie la cui adozione può permettere di incrementare i risultati odierni.

Si illustrerà come la blockchain è in grado di fornire gli strumenti applicativi essenziali per rinnovare e velocizzare il processo di crescita delle start-up innovative e allo stesso tempo permettere la raccolta di capitali presso investitori retail e non solo istituzionali attraverso il meccanismo della tokenizzazione di asset illiquidi.

Non si tratterà direttamente il mondo delle criptovalute, intese come asset finanziari digitali, ma solamente il loro corrispettivo informatico ovvero i ‘’token’’*, “un indicatore univoco registrato in un registro condiviso, con funzione di rappresentare un oggetto digitale, di certificare la proprietà di un bene o di consentire l'accesso a un servizio”*[1], come mezzo applicativo.

Nel primo capitolo viene trattato il contesto generale in cui operano i Venture Capital, ovvero la tipologia di operatori presenti nel mercato che effettuano cospicui investimenti per finanziare le società che apportano comunemente soluzioni innovative: le Start-up. Vengono pertanto descritti il funzionamento di un VC ed il suo processo di investimento, le strategie di remunerazione e le metriche osservate nella fase di screening delle start-up. È riportata un’analisi dei contribuiti non monetari che i VC apportano alle proprie partecipate e del processo di due diligence dagli stessi svolto. Infine, il capitolo si conclude con un richiamo al mondo del Private Equity visto anche come una delle alternative di exit per una Start-up vincente.

Nel secondo capitolo viene invece descritto il funzionamento delle blockchain riportando le caratteristiche principali e le basi da dover conoscere per poter adoperare correttamente ed autonomamente questa particolare tecnologia. Vengono riportati approfondimenti riguardo il meccanismo operativo, i sistemi di sicurezza, gli algoritmi di consenso sia in un contesto

[1] Definizione “token” Enciclopedia Treccani: https://www.treccani.it/enciclopedia/token/#:~:text=In%20informatica%2C%20termine%20con%20cui,l%27accesso%20a%20un%20servizio.

generale sia in riferimento alle due principali blockchain ad oggi esistenti: Bitcoin ed Ethereum. Il capitolo ha inoltre un intento esplicativo per far luce sul vero potenziale che questa tecnologia può offrire per rispondere al quesito iniziale. Il capitolo si conclude con l'analisi e la descrizione delle applicazioni decentralizzate e degli smart contract, due strumenti cardine per permettere l'utilizzo delle blockchain per finanziare progetti innovativi.

Il terzo capitolo è il capitolo fulcro dell'elaborato, all'interno di esso viene descritto, analizzato e osservato da vari punti di vista il meccanismo che consente il passaggio dal mondo reale al mondo virtuale on-chain. La tokenizzazione di asset reali è una realtà che si sta affermando in questi anni e prenderà spazio molto rapidamente nel corso di questo decennio. Stime di istituzioni riconosciute in tutto il mondo, come Boston Consulting Group e le più importanti banche di investimento, prevedono una crescita talmente repentina da poter arrivare a sbloccare un valore complessivo degli asset tokenizzati superiore all'intera capitalizzazione del mercato azionario americano entro il 2030. Infine, viene presentato il MiCA, ovvero la più recente regolamentazione in merito al mondo delle criptovalute approvata dal Consiglio Europeo il 16 maggio 2023, e gli obblighi introdotti per rendere il panorama crypto più sicuro ed affidabile per gli investitori.

Nel quarto ed ultimo capitolo vengono analizzati due diversi case study: il primo, su The DAO, incentrato su avvenimenti passati che hanno condizionato lo sviluppo del mondo blockchain evidenziando i principali punti di fragilità ed i relativi insegnamenti; il secondo, su Seed Venture, che prende in considerazione una start-up italiana impegnata ed attiva nell'ambito della tokenizzazione di quote di partecipazione delle piccole società innovative.

L'ultimo paragrafo presenta un breve excursus sui possibili sviluppi futuri sottolineando come la regolamentazione avrà un ruolo chiave nell'indirizzare lo sviluppo di simili soluzioni[2].

[2] Le fonti per gli approfondimenti teorici e tecnici sono tratte da paper scientifici di università ed istituzioni; per il quarto capitolo le informazioni sul secondo case study sono state raccolte attraverso interviste dirette con la società oggetto del di studio.

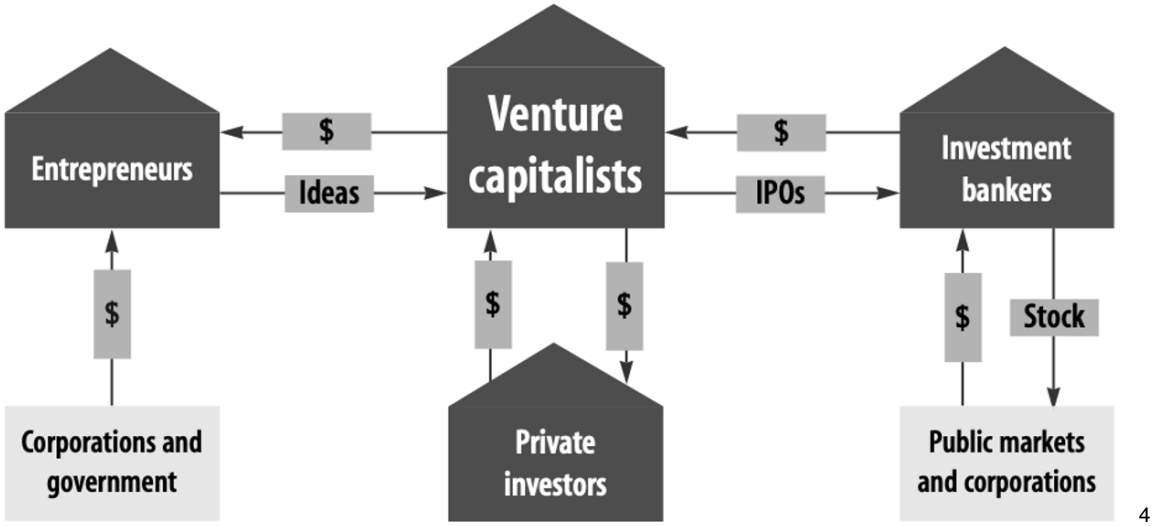
1. VENTURE CAPITAL

1.1. Come funziona un Venture Capital

Con il termine Venture Capital si indicano *''attività di investimento istituzionale in capitale di rischio di aziende non quotate, in fase di start up, caratterizzate da un elevato potenziale di sviluppo"* [3].Si tratta perciò di capitali di investimento destinati ad essere collocati in attività ad alto rischio, come il finanziamento di una start up innovativa, che promettono o quantomeno prospettano un alto rendimento e un ritorno sull'investimento elevato in un arco di tempo medio.

Le società di Venture Capital raccolgono fondi da una varietà di investitori, ricercano le imprese promettenti e le aiutano a crescere. I soggetti che pongono in essere questo tipo di azioni sono detti Venture Capitalist e hanno come obiettivo quello di massimizzare il rendimento attraverso l'investimento in società in fase di sviluppo con un alto potenziale di crescita che perciò, per loro natura, rappresentano un asset altamente rischioso. Gli altri attori che popolano il mondo dei Venture Capital sono fondamentalmente tre:

- Gli imprenditori: che hanno bisogno di fondi e sono in cerca di capitali e finanziamenti
- Gli investitori: che cercano alti rendimenti e profitti in attività ad alto rischio
- Le banche di investimento: in cerca di nuove opportunità e società da poter vendere



[4]

[3] Definizione "Venture Capital" Borsa Italiana

[4] *"How Venture Capital Works",'* Bob Zider - Harvard Business Review-1998

La sfida principale per i Venture Capital è quella di identificare gli imprenditori che possono far avanzare una tecnologia chiave in una certa fase per poi poter vendere la società oppure quotarla in borsa. Come sostiene Bob Zider, autore del paper "How Venture Capital Works" (Harvard Business Review-1998), nell'omonimo documento, si può dire che i Venture Capital investano in buone industrie che, per essere tali, presentano maggiori possibili tassi di crescita e, di conseguenza, di remunerazione di un investimento. Ciò che conta perciò, piuttosto che l'idea, è il settore o industria di appartenenza della società in cui il Venture Capital vuole investire.

In cambio del finanziamento di 2-3 anni dall'avvio di un'azienda un Venture Capital si aspetta un ritorno del capitale 10 volte superiore in un lasso di tempo di circa 5 anni. Il guadagno principale di un Venture Capital risiede nell'apprezzamento del valore della singola società o del portafoglio di società a cui ha concesso finanziamenti detenendo una partecipazione di circa il 20/30%. La quantità di denaro che ogni partner riceve è perciò una funzione della crescita totale del valore del portafoglio e della quantità di denaro gestito per partner. Come detto l'attività dei Venture Capitalist è estremamente rischiosa in quanto le probabilità che le società in cui investono ottengano la crescita desiderata è ottimisticamente di 1/10. Vi sono molte componenti fondamentali per il successo di un'azienda dove per ognuna di esse una buona azienda potrebbe avere una probabilità di successo dell'80%. La probabilità combinata di successo, anche con queste prospettive ottimistiche, è solo del 17% e scende fino al 10% nel caso in cui anche solo una di queste variabili avesse il 50% di possibilità di successo. Chiaramente ad un Venture Capital non occorre che tutte le società in cui investe abbiano successo e diventino grandi aziende, ma basta che solo il 10-20% di esse diventi un vero vincitore per raggiungere il tasso di rendimento target del 25-30%. [5]

Per proteggersi dal rischio i Venture Capital intervengono direttamente nei processi di gestione e nelle scelte che le singole società effettuano avendo nei confronti di esse un notevole potere contrattuale. Inoltre, genericamente vi è un investitore ''lead'' e diversi ''follower'': i VC preferiscono avere 2 o 3 gruppi coinvolti nella maggior parte delle fasi di finanziamento per non limitarsi ad essere gli unici investitori assorbendo in tal modo tutto il

[5] *"How Venture Capital Works''* Bob Zider - Harvard Business Review - 1998

rischio dell'operazione. Riducono inoltre il carico di lavoro dei propri partner coinvolgendo altri nella valutazione dei rischi durante il periodo di due diligence (tema che verrà approfondito nel paragrafo 1.3).

Per migliorare l'efficacia delle proprie valutazioni e per tenere sotto controllo i rischi a cui si sottopongono, i Venture Capital non forniscono interamente il denaro di cui una società ha bisogno ma ad ogni stadio di crescita offrono il quantitativo necessario per raggiungere lo stadio di sviluppo successivo ottenendo un certo grado di specializzazione relativo allo stadio in cui intendono investire (pre-seed, seed, early stage e successivi round di finanziamenti). Questo meccanismo giova ad entrambe le parti in quanto ai Venture Capital conviene arginare i rischi esponendo solo un quantitativo limitato di capitale legato alla fase in cui intervengono, dall'altra parte gli imprenditori e founder delle start-up mirano ad ottenere il capitale in fasi diverse in modo da non diluire eccessivamente le quote e per cedere un quantitativo limitato di partecipazioni in ogni round di finanziamento grazie alla crescita delle valutazioni pre e post-money.

Per capire meglio come funziona questo sistema bisogna comprendere in che modo una start-up ottiene accesso al capitale; i Venture Capital offrono liquidità e denaro circolante in cambio di una partecipazione all'interno della società in cui intendono investire. La quantità di denaro fornito, corrispondente ad una determinata percentuale di quote della società, determina la valutazione e quindi il valore della società stessa. La prima valutazione, detta pre-money, può avere come riferimento alcuni parametri o proprietà aziendali, come ad esempio un brevetto, oppure essere fatta dal Venture Capital stesso che determina la quantità di denaro da investire, ad esempio 100.000€, a fronte di una determinata quota della società, ad esempio pari al 5%. A seguito di questo finanziamento la valutazione finale, anche detta post-money, della società sarà pari a 2.000.000 di euro. In questo momento il Venture Capital ha limitato la sua esposizione di capitale fornendo la liquidità necessaria alla start-up per portare a termine la prima fase di sviluppo. Nel round di finanziamento successivo, pari ad esempio a 500.000€, il Venture Capital chiederà come contropartita un ulteriore quota di partecipazione, sempre pari ad esempio al 5%; la valutazione post-money, a seguito del secondo round sarà perciò pari a 10.000.000 di euro.

Dividendo in due round il finanziamento di cui necessitava, la start-up ha potuto vendere una partecipazione complessiva del 10%, quota che sarebbe stata notevolmente maggiore qualora

avesse ottenuto gli investimenti in un unico round, che gli ha concesso di arrivare ad una valutazione finale di 10 milioni di euro.

Se avesse, invece, chiesto il finanziamento tutto in un unico round la sua valutazione finale sarebbe stata di solamente 6 milioni (600.000€ a fronte del 10% di quote). Allo stesso tempo il Venture Capital ha ridotto il rischio dell'operazione e, qualora vi fosse un acquirente disposto a comprare la società, potrebbe liquidare una partecipazione del 10% dal valore di 1 milione di euro a fronte di un investimento complessivo di 600.000€.

Come introdotto precedentemente, i Venture Capitalist non sono investitori passivi, non si limitano perciò ad osservare la maturazione del proprio investimento, e tendono a specializzarsi nei settori in cui vogliono investire, prediligendo industrie difficilmente valutabili dall'esterno e sottoponendo a stretto monitoraggio le start-up.

Tuttavia, il ruolo di un Venture Capital è ben più ampio: offrono alle start-up consigli utili, supporto nelle decisioni e nella scelta del team manageriale e forniscono loro contatti personali e opportunità di networking. Questi concetti verranno approfonditi successivamente nel paragrafo 1.3.

Questo genere di attività comporta vantaggi e rischi per entrambe le parti coinvolte e non solo per i Venture Capital che decidono di investire in attività estremamente rischiose il proprio capitale; da un lato le start-up ricevono denaro liquido da poter utilizzare per espandere il proprio business e le proprie attività, dall'altro, però, cedono una parte della proprietà vincolandosi perciò alla partecipazione dei Venture Capital alle decisioni aziendali sia strategiche che operative e accettando dei limiti imposti dai propri investitori. Inoltre, le start-up dovranno impegnarsi nel crescere rapidamente e generare profitti stabili e crescenti, nonché significativi, per soddisfare le attese degli investitori e remunerare il loro finanziamento per poter avere accesso ai nuovi round di finanziamento e mantenere alta la fiducia nei propri confronti.

Nonostante i rischi, più o meno grandi, in cui entrambe le controparti possono incorrere, il legame tra start-up e Venture Capital risulta essere vincente e nel lungo periodo sembra essere il connubio ideale per la creazione di una realtà aziendale di successo destinata non solo ad ottenere alti profitti ma ad avere un impatto reale sull'economia.

A riguardo sono stati effettuati diversi studi negli anni e come dimostrano Gornall e Strebulaev nel paper *"The economic impact of Venture Capital: evidence from public companies"* [6], delle cinque più grandi società quotate per capitalizzazione di mercato all'epoca degli studi (in ordine: Apple, Google, Berkshire Hathaway, Microsoft ed Exxon Mobil), ben tre hanno ottenuto finanziamenti da Venture Capital nella fase iniziale di sviluppo (Apple, Google e Microsoft). Ciò che risulta essere stupefacente, oltre la dimensione raggiunta, è l'impatto reale che le aziende finanziate da fondi di Venture Capital hanno avuto sull'economia. I dati al 2015 sono impressionanti considerando che si tratta di risultati sottostimati in quanto solo le "public companies" divulgano tutti i dati necessari e gran parte delle società finanziate da Venture Capital finiscono per essere acquisite da altri operatori e non quotate sul mercato. Gli studi di Gornall e Strebulaev (2015) indicano che *"nonostante la giovane età dell'industria dei venture capital, le società quotate finanziate da Venture Capital forniscono lavoro a 4 milioni di persone, impattano per un quinto della capitalizzazione di mercato e per il 44% degli investimenti in ricerca e sviluppo negli Stati Uniti"* [7].

Ulteriori studi evidenziano l'importanza del mondo dei Venture Capital, in particolare Astrid Romain e Bruno van Pottelsberghe (Université Libre de Bruxelles) nel paper *''The Economic Impact of Venture Capital"* [8], mostrano come il ''social rate of return'' delle attività dei Venture Capital sia nettamente maggiore rispetto a quello dei reparti di ricerca e sviluppo (R&D) di aziende sia private che pubbliche. Nello stesso documento viene dimostrato come i Venture Capital abbiano un effetto indiretto positivo sulla crescita della produttività incrementando l'elasticità degli output della ricerca e sviluppo; inoltre, un'elevata intensità delle attività dei Venture Capital rende più semplice assorbire le conoscenze generate da università ed imprese migliorando di conseguenza la performance economica aggregata.

[6] University of British Columbia, Stanford University e National Bureau of Economic Research - November 2015

[7] *''The economic impact of Venture Capital: evidence from public companies''*, W. Gornall, I.A. Strebulaev - University of British Columbia, Stanford University e National Bureau of Economic Research - November 2015

[8] Van Pottelsberghe de la Potterie, Bruno; Romain, Astrid (2004): The Economic Impact of Venture Capital, Discussion Paper Series 1, No. 2004,18, Deutsche Bundesbank, Frankfurt a. M.

1.2 Strategie di remunerazione di un VC e metriche di valutazione delle Start-up

In merito agli obiettivi e metodi di remunerazione esistono diverse strategie che un Venture Capital può porre in essere. Occorre specificare che non esiste un metodo migliore o più vantaggioso, né tantomeno un unico metodo in quanto ogni Venture Capital adotta e sceglie la strategia in base ai propri obiettivi e alle proprie necessità.

A livello generale l'obiettivo perseguito è quello della massimizzazione del profitto e del rendimento determinato dalla crescita del valore delle partecipazioni nelle società o start-up. Il mezzo attraverso cui viene incassato e monetizzato questo rendimento è la liquidazione della partecipazione ovvero la vendita delle quote che avviene genericamente tramite exit, come IPO o operazioni di M&A, o alle volte attraverso la cessione e vendita ad altri fondi di Venture Capital o Private Equity.

Gli obiettivi di remunerazione variano a seconda della fase in cui un fondo vuole entrare e tengono conto di alcune metriche di valutazione. Solitamente un Venture Capital non si pone degli obbiettivi specifici e non determina delle aspettative concrete in quanto investe in una fase ancora embrionale di sviluppo a differenza, ad esempio, di un fondo di Private Equity che interviene in una fase più avanzata e ha la possibilità di determinare delle aspettative plausibili.

Chiaramente, in termini di potenzialità di crescita e quindi di remunerazione, un Venture Capital ha maggiori margini a fronte, però, di un maggiore rischio. I rischi in cui un Venture Capital può incorrere sono legati al possibile fallimento della start-up in cui ha investito e perciò alla svalutazione delle partecipazioni iscritte a bilancio; inoltre, un ulteriore rischio, non di secondaria importanza, a cui un Venture Capital deve far fronte è legato alla responsabilità connessa alle azioni delle società partecipate, in quanto legalmente risulta esserne socio e partecipa all'approvazione dei bilanci.

Per far fronte a questi rischi vengono solitamente disposte alcune clausole negli accordi tra imprenditori e Venture Capital o, in alcuni casi, queste vengono previste direttamente all'interno degli statuti delle singole società. Una delle più comuni è la "put option" con la quale il Venture Capital si riserva il diritto di rivendere la propria partecipazione alla start-up per una cifra predeterminata. Si tratta di una clausola che assicura il Venture Capital dal rischio che la start-up possa mettere in atto operazioni illegittime, non corrette o volte a trasmettere informazioni

non veritiere che pregiudicherebbero il rapporto tra le due parti e potrebbero essere influenti anche riguardo la credibilità del fondo stesso.

Un altro meccanismo solitamente utilizzato è la verifica del team attraverso processi di "anti-money laundering" (AML), o riciclaggio di denaro, per scongiurare il rischio che nei rapporti ed esperienze passate dei founders vi siano delle associazioni o attività che possano, nel futuro, rivelarsi un problema non indifferente.

Per quanto riguarda le metriche che i Venture Capital adottano per valutare le proprie partecipate, ve ne sono diverse legate alla fase in cui avviene la valutazione e alla disponibilità di dati ed informazioni. Nelle fasi iniziali, ovvero quelle dove avvengono gli screening di tutte le società che cercano fondi da parte di Venture Capital, l'oggetto di valutazione è il team ed ogni singolo componente. Contemporaneamente viene osservato il mercato ed il settore in cui la start-up vuole avviare il proprio business.

Nelle fasi successive, ovvero quelle in cui le partecipate hanno superato diversi step di screening e di valutazione preliminari, si raccolgono i dati sulle operazioni svolte e si cerca di determinare e quantificare alcune metriche operative e finanziarie. Si cerca di valutare in primis degli aspetti legati al marketing e gli sviluppi raggiunti attraverso l'"AAARRR funnel", ovvero una serie di obiettivi che scremano man mano il mercato di riferimento cercando di ridimensionarlo il più possibile. Vengono valutati aspetti in termini di: (a) awareness, quantità di persone raggiunte; (b) acquisition, quante persone si interessano; (c) activation, quante persone eseguono l'azione desiderata (come una registrazione); (d) retention, quante persone ripercorrono gli step precedenti per la seconda volta; (e) revenue, quante persone si rendono disponibili a pagare; (f) referral, quante persone consigliano il prodotto o servizio proposto.

Questo percorso appena descritto ha come obiettivo quello di determinare e quantificare quelli che sono i clienti reali e quelli su cui fare maggior leva per espandere il business. In seguito a questo passaggio, o anche simultaneamente, vengono analizzate delle metriche da un punto di vista più finanziario; tra queste quelle più importanti sono: (a) MRR/ARR (monthly recurring revenue/annual recurring revenue), ovvero i redditi mensili o annuali ricorrenti per ottenere una proiezione del cash flow in entrata; (b) ACV/ARPU (average contract value/average revenue per user), ovvero la media dei guadagni provenienti rispettivamente dai contratti chiusi e dai clienti acquisiti; (c) CAC (customet acquisition cost), ovvero il costo sopportato dalla start-up per acquisire nuovi clienti, calcolato come totale delle spese di

marketing diviso il numero di nuovi utenti acquisti; (d) LTV (lifetime value), ovvero la media di ricavi che ci si può attendere da un cliente, ha bisogno di dati consistenti per ottenere una valutazione attendibile.

Queste ultime metriche servono alle imprese e ai Venture Capital per comprendere realisticamente quali sono i possibili ricavi e costi della società, in questo modo si può stimare il cash flow utile per avere una valutazione verosimile del valore della società.

1.3 Apporto non monetario e due diligence

Una caratteristica che determina il successo dei Venture Capital e che li contraddistingue come investitori è l'apporto non monetario che forniscono alle start-up. Con apporto non monetario si intendono tutte quelle attività, servizi e opportunità che un Venture Capitalist concede agli imprenditori dietro le società oggetto dei propri investimenti. Come anticipato nel paragrafo 1.1, tra queste spiccano come importanza il network di informazioni e contatti nonché il supporto nella scelta del team manageriale e delle nuove figure che le start-up dovranno acquisire per ampliare il proprio business e diventare una realtà affermata.

Tra la gamma di agevolazioni e servizi rientrano anche le strutture in cui avviare le prime attività, come uffici e magazzini, e i servizi tecnologici, come hardware e software. Si tratta di servizi che permettono, da un lato, alle start-up di risparmiare sui costi fissi che spesso in fase di avviamento di un'attività possono risultare gravosi e, dall'altro, ai Venture Capitalist di rimanere a stretto contatto e lavorare direttamente, all'interno dello stesso immobile, con le start-up e le società in cui hanno investito.

Dal punto di vista dei Venture capital queste agevolazioni risultano essere veri e propri investimenti in quanto richiedono sforzi organizzativi e spese di capitale alle volte non così inconsistenti. Tutto ciò permette, però, di creare dei veri e propri hub innovativi radunando nello stesso centro diverse start-up permettendo loro anche di collaborare e di "contaminare" le proprie idee condividendo soluzioni a problematiche comuni e ampliando di conseguenza il range e la portata di innovazione del Venture Capital. Questo sistema, sempre dal punto di vista dei Venture Capital, risulta efficace nell'attirare nuovi investitori e partner in fase di investimento nonché possibili acquirenti interessati alle operazioni di M&A.

Un ulteriore aspetto che riguarda i Venture Capital e che li distingue come investitori attivi è il modo in cui i Venture Capitalists spendono il proprio tempo.

Come detto le attività in cui son coinvolti e di cui si occupano indirettamente sono molteplici e pertanto solitamente la maggior parte dei propri sforzi, circa il 25%*, sono dedicati al monitoraggio attivo. La seconda attività i cui sono maggiormente coinvolti, a cui dedicano il 20%* del proprio tempo, è la selezione e reclutamento del management e dei nuovi membri del team. Subito dopo si comportano come consulenti, 15%* del tempo, e assistono le start-up nelle relazioni esterne per circa il 10%* del proprio tempo[9] .

In aggiunta la presenza di un Venture Capitalist dietro le attività aziendali e soprattutto alle decisioni strategiche può fungere da certificazione e garanzia per nuovi possibili investitori aiutando di conseguenza la start-up ad accedere più agevolmente a nuovi investimenti. Questo fenomeno in alcuni casi porta gli imprenditori e founder a preferire valutazioni inferiori e una minor quantità di denaro per essere affiancati a Venture Capital con una reputazione migliore[10] .

Un altro aspetto particolare riguarda l'"agency theory" dal cui punto di vista nella relazione Venture Capitalist - imprenditore il primo risulta essere il "principal" mentre il secondo l'"agent". Gli Agency problems che il Venture Capital si trova a dover affrontare durante tutta la durata di questo rapporto riguardano le asimmetrie informative (adverse Selection and moral hazard) e la separazione tra proprietà e controllo; quest'ultima risulterebbe essere particolarmente influente qualora vi fossero delle significative divergenze tra gli obiettivi delle due parti.

Tutte queste problematiche e i relativi rischi da essi derivanti vengono arginati e circoscritti attraverso una pratica comune nella prassi aziendale e finanziaria che può avere una profondità ed accuratezza variabili a seconda delle necessità: la due diligence.

Nella prassi finanziaria con l'espressione due diligente si intende "*Attività di acquisizione delle informazioni necessarie per la preparazione della documentazione richiesta dalla prassi operativa e dalla normativa in merito ad una operazione di emissione di strumenti finanziari."* [11]

---

[9] *''How Venture Capital works"*, Bob Zider - Harvard Business Review, 1998

[10] *"Value-adding and Monitoring Activities of Venture Capital: a Synthesis Literature Review"* – S. Ed-dafali, A. Chakir, B. Bouzahir -Research Journal of Finance and Accounting

[11] Definizione "Due Diligence" Borsa Italiana: https://www.borsaitaliana.it/borsa/glossario/due-diligence.html#:~:text=Glossario%20finanziario%20%2D%20Due%20Diligence&text=Attività%20di%20acquisizione%20delle%20informazioni,di%20emissione%20di%20strumenti%20finanziari

Solitamente è una fase importante e necessaria al centro delle operazioni di Mergers and Acquisitions (M&A) con la quale si pone particolare attenzione alla valutazione della società target oggetto di acquisizione e si controllano le attività che questa pone in essere in un arco di tempo variabile dalla durata media di alcuni mesi. È svolta da advisor, ovvero soggetti esperti preposti al controllo della realtà effettiva aziendale, presentati dal soggetto acquirente che controllano la veridicità, i limiti e i rischi di quanto riportato nei documenti presentati dalla controparte nelle fasi precedenti.

I parametri di maggior interesse che vengono osservati nella fase di due diligence sono: (a) parametri legali, (b) parametri fiscali con particolare attenzione alla compliance, (c) parametri contabili.

L'obiettivo principale di questa fase è ridurre le asimmetrie informative presenti tra venditore e compratore riducendo in tal modo anche le problematiche legate alla selezione avversa che un'operazione del genere può presentare. Inoltre, è compito di chi attua la fase di due diligence, presentare al mercato informazioni complete e veritiere, aspetto quest'ultimo di elevata importanza e delicatezza quando oggetto di acquisizione sono società quotate.

Per quanto riguarda il mondo delle start-up, la due diligence è un processo delicato e non di facile attuazione in quanto le informazioni necessarie per completare questo processo possono non essere affidabili o non essere presenti. Per questo motivo i Venture Capital si può dire attuino una due diligence continua interagendo direttamente con le start-up. Anche in questo caso esistono diversi tipi di due diligence legati necessariamente alla fase di sviluppo della nuova società.

Il primo avviene in una fase di screening in cui i Venture Capital si trovano a dover selezionare un numero limitato di start-up a cui concedere i finanziamenti durante il quale valutano l'idoneità della società secondo alcune componenti specifiche. I parametri a cui si fa riferimento in questa fase sono solitamente il team, il mercato, il prodotto, aspetti legali e finanziari e le aspettative di crescita nonché il contributo che il Venture Capital è consapevole di poter dare alle start-up. In aggiunta possono essere considerate anche le possibili strategie di exit.

Dopo aver superato la fase di screening, la start-up entra in una fase in cui viene posta sotto osservazione per un periodo di tempo più o meno lungo dalla durata media di almeno un mese. Durante questo periodo, in cui avviene la vera e propria due diligence, il Venture Capital per proprio conto e per conto dei propri partner determina una serie di metriche e documenti che

la start-up dovrà monitorare e condividere con i propri investitori. Tutti i dati raccolti verranno analizzati per determinare le vere potenzialità di crescita del business e per evidenziare i punti di forza e di debolezza. Le conclusioni verranno poi successivamente riportate e sintetizzate in un documento di rendicontazione finale noto come "due diligence report".

Al termine di questo processo investitori e imprenditore avranno modo di trarre le proprie conclusioni in merito alla start-up oggetto di valutazione, ciò potrebbe determinare il futuro della stessa marcando il punto di svolta verso una crescita futura supportata da un Venture Capital o verso una strada meno promettente che spesso conduce all'estinzione della società.

1.4. Private Equity

Con il termine Private Equity si indicano *"attività di investimento istituzionale in capitale di rischio di aziende non quotate caratterizzate da un elevato potenziale di sviluppo"* [12].

Si tratta perciò sempre di un'operazione finanziaria, molto simile alla realtà dei Venture Capital, che ha come obiettivo quello di fornire capitale di rischio (equity) proprio (private) a società già presenti ed operanti sul mercato. La differenza principale con i Venture Capital risiede nel target a cui viene destinato il capitale di rischio e nella fase in cui questo viene fornito alla società: i finanziamenti provenienti da Venture Capital sono destinati a società piccole o piccolissime, come start-up, con un alto potenziale innovativo e di crescita in una fase preliminare quando il business non è pienamente formato e deve essere ancora ben strutturato. I finanziamenti provenienti da Private Equity, invece, sono destinati a società medio-grandi con un proprio business e attività già avviate e consolidate con alle spalle uno storico di informazioni e risultati economico-finanziari.

Ciò che accomuna e rende per certi versi simili questi due mondi è l'apporto non monetario che esse forniscono alle società oggetto di investimento. Riprendendo quanto detto nel paragrafo precedente, anche nel Private Equity l'investimento non si esaurisce nel mero apporto di capitali in quanto alle società che ottengono i finanziamenti vengono destinate attività di supporto di vario genere, soprattutto in ambito manageriale.

[12] Definizione "Private Equity" Borsa Italiana: https://www.borsaitaliana.it/borsa/glossario/private-equity.html

L'obiettivo, anche in questo caso, è quello di ottenere alti rendimenti a fronte di un'elevata esposizione ai rischi, anche se nella fattispecie del Private Equity questi sono decisamente più contenuti dal momento che le società oggetto di investimento hanno un passato conosciuto e dei parametri economico finanziari misurabili.

L' investimento di capitali sotto forma di Private Equity non si limita ad essere un buon investimento, ma risulta essere indicativamente migliore rispetto all'investimento nel più grande indice di mercato azionario se si confrontano i rendimenti.

Lo studio condotto da Robert S. Harris, Tim Jenkinson e Steven N. Kaplan[13] e pubblicato nel paper *''Private Equity Performance: What do we know?''* [14] analizza e compara le performance di 1400 fondi di Private Equity, derivati dalle partecipazioni di più di 200 investitori istituzionali, rispetto all'indice S&P 500. Questo documento dimostra come i fondi di Private Equity hanno superato il più importante indice azionario in termini di performance, in media, per il 20-27% in totale lungo la vita del fondo e per più del 3% all'anno.

Harris, Jenkinson e Kaplan hanno basato i propri studi sull'analisi del ''public market equivalent'' (PME), metrica simile all' IRR/TIR (internal rate of return/tasso interno di rendimento) designata per poter comparare rendimenti dei fondi privati e quelli dei benchmark pubblici di riferimento. Questo multiplo indica che, al netto delle tasse, un PME di, ad esempio, 1,20 implica un guadagno netto finale, lungo la vita del fondo, del 20% maggiore rispetto a quello che si sarebbe potuto ottenere investendo lo stesso capitale per lo stesso tempo in un indice pubblico, come l'S&P 500.

In questo studio i tre autori dimostrano come, comparando l'IRR del fondo e quello dell'S&P 500, vi sia un eccesso di rendimento annualizzato positivo con un PME maggiore di 1, e un eccesso di rendimento annualizzato negativo con un PME minore di 1[15].

[13] Rispettivamente University of Virginia, Said Business School - Oxford University, University of Chicago and NBER
[14] Journal of Finance forthcoming, July 2013

[15] 'Private Equity Performance: What do we know?'', Journal of FInance forthcoming; Robert S. Harris, Tim Jenkinson, and Steven N. Kaplan - Luglio 2013)

2. BLOCKCHAIN

2.1 Blockchain: definizione e caratteristiche principali

La definizione di ‘’blockchain’’ varia a seconda del punto di vista o istituzione da cui viene interpretata, ad esempio da un punto di vista finanziario è vista come *“un paradigma tecnologico che permette di sviluppare applicazioni basate su un sistema decentralizzato di condivisione e validazione delle informazioni dalle numerose applicazioni.”* [16].

“Tecnologia basata su una catena di blocchi che registrano e gestiscono le operazioni contabili accessibili solo agli utenti di ciascun nodo, per assicurarne la tracciabilità.” [17]

“La blockchain rappresenta un particolare tipo di DLT. Nello specifico, si parla di blockchain perché le transazioni memorizzate sono raggruppate in una sequenza di “blocchi” collegati tra loro per via crittografica, creando così una registrazione in ordine cronologico e non modificabile di tutte le transazioni effettuate fino a quel momento.” [18]

Sebbene queste definizioni non differiscano eccessivamente l’una dall’atra, tutte toccano in maniera diretta dei punti che fanno tutti parte del concetto alla base di questa tecnologia, facendo emergere che non esiste una vera e propria definizione che metta insieme i molteplici punti di vista da cui viene trattata.

Volendo provare a fornire una definizione complessiva si può affermare che la blockchain sia una struttura dati condivisa, verificabile ed immutabile; un registro digitale le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico, la cui integrità è garantita dall’uso della crittografia e dove il consenso è distribuito su tutti i nodi della rete.

[16] Definizione “Blockchain” Borsa Italiana
[17] Definizione “Blockchain” Enciclopedia Treccani
[18] Comunicazione della Banca d’Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività - Banca d’Italia, giugno 2022

Le blockchain sono una famiglia facente parte di un sottoinsieme derivato dalle ‘’Distributed Ledger Technologies’’ (DLT) ovvero ‘*’libri mastri (o registri) elettronici, distribuiti geograficamente su un’ampia rete di nodi, i cui dati sono protetti da potenziali attacchi informatici grazie al fatto che le stesse informazioni sono ridondate, verificate e validate mediante l’adozione di diversi protocolli (o regole) comunemente accettati da ciascun partecipante.”* [19].

Ciò che differenzia la blockchain e più in generale le DLT è l’assenza di dipendenza e fiducia nei confronti di un unico operatore all’interno dell’ecosistema, questa caratteristica, che rende unica questa tipologia di tecnologie, è detta decentralizzazione. La blockchain, infatti, opera come un database distribuito in cui non vi è un unico punto nevralgico e centrale da cui dipende la sicurezza dell’intera rete, come invece accade nei database tradizionali in cui il network dipende da un solo computer/server. Ogni computer/utente all’interno dell’ecosistema blockchain è anche detto ‘’nodo’’ ovvero un dispositivo che partecipa alla rete e gestisce il software del protocollo su cui si basa l’intero network. Quest’ultimo consente di convalidare le transazioni e mantenere sicuro l’intero ecosistema. Ogni nodo ha lo stesso valore, uno vale uno, sono tra loro paritari, non vi sono criteri che determinano l’importanza, e sono tra loro in competizione. La peculiarità delle tecnologie e dei sistemi DLT risiede nella trasparenza e disponibilità di informazioni che vengono di fatto condivise tra tutti i nodi, i quali possiedono nello stesso momento una copia del database o registro condiviso; tutti i nodi possono consultarlo ma per modificarlo occorre l’approvazione della maggioranza di quelli attivi. Il modo in cui questo consenso democratico viene raggiunto varia a seconda della tipologia di blockchain e viene definito da uno specifico ‘’algoritmo di consenso’’.

Gli algoritmi di consenso sono vari e possono essere programmati arbitrariamente al momento della creazione di una blockchain o si può prevedere l’utilizzo di uno già esistente. Come detto ne esistono diversi ma quelli più comuni ed utilizzati sono essenzialmente due: (i) Proof of Work, o prova del lavoro, utilizzata da Bitcoin (nome della blockchain su cui viene scambiata bitcoin o BTC, la prima criptovaluta nonché quella più conosciuta e importante al mondo anche in termini di capitalizzazione di mercato); (ii) Proof of Stake, o prova della ‘’puntata’’/capitale, utilizzata da Ethereum (nome della blockchain su cui vengono scambiati gli

[19] Definizione ex MISE, attuale Ministero delle Imprese e del Made in Italy

ether o ETH, che presenta caratteristiche alternative rispetto a Bitcoin). Il funzionamento di questi due meccanismi di consenso verrà poi approfondito nei paragrafi successivi.

All'interno della famiglia Blockchain si possono individuare due grandi ramificazioni, due tipologie che si differenziano in base al modo in cui un attore può partecipare alla rete.

La prima tipologia è detta ''permissionless'', senza permesso, e sono quelle con cui più comunemente sono indicate le blockchain ispirate al network Bitcoin. In questa ramificazione chiunque può partecipare alla rete senza bisogno di una pre-approvazione, è necessario un digital asset nativo per il funzionamento (come i bitcoin per la rete Bitcoin) ed è prevista una governance democratica: chiunque può partecipare alla validazione delle informazioni. I benefit legati a questa tipologia risiedono nell'alto grado di decentralizzazione, elevata sicurezza e alla resistenza alla censura. Le problematiche che presenta sono, invece, legate maggiorente alla scalabilità e velocità di approvazione delle transazioni e al consumo energetico che queste richiedono in quanto un numero indefinito di nodi convergerà più difficilmente verso un unico consenso.

La seconda tipologia è detta ''permissioned'', con permesso, dove occorre registrarsi o essere pre-approvati da una o più entità centrali. In questo caso non è necessario che vi sia un digital asset nativo ed è prevista una governance elitaria: alla validazione delle informazioni partecipano solo attori designati e riconoscibili. Questa tipologia permette alte velocità e bassi costi di transazione a scapito però di una minore decentralizzazione in quanto sono solo alcuni nodi selezionati a dover convergere verso il consenso.

Una volta raggiunto il consenso, a prescindere dal tipo di rete, le informazioni vengono trascritte, crittografate ed archiviate all'interno di un blocco che getta le basi per la creazione di quello successivo. Questo meccanismo di archiviazione determina una concatenazione, possibilmente infinita, di blocchi, da cui il nome ''blockchain''. All'interno di ogni singolo blocco si possono trovare le informazioni riguardanti tutti i blocchi precedenti, in aggiunta alle nuove informazioni/transazioni validate, che non possono essere rimosse o modificate. L'unico modo attraverso cui questo meccanismo può essere alterato è riottenere il consenso per ogni blocco creato a partire da quello in cui è contenuta l'informazione che si vuole modificare dovendo perciò avere la complicità della maggioranza dei nodi attivi nella rete. Essendo network composti da un numero elevato di operatori, specialmente nelle blockchain permissionless,

ottenere questo tipo di consenso è quasi impossibile ed è per questo che la sicurezza della rete risulta essere maggiore rispetto ai database tradizionali.

2.1.1 Teoria dei giochi e problema dei generali bizantini

Il principio alla base del funzionamento delle blockchain è la teoria dei giochi, ovvero la branca della matematica che studia i modelli di interazione tra agenti razionali (giocatori) nonché le strategie che essi possono adoperare per ottenere la massimizzazione del proprio guadagno (payoff).

La teoria dei giochi mette in risalto l'esistenza di due tipi di interazione tra gli attori all'interno di un sistema: vi può essere un'interazione di carattere cooperativo o conflittuale, fermo restando che l'obiettivo ultimo di ogni giocatore è quello di massimizzare il proprio payoff.

L' interno meccanismo di funzionamento della blockchain si basa sul fornire incentivi e disincentivi agli operatori, nodi, a mettere in atto determinate azioni. L'incentivo risiede nella possibilità di ottenere un guadagno economico dall'agire secondo le regole, codificate all'interno di algoritmi, progettate per portare benefici all'intera rete senza porre in essere comportamenti che possano destabilizzare la stessa e metterne a rischio la sicurezza e l'integrità.

All'interno delle implicazioni della teorica dei giochi risiedono sia i punti di forza che la più grande vulnerabilità della tecnologia blockchain. La creazione di un nuovo blocco non contribuisce solamente a rendere più sicura e longeva l'intera catena, ma attribuisce ad ogni creatore, definito come "miner", una ricompensa economica sotto forma di valuta digitale, o criptovaluta, nativa della blockchain su cui si sta creando il blocco. I nodi sono perciò tra loro tutti in competizione, gareggiando per riuscire a risolvere ed ottenere la soluzione al problema matematico posto dall'algoritmo di consenso. Una volta trovata la soluzione a questo problema, attraverso calcoli complessi effettuati da un hardware specifico, il miner ottiene una ricompensa diretta, che l'algoritmo di consenso prevede come premio per aver risolto il problema matematico e aver creato il blocco, e una ricompensa indiretta, formata da delle commissioni per ogni transazione che viene validata ed archiviata all'interno del blocco appena creato. Questo meccanismo di ricompensa, dal valore direttamente proporzionale al valore della

criptovaluta, rappresenta l'incentivo che gli operatori hanno nell'operare correttamente rimanendo in costante competizione.

La più grande debolezza di questo sistema risiede nel comportamento scorretto e malevolo dei nodi e nel loro possibile atteggiamento collusivo volto ad arginare i meccanismi che regolano il funzionamento della rete, questo problema è anche definito come "problema dei generali bizantini".

Il problema dei generali bizantini è una delle metafore più note ed efficienti per comprendere quale sia la soluzione principale adottata dalla tecnologia blockchain ad uno dei problemi che persiste maggiormente all'interno dei sistemi informatici distribuiti. Il problema alla base riguarda la capacità di utenti all'interno della stessa rete di poter comunicare tra di loro in maniera limitata raggiungendo un obiettivo comune senza mettere a rischio l'intera rete. Il punto focale di questa problematica riguarda la presenza, statisticamente probabile e pertanto presumibile come certa, di attori malevoli che agiscano per trarre benefici personali a scapito degli altri operatori.

La metafora dei generali bizantini è stata teorizzata nel 1982 da tre matematici statunitensi esperti di informatica e registri distribuiti, e riguarda la storia di un esercito, al cui comando vi sono diversi generali, che sta assediando una città nemica con lo scopo di conquistarla. I generali, situati tutti in diversi punti strategici, non hanno la possibilità di comunicare tra di loro se non attraverso lo scambio di messaggi diretti con i quali devono accordarsi per scegliere il momento più opportuno per agire. Ogni generale, nell'inviare e nel ricevere messaggi, si pone il problema del verificare che questi non arrivino a, o prevengano da un generale corrotto o traditore che abbia quindi l'intenzione di minare la riuscita del piano. Per risolvere questo dilemma viene spedito lo stesso messaggio, contenente le informazioni corrette, sotto forma di problema matematico la cui soluzione fornisce la chiave di interpretazione del messaggio e quindi le informazioni necessarie per coordinare l'attacco. Nel momento in cui uno dei generali riesce a trovare la soluzione potrà inviarla a tutti gli altri che, inserendola all'interno del problema matematico ricevuto, potranno decifrarlo e agire contemporaneamente senza che alcun generale traditore possa alterare le informazioni ivi contenute.

La chiave di questa metafora, che rappresenta il punto di forza della soluzione adottata dalla tecnologia blockchain al problema dei registri distribuiti, è il problema matematico

rappresentato dall'algoritmo di consenso che in modo inequivocabile permette di risolvere questo dilemma mantenendo la rete sicura dagli attacchi degli attori malevoli.

Il problema dei generali bizantini pone inoltre un'ulteriore questione riguardante il comportamento collusivo dei nodi; siccome il consenso viene raggiunto in maniera democratica e quindi attraverso la votazione a favore, ad esempio dell'approvazione di una transazione da iscrivere nel registro o blocco, la rete potrebbe essere danneggiata qualora il 51% dei nodi colluda intenzionalmente per votare a favore di un'azione fraudolenta. Questo problema viene risolto dalla presenza di un numero elevatissimo di nodi nella rete e, nuovamente, dagli algoritmi di consenso che pongono una barriera all'entrata, di diverso tipo, per prendere parte alle decisioni disincentivando un nodo ad agire contro la rete stessa.

2.1.2 Aggiornamenti della rete: fork

Trattandosi di un registro distribuito, il codice sorgente che permette il funzionamento di una rete blockchain è pubblico (open source) e per tanto può essere visto e letto da chiunque. Ciò permette a chiunque, qualora abbia le necessarie competenze pratiche, di sviluppare autonomamente un nuovo aggiornamento, delle correzioni o delle modifiche al codice. Questi sviluppi vengono condivisi all'interno della comunità e quindi tra i nodi partecipanti nella blockchain e vengono adottati qualora la maggioranza, nelle blockchain permissionless, o chi ha il potere decisionale, nelle blockchain permissioned, si esprima a favore dell'adozione. Ogni qualvolta viene proposto un aggiornamento o una modifica sostanziale si genera un fenomeno, detto "fork", che può causare due possibili conseguenze.

Con il termine "fork", o biforcazione, si intende la divisione della blockchain in due ramificazioni dando vita ad una nuova la quale, pur condividendo l'intera cronologia con la blockchain originaria, punta verso una nuova direzione prevista dagli aggiornamenti.

Vi possono essere due tipi di fork: (i) soft fork: simile ad un aggiornamento di sistema, si tratta di una modifica retrocompatibile con il sistema originario e con i blocchi precedentemente creati; (ii) hard fork: avviene a seguito di un significativo cambiamento del codice generando una nuova catena i cui blocchi non sono compatibili con quelli della blockchain originaria. Questo tipo di fork porta alla formazione di due nuove blockchain completamente distinte una

dall'altra e alla creazione di una nuova criptovaluta; alcuni esempi di questo tipo di biforcazione sono le varianti di bitcoin come bitcoin cash (BCH) o bitcoin gold (BTG), entrambe formate a seguito di un hard fork di Bitcoin da cui si sono generate le rispettive blockchain.

2.2 BITCOIN: la prima blockchain

"Una versione puramente peer-to-peer del denaro elettronico consentirebbe di inviare pagamenti online direttamente da una parte all'altra senza passare attraverso un'istituzione finanziaria. Le firme digitali forniscono una parte della soluzione, ma i vantaggi principali si perdono se è ancora necessaria una terza parte fidata per evitare la doppia spesa. Proponiamo una soluzione al problema della doppia spesa utilizzando una rete peer-to-peer. La rete marca il tempo delle transazioni, inserendole in una catena continua di proof-of-work basati su hash, formando un record che non può essere modificato senza rifare il proof-of-work. La catena più lunga non serve solo come prova della sequenza di eventi a cui si è assistito, ma anche come prova che proviene dal più grande pool di CPU. Finché la maggior parte della potenza della CPU è controllata da nodi che non cooperano per attaccare la rete, essi genereranno la catena più lunga e supereranno gli aggressori. La rete stessa richiede una struttura minima. I messaggi vengono trasmessi al meglio e i nodi possono uscire e rientrare nella rete a piacimento, accettando la catena di proof-of-work più lunga come prova di ciò che è accaduto durante la loro assenza." [20].

Il testo sopra riportato è l'abstract del documento *"Bitcoin: A Peer-to-Peer Electronic Cash System",* anche noto come White Paper di Bitcoin, con cui il 31 ottobre 2008 l'autore, o gruppo di autori, dal nome Satoshi Nakamoto sancisce la nascita della prima blockchain ad oggi conosciuta: Bitcoin.

Come riportato all'intero del documento, Bitcoin nasce con uno scopo preciso, ovvero quello di permettere pagamenti virtuali attraverso una moneta elettronica senza il passaggio attraverso un intermediario o una terza parte. Per fate ciò le soluzioni adottate sono diverse tutte basate sull'approccio e la logica matematica nonché sulla crittografia per garantire la sicurezza della rete. Tra queste vi sono l'adozione di algoritmi di consenso e la creazione di un

[20] Traduzione dell'abstract del paper *"Bitcoin: A Peer-to-Peer Electronic Cash System";* Satoshi Nakamoto, Ottobre 2008

sistema peer-to-peer, tutti fattori estremamente disruptive per l'epoca in cui sono stati implementati e con la logica attraverso cui sono stati assemblati. Infatti, considerando il contesto storico, economico e tecnologico in cui nasce, Bitcoin risulta essere una soluzione avveniristica in grado di portare tempestivamente la soluzione ad uno dei più grandi problemi che il mondo stesse affrontando in quegli anni. Nel 2008 infatti gli Stati Uniti, così come la maggior parte del resto del mondo, si trova a dover affrontare la crisi generata dai mutui subprime, la più grande crisi finanziaria della storia fino a quel momento, la quale, sopra ogni cosa, ha minato le basi dell'affidabilità del settore finanziario e soprattutto di quello bancario. Il tempismo con il quale viene proposta al mondo Bitcoin è inevitabilmente uno dei fattori che ne ha determinato il successo, soprattutto per i primi utilizzatori. Satoshi Nakamoto infatti non solo propone, ma spiega in modo semplice, chiaro e diretto come sarebbe stato possibile permettere lo scambio di liquidità, e quindi mantenere in vita l'economia, senza doversi affidare ad un intermediario finanziario, nel momento in cui la fiducia verso gli stessi era probabilmente ai minimi storici. Nonostante ciò, l'adozione di Bitcoin nonché la popolarità della sua criptovaluta bitcoin (BTC) ha impiegato diversi anni ad affermarsi fino ad esplodere definitivamente tra il 2015-2017, anni in cui è diventato un fenomeno globale di massa che ha attirato l'attenzione di utenti ed investitori da ogni parte del mondo.

2.2.1 Hash e Proof of Work

Uno degli aspetti che rappresenta uno dei punti di forza dell'ecosistema Bitcoin è la crittografia che sorregge e garantisce la sicurezza dell'intero network. In particolare, la funzione crittografica utilizzata da Satoshi Nakamoto è una delle più sicure al mondo ed è indicata come "hash". L' hash è l'impronta digitale di un documento, ovvero l'identificativo univoco che differenzia ogni transazione che avviene tramite blockchain; si tratta di un algoritmo di crittografia avanzata ideato in ambito militare per la sicurezza della trasmissione di dati sensibili. L'algoritmo specifico utilizzato nella blockchain di Bitcoin prende il nome di SHA256, Secure Hash Algoritm che occupa 256 bit di memoria. Il funzionamento dello SHA256 è estremamente complicato a livello matematico ed informatico, ma di facile comprensione a livello logico: l'algoritmo prende in input vari tipi di informazioni, come numeri, testo, documenti

etc., e restituisce come output 64 caratteri alfanumerici. Per ogni input corrisponde un unico output esclusivo a prescindere dal numero di informazioni immesse come; la peculiarità risiede nel fatto che ogni combinazione di caratteri, ad esempio di un testo, genera un output completamente diverso l'uno dall'altro nonostante il significato magari rimane lo stesso. Il funzionamento, inoltre, è unidirezionale in quanto lo stesso input genera sempre lo stesso output, ma dall'output non si può risalire all'input. Per capire ancora meglio il funzionamento verranno riportati di seguito una serie di esempi[21]:

Input: 1
Output: 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
Input: 0
Output: 5feceb66ffc86f38d952786c6d696c79c2dbc239dd4e91b46729d73a27fb57e9
Input: 10
Output: 4a44dc15364204a80fe80e9039455cc1608281820fe2b24f1e5233ade6af1dd5

Nel caso si trattasse di un testo l'output restituito cambierebbe completamente qualora in input venga inserito un carattere piuttosto che un altro, ad esempio una lettera maiuscola o minuscola, oppure uno spazio in più o in meno:

Input: Hello world
Output: 64ec88ca00b268e5ba1a35678a1b5316d212f4f366b2477232534a8aeca37f3c
Input: hello world
Output: b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

Come detto, l'output rimarrà sempre una combinazione casuale di 64 caratteri alfanumerici a prescindere dalla quantità di informazioni inserite, come ad esempio a prescindere dalla lunghezza del testo. Se si inserisse come input l'intero abstract del White paper di Bitcoin, riportato all'inizio del paragrafo 2.2, si otterrebbe come output:

f00fd664db1df4cba6ad91dae55fab57ae355851e24bf3241c2bc4971071623b

[21] Fonte degli output: https://emn178.github.io/online-tools/sha256.html

Una volta compreso il meccanismo di funzionamento dello SHA256 è possibile capire in che modo una catena di blocchi si mantiene sicura nel corso del tempo dove ogni singola transazione, ogni singola informazione inserita all'interno della rete viene protetta da un così alto livello di sicurezza informatica.

Il passaggio successivo per comprendere come funzioni la blockchain di Bitcoin e come faccia a rimanere imperturbabile, riguarda il suo algoritmo di consenso e chi può eseguirlo.

L'algoritmo di consenso di Bitcoin è la cosiddetta Proof-of-Work (POW) ovvero un meccanismo che consente di partecipare alla rete e creare, in gergo tecnico "minare", nuovi blocchi guadagnando, come visto precedentemente, da un premio diretto e dalle commissioni sulle transazioni iscritte nel nuovo blocco. La POW è immaginabile come il problema matematico complesso da dover risolvere la cui soluzione permette di ottenere un guadagno economico elevato; la barriera all'entrata, ovvero lo sforzo e il costo che si deve sopportare per risolvere la proof-of-work, è la capacità computazionale e di calcolo dell'hardware che opera per trovare la soluzione al problema posto. Gli hardware utilizzati dagli operatori sono specifici e con un costo elevato, sommando a questo costo il consumo energetico, espresso sia in termini economici sia come capacità computazionale, si ottiene il forte disincentivo ad operare contro la rete visto che gli attori che si trovano a competere sono molteplici.

I soggetti, o nodi, chiamati a risolvere la Proof-of-Work sono detti "miner", ovvero coloro i quali partecipano all'attività di "mining" dei blocchi della blockchain di Bitcoin. I miner competono tra di loro per trovare la soluzione al problema posto dalla POW che consiste nel trovare un numero, espresso in hash, al di sotto di una determinata soglia impostata dal problema. Il numero attraverso cui vengono effettuati i tentativi di risoluzione è detto "nonce"[22] con cui si cerca di impostare un hash Block header minore del livello di difficoltà imposto dal protocollo e richiesto dalla POW. Una volta ottenuto questo risultato, l'unico possibile per risolvere la POW, e verificato dagli altri nodi, il miner vincitore si attesta la cosiddetta "coinbase", ovvero la prima transazione iscritta nel nuovo blocco che il miner fa verso sé stesso e formata dalla ricompensa diretta, e genera il nuovo blocco che sarà da quel momento pienamente operativo e funzionante. Ogni 2016 blocchi la difficoltà del problema matematico richiesto dalla

[22] *"... nonce Proof of Work, un valore casuale di un blocco usato proprio per soddisfare il Proof of Work. In crittografia il nonce è un numero casuale o pseudocasuale utilizzato una volta sola..."* – Definizione Borsa Italiana

POW si aggiorna automaticamente; inoltre, la ricompensa diretta ottenuta dai miner è programmata per diminuire progressivamente nel corso del tempo. Infatti, ogni circa 4 anni la "Block reward" si dimezza attraverso un fenomeno detto "halving": inizialmente la ricompensa era di 50 BTC per ogni blocco minato, nel 2013 è passata a 25 BTC, nel 2017 era di 12,5 BTC mentre ad oggi è di 6,25 BTC. Il prossimo halving è previsto essere intorno alla metà del 2024 e risulta essere uno dei più attesi visto che a seguito degli ultimi 3 il prezzo dei BTC è salito ogni volta considerevolmente.

Tenuto conto del fatto che un blocco sulla blockchain di Bitcoin viene validato ogni circa 10 minuti e che il numero massimo di bitcoin generali (total supply) è programmato a 21 milioni, all'incirca intorno all'anno 2140 cesserà il mining di nuovi BTC e gli halving saranno interrotti.

2.3 Ethereum

Ethereum è il nome della seconda blockchain più conosciuta al mondo, madre della seconda criptovaluta più importante in termini di capitalizzazione seconda solo a bitcoin: Ether (ETH), digital asset nativo che alimenta il protocollo.

Nasce nel 2014 sotto forma di piattaforma open source decentralizzata e basata su blockchain con obiettivo principale quello di creare un protocollo alternativo per la creazione di applicazioni decentralizzate, DApp (decentralized Application). Il suo fondatore/creatore, Vitalik Buterin, ha dato vista a questo sistema all'età di 20 anni per poi lanciarlo ufficialmente nel 2015 riscuotendo da subito molto successo.

A differenza di quanto visto nei paragrafi precedenti, Ethereum si differenzia da Bitcoin per una caratteristica fondamentale, quella di essere sostanzialmente aperta. Su Ethereum, infatti, è possibile dar vita ad applicazioni e altre iniziative che superino il solo scambio di valuta decentralizzato. Come Bitcoin l'architettura informatica e matematica nascosta dietro al funzionamento della rete rimane la stessa, Ethereum infatti permette di archiviare le informazioni direttamente on chain, ovvero sulla propria blockchain rendendo maggiormente interattivo il settore e gettando le basi per quella che è stata, ed è ancora tutt'ora, la rivoluzione del cosiddetto Web3.0.

Essendo di fatto la seconda blockchain mai creata e la prima aperta, interconnessa e soprattutto gestita da una community attiva di programmatori esperti, Ethereum risulta essere allo stesso tempo molto simile, in quanto adotta la stessa tecnologia, ed estremamente diversa rispetto a Bitcoin. Il fatto di essere gestita, a livello informatico, direttamente da un team di persone fisiche conosciute e note permette di accantonare quel velo di mistero che tutt'ora aleggia intorno a Bitcoin e al suo fondatore anonimo. Inoltre, Ethereum opera per certi versi come una vera e propria azienda, sebbene non abbia come scopo ultimo quello di generare profitti, con un team di programmatori e con progetti e piani pubblici che innova costantemente nel corso del tempo.

Ciò che però contraddistingue e differenzia Ethereum dalla sua rivale è la velocità di creazione dei blocchi (uno ogni circa 15 secondi), di esecuzione delle transazioni, i costi delle stesse e soprattutto la scalabilità e le opportunità operative. Ethereum permette infatti al suo interno di creare ulteriori applicazioni e addirittura la creazione di altri ecosistemi blockchain basati sul suo meccanismo di sicurezza. Questa capacità espansiva ha permesso da un lato di aumentare esponenzialmente il numero di utilizzatori e nodi attivi, anche in fase iniziale; dall'altro di dare vita alla creazione del Web3.0, la nuova frontiera del web che rivoluzionerà e sta iniziando a rivoluzionare il modo di utilizzare e di concepire internet rispetto a come siamo stati abituati fino ad oggi.

Nonostante i numerosi vantaggi però Ethereum rimane soggetta al "blockchain trilemma" che prevede la realizzazione di una combinazione di solo due dei tre seguenti fattori: scalabilità, sicurezza e decentralizzazione.

2.3.1 Algoritmo di consenso: Proof-of-Stake

Come anticipato all'inizio di questo capitolo la più grande differenza tra la blockchain di Ethereum e Bitcoin risiede nell'algoritmo di consenso utilizzato gestito attraverso un meccanismo definito come Proof-of-Stake.

Questo meccanismo di consenso, ideato da Sunny King e Scott Nadal e teorizzato all'interno del paper *"PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake"* nell'Agosto del 2012, funziona tramite una pratica molto nota nel mondo crypto, ovvero lo staking. Con

staking si intende "*l'atto di bloccare criptovalute per ricevere ricompense"* [23] e partecipare al corretto funzionamento della rete. Attraverso lo staking un utente può di fatto bloccare una porzione delle valute che detiene per impiegarle a beneficio della rete ottenendo in cambio una ricompensa espressa sempre in termini della valuta che è stata bloccata.

La proof-of-stake utilizza lo staking come mezzo per rendere ancora più decentralizzata e conveniente la partecipazione al funzionamento della blockchain. Infatti, questo meccanismo di consenso prevede che per validare un blocco e le transazioni ivi comprese, debbano essere bloccate un quantitativo di monete (minimo 32 ETH) per ottenere la possibilità di essere scelti dal protocollo per convalidare l'operazione. Nello specifico, il protocollo assegna casualmente ad un utente il diritto di validare il prossimo blocco nella rete, la probabilità di vedersi assegnato questo diritto è direttamente proporzionale alla quantità di monete messe in staking. Questo principio, che all'apparenza può destare qualche dubbio sulla sicurezza della rete, mette come barriera all'entrata, sebbene decisamente meno forte e più accessibile, il rischio di perdere la propria puntata, ovvero le monete messe in staking, e di conseguenza di perdere un ammontare di denaro non indifferente. In questo modo la rete si mantiene sicura da comportamenti fraudolenti disincentivando possibili attori malevoli dall'agire contro il network. Il tutto risulta più affidabile se si tiene in considerazione che vi è una componente significativa di attori, rappresentato dalla community di Ethereum in costante crescita, che ha come obiettivo quello di tutelare la rete e la propria blockchain.

I benefici apportati dalla POS riguardano l'efficienza energetica in quanto questo meccanismo, utilizzando come requisito la disponibilità economica e di valuta piuttosto che la capacità computazionale dell'hardware (POW), consente di minimizzare l'utilizzo di energia aumentando le prestazioni della rete (basti pensare che i processi di POW di Bitcoin causano un consumo di energia da parte dei miner pari a quello di un paese sviluppato). Infatti, su Ethereum i tempi di elaborazione delle transazioni nonché i tempi di creazione e validazione di un blocco sono significativamente inferiori rispetto a Bitcoin e alla POW. Inoltre, applicando una barriera all'entrata più debole, partecipare come nodo validatore attivo nella blockchain di

[23] Definizione Binance Academy – piattaforma educativa del più grande exchange di criptovalute al mondo nonché creatore di BSC (Binance Smart Chain), una delle blockchain più efficienti ed utilizzate al mondo

Ethereum risulta essere più semplice permettendo così alla comunità e alla rete di raggiungere un bacino di utenza maggiore e facilmente scalabile.

2.3.2 The Merge

Una volta capito come funziona questo meccanismo di consenso e appresi i vantaggi che comporta è facile capire come mai la community di Ethereum abbia deciso di utilizzarlo.

Occorre specificare, però, che Ethereum non ha da sempre adottato la POS ma, essendo nata come blockchain alternativa a Bitcoin dalla quale traeva spunto anche in termini di algoritmi di consenso, la scelta originale ricadeva sulla POW, meccanismo che utilizzava fino alle ore 06:42:59 del 15 settembre 2022, istante in cui è avvenuto l'aggiornamento della rete noto con il nome "The merge".

Questo avvenimento risulta essere di importanza assoluta per l'intero mondo cripto e blockchain in quanto si tratta di una delle prime volte in cui una delle più grandi chain esistenti cambiasse drasticamente l'algoritmo di consenso. Con il merge Ethereum ha modificato di fatto il suo "execution layer" originale fondendolo con uno di nuova creazione detto "consensus layer" presente all'interno della "beacon chain". La beacon chain era nata nel 2020 come progetto strutturato per la realizzazione di una blockchain appositamente compatibile con Ethereum in grado di funzionare attraverso POS e rimpiazzando così l'originale POW prevista nella blockchain originaria. Le due catene di blocchi, fino a quel momento separate, si sono così fuse, da qui il termine "merge", permettendo così di realizzare il tanto atteso aggiornamento.

Nell' aprile 2023 è stato eseguito un ulteriore aggiornamento della rete, detto Shapella, composto di due fasi principali, aggiornamento Shangai e aggiornamento Capella, con cui è stato permesso agli utenti che avevano messo in stalking i propri ether (ETH), a partire da settembre 2022, di ritirare le proprie ricompense e la quantità di denaro bloccata per permettere il corretto funzionamento della rete. L'effetto di tutti questi aggiornamenti è stato visto di buon occhio dal mercato producendo un improvviso aumento del valore degli ETH, sintomo di una buona riuscita e fiducia nel progetto.

2.4 Decentralized Application e Smart Contract

I fattori che hanno contribuito alla crescita e adozione esponenziale della blockchain di Ethereum sono innumerevoli ma i due che meritano maggiore attenzione, in quanto verranno approfonditi e integrati nel proseguo di questo documento, sono essenzialmente due: DApp, Decentralized Application/Applicazioni Decentralizzate, e gli Smart contract, contratti intelligenti.

2.4.1 DApp

Le applicazioni che comunemente vengono utilizzate e scaricate sui vari dispositivi, mobili e non, sono gestiti da server centralizzati nei quali vengono eseguiti i codici definiti come "back-end"; al contrario le applicazioni decentralizzate hanno il proprio codice di back-end in esecuzione su una rete peer-to-peer decentralizzata. Questo tipo di applicazioni non devono necessariamente funzionare tramite blockchain ma si avvalgono di una rete peer-to-peer ovvero una *"rete informatica nella quale i computer degli utenti connessi fungono nello stesso tempo da client e da server"* [24].

Visto il funzionamento di questo particolare tipo di applicazioni, è facilmente intuibile come la tecnologia blockchain possa giovare notevolmente per il loro sviluppo; in particolare in termini di scalabilità e sicurezza.

Tra le caratteristiche che contraddistinguono le applicazioni decentralizzate e per far si che esse vengano identificate come tali, in accordo con quanto afferma la comunità di Ethereum direttamente sul proprio portale [25], devono essere:

- Decentralizzate: le DApps operano su Ethereum, rete che di per sé opera in maniera decentralizzata
- Deterministiche: viene eseguita la stessa funzione a prescindere dall'ambiente dove questa viene eseguita
- Turing Complete: possono eseguire qualsiasi azione una volta fornite le risorse necessarie

[24] Definizione "Decentralized Application" enciclopedia Treccani
[25] "Introduzione alle DApp" portale Ethereum

- Isolate: funzionano in modo indipendente dalla blockchain di Ethereum interagendo con la stessa attraverso un motore virtuale, detto EVM (Ethereum Virtual Machine), che permette di mantenere la blockchain al sicuro dalla presenza ad esempio di bug

I vantaggi che comporta lo sviluppo di un'applicazione decentralizzata riguardano diversi fattori come l'assenza del tempo di inattività in quanto operando attraverso un contratto intelligente, una volta che questo viene distribuito sulla blockchain, l'intera rete potrà servire gli utenti che vogliono interagire con il contratto impedendo ad attori malevoli di bloccare l'esecuzione e sospendere l'attività. Inoltre, i dati immessi nelle applicazioni così come nella blockchain sono immutabili e presentano una completa integrità. Questa peculiarità risulta essere al contempo uno dei più grandi svantaggi in quanto essendo estremamente difficile modificare i dati contenuti in una DApp, sarà allo stesso modo difficile, ma non impossibile, applicare modifiche o aggiornamenti una volta che queste vengono create, distribuite e rese operative.

2.4.2 Smart Contract

Per funzionare correttamente sia le applicazioni decentralizzate, sia tutte le altre iniziative di attività sviluppate tramite blockchain hanno bisogno di uno strumento essenziale introdotto in Ethereum e discusso notevolmente anche da un punto di vista legale in tutto il mondo: gli Smart Contract.

Gli Smart Contract o contratti intelligenti, sono dei programmi informatici in cui sono contenuti i termini di un contratto all'interno del codice; contengono azioni automatizzate codificate che vengono eseguite nel momento in cui vengono soddisfatte una serie di condizioni previste.

Il contratto intelligente regola i termini e le condizioni di un accordo preso tra le parti ed essendo raccolti all'interno di un codice programmato su una blockchain come Ethereum, la loro esecuzione è automatica e non è previsto l'intervento di una terza parte che interferisce nel processo e regola l'esecuzione. Gli smart contract permettono agli sviluppatori di creare

applicazioni che sfruttano la sicurezza, affidabilità e accessibilità della blockchain offrendo funzionalità peer-to-peer tra cui rientrano la concessione o richiesta di prestiti.

Ciò che differenzia un contratto intelligente da un contratto normale o "reale" è che le condizioni sono scritte in codice e non su carta, archiviate sulla blockchain e non da un notaio o terza parte. Il carattere che rende utili e speciali gli smart contract è la loro possibile applicazione in qualsiasi ambito e in qualsiasi modo permettendo il superamento del concetto di blockchain originariamente pensato da Bitcoin. Attraverso questo tipo di contratti si può creare qualsiasi cosa che vada oltre il semplice scambio di denaro permettendo alla blockchain di diventare un sistema interattivo invece che un mero sistema di pagamento virtuale.

Fino a questo momento Ethereum è la piattaforma più diffusa, nonché la prima ad averne previsto l'utilizzo, che permette la creazione e l'esecuzione di smart contract, sebbene non sia l'unica. Chiunque può scrivere uno smart contract e distribuirlo sulla blockchain, il codice rimane sempre trasparente e verificabile da chiunque ed inoltre, essendo "pubblicato" su blockchain, rimane immutabile e inalterabile garantendo così la sicurezza e permettendo a chiunque di leggere quanto scritto e previsto dal contratto. Per scrivere uno smart contract possono essere utilizzati diversi linguaggi di programmazione che, da chi ha le competenze necessarie, può all'occorrenza essere "tradotto" in linguaggio comune. Ogni nodo nella rete memorizza una copia del contratto ed esegue il suo codice ogni volta che questo riceve fondi o viene richiamato da un utente. Questo meccanismo consente che non vi sia una controparte fraudolenta, che non rispetta la propria obbligazione, o che possano intervenire attori che blocchino l'esecuzione o danneggino una delle parti.

La stesura di uno smart contract non è di competenza solo di un programmatore informatico esperto ma, come avviene nella maggior parte dei casi, richiede la partecipazione di altre figure, tra cui almeno una legale che possa prevedere le varie clausole e renderle compatibili con l'ordinamento vigente. Infatti, a livello legale a partire dal 2019 con il Decreto Semplificazioni la normativa italiana ha inglobato la fattispecie degli smart contract all'interno del proprio ordinamento sebbene non prevedendo una normativa o un articolo specifico. L'articolo 8-ter dell'omonimo decreto afferma *"Si definisce «smart contract» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti*

interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto" [26].

Da quanto emerge a seguito dalle analisi e dalle evoluzioni della giurisprudenza, lo smart contract ha valore legale qualora soddisfi i requisiti di legge, previsti dal legislatore, attualmente in vigore e solo dal momento in cui questo viene eseguito. Questa apertura rappresenta una svolta importante nell'evoluzione sia per il futuro della tecnologia blockchain, e della sua applicazione commerciale, sia per la regolamentazione che dovrà vigilare ed intervenire sugli sviluppi futuri.

Gli smart contract sono uno strumento essenziale anche per la creazione e realizzazione del meccanismo che verrà discusso nel prossimo capitolo, che può rappresentare una rivoluzione per l'intero settore finanziario: la tokenizzazione di asset reali.

[26] Art 8-ter del DECRETO-LEGGE 14 dicembre 2018, n. 135; coordinato con la legge di conversione 11 febbraio 2019, n.12 recante: «Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione.». (19A00934)

3. TOKENIZZAZIONE DI ASSET REALI

Con tokenizzazione di asset reali si fa riferimento al *"Processo di assegnazione di un token a un dato bene, che comporta la rappresentazione digitale di asset fisici su un registro distribuito oppure l'emissione di classi di asset tradizionali sotto forma di token."*[27]

Prima di entrare nello specifico nella fattispecie della tokenizzazione occorre definire cosa sia un token, quali e quanti tipi di token esistono, come possono essere generati e per cosa possono essere utilizzati.

Secondo quanto riporta l'enciclopedia Treccani con token si indica "*In informatica, termine con cui si designa un indicatore univoco registrato in una blockchain (registro condiviso), con funzione di rappresentare un oggetto digitale, di certificare la proprietà di un bene o di consentire l'accesso a un servizio."* [28]. Si tratta perciò di uno strumento digitale che può contenere e rappresentare diverse funzioni che viene archiviato e protetto dalla tecnologia blockchain. È una delle innovazioni che quest'ultima ha portato negli ultimi anni in grado di destare notevole scalpore visto la sua eterogeneità applicativa; studiosi, sviluppatori ed istituzioni studiano questo strumento da anni per capirne il vero potenziale e cogliere i principali punti di fragilità. Tra le istituzioni attirate dall'uso dei token nonché, più in generale, dal possibile utilizzo della blockchain su vasta scala, ve ne sono diverse sia nel panorama nazionale che internazionale. Una delle prime ad aver studiato i fenomeni derivanti in generale dal mondo crypto è la BCE (Banca Centrale Europea) che ha realizzato diverse pubblicazioni a partire dal 2015, alcune delle quali in collaborazione con altre banche centrali o istituzioni finanziarie di tutto il mondo. Il motivo che attrae maggiormente l'interesse delle banche centrali, come BCE o FED, è l'opportunità di poter generare un nuovo tipo di criptovaluta nota con come "Central Bank digital Currency" (CBDC); si possono trovare dei riferimenti agli studi da parte della BCE

[27] Definizione "tokenizzazione" accademia della Crusca (https://accademiadellacrusca.it/it/parole-nuove/tokenizzazione/23537#:~:text=Definizione,tradizionali%20sotto%20forma%20di%20token).
[28] Definizione "token" enciclopedia Treccani (https://www.treccani.it/enciclopedia/token/#:~:text=In%20informatica%2C%20termine%20con%20cui,l%27accesso%20a%20un%20servizio).

in una serie di paper pubblicati negli ultimi anni[29] [30]. Anche il Fondo Monetario Internazionale (IMF) così come l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD) hanno studiato questo fenomeno in seguito al crescente interesse da parte di investitori ed utilizzatori. In Italia l'interesse istituzionale è arrivato leggermente in ritardo rispetto ai corrispettivi internazionali, con l'intento di osservare lo sviluppo da un'ottica legale e di regolazione; la Consob, infatti, ha pubblicato in data 25 gennaio 2023 un paper dal titolo *"Tokenizzazione di azioni e azioni tokens"* [31] con cui analizza il fenomeno delle partecipazioni azionarie sottoforma di tokens riportando la divisione ed il possibile inquadramento giuridico dei diversi tipi di token esistenti.

Il più recente sconvolgimento normativo avviene nei giorni di stesura del presente elaborato: il Parlamento Europeo nella seduta del 20 aprile 2023 ha approvato il testo normativo ufficiale riguardante il mondo dei crypto-assets (MiCAR – *Market for Crypto-Assets Regulation*) cha rimane ora in attesa della votazione del Consiglio Europeo prevista per il 16 maggio 2023 per l'ingresso nella gazzetta ufficiale; la data prevista per l'entrata in vigore del testo è luglio 2023. Le implicazioni nonché le regole che questo testo genera nel mercato europeo delle valute digitali verranno poi discusse successivamente nei prossimi paragrafi.

Come preannunciato, esistono diversi tipi di token suddivisi in due contrapposizioni:

- Fungibili vs Non Fungibili: i token fungibili possono essere sostituiti con una loro versione identica in quanto non incorporano caratteri di unicità (ad esempio le criptovalute, fan token, Stablecoin e le CBDC). I token Non Fungibili, noti anche con il nome di NFT (Non Fungible token), presentano ognuno degli attributi che li rendono unici e diversi l'uno dall'altro come un codice identificativo (vengono utilizzati ad esempio per la creazione di arte o identità digitali)

[29] *"Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures"* ECB Crypto-Assets Task Force, Occasional paper series No 223 / May 2019

[30] "*Report on a digital euro"* ECB, October 2020
"The optimal quantity of CBDC in a bank-based economy" L. Burlon, C. Montes-Galdón, M. A. Muñoz, F. Smets; Working Paper Series, No 2689 / July 2022

[31] "*Tokenizzazione di azioni e azioni tokens"* P. Carrière, N. de Luca, M. de Mari, G. Gasparri, T.N. Poli; quaderni giuridici Consob

- Utility vs Security: i token utility hanno un'utilità specifica all'interno dell'ecosistema in cui si muovono (possono essere utilizzati ad esempio per reclamare dei benefit legati ad un servizio, per generare dei punti fedeltà o dei biglietti per l'accesso ad eventi). I security token, invece, rappresentano una vera e propria attività finanziaria, hanno come sottostante un titolo o uno strumento finanziario (come bond, azioni o opzioni)

Di seguito verranno riportate la classificazione di due istituzioni appartenenti a due stati diversi, Italia e Svizzera, per mostrare come l'attenzione delle istituzioni fosse già stata catturata in passato da questi strumenti.

La Banca d'Italia, all'interno di un documento su questioni di economia e finanza denominato "*Aspetti economici e regolamentari delle «cripto-attività» "* [32], identifica quattro tipologie di token in base alle funzioni che possono svolgere:

1. DT1 - "valute virtuali" ("crypto-assets" privi di diritti o passività): gettoni digitali privi di diritti incorporati o passività; sono negoziabili e convertibili in moneta legale (fiat) o altre valute virtuali
2. DT2 – digital coins o payment tokens: strumenti che intendono, a differenza dei DT1, replicare le funzionalità della moneta mantenendo con essa un valore fisso. Questi gettoni digitali sono un diritto o una passività dell'emittente. Questi sono:
    a. Privati a valore fisso (stable coins): essi sono emessi da una entità giuridica a fronte di una unità di moneta (uno-a-uno con euro, dollaro, ecc.) segregata presso un soggetto regolato
    b. Emessi da una banca centrale (CBDC): rappresentano una passività della banca centrale e sono ancora in fase di sperimentazione
    c. Non convertibili: sono *digital tokens* che favoriscono il baratto. Si distinguono da altri tipi di gettoni digitali poiché non sono convertibili con moneta legale o con altre "valute virtuali"; danno il diritto a scambiare beni o servizi tra i partecipanti al circuito, ma sono a diffusione e spendibilità limitata

[32] "Aspetti economici e regolamentari delle «cripto-attività»", A. Caponera e C. Gola, Questioni di Economia e Finanza – Occasional Paper, marzo 2019

3. DT3 – security/asset token: sono gettoni digitali trasferibili e potenzialmente negoziabili. su una piattaforma, tipicamente offerti tramite una operazione di *Initial Coin Offering* (ICO). Essi sono simili a titoli smaterializzati, che tuttavia vengono trasferiti tramite la DLT. Lo *status* giuridico e regolamentare dei *security/asset tokens* è incerto
4. DT4 – utility/consumer tokens: sono gettoni digitali non negoziabili (pur essendo talvolta trasferibili) che offrono unicamente diritti amministrativi o licenze d'uso, quali l'accesso a una piattaforma, a una *facility*, a un *network* di persone, a schemi di "fidelizzazione"

La FINMA (autorità federale di vigilanza sui mercati finanziari), corrispettiva svizzera della Consob, identifica all'interno della propria "*Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle Initial Coin Offering (ICO)"* [33] tre tipologie principali di token:

1. Token di pagamento: a categoria «*token* di pagamento» (sinonimo di semplici «criptovalute») comprende *token* che, effettivamente o nelle intenzioni dell'organizzatore, sono accettati come mezzi di pagamento per l'acquisto di beni o servizi oppure sono finalizzati al trasferimento di denaro e di valori. Le criptovalute non conferiscono diritti nei confronti di un emittente.
2. Token di utilizzo: la FINMA definisce «token di utilizzo» quei token che permettono di accedere a un'utilizzazione o a un servizio digitale forniti su o die- tro utilizzo di un'infrastruttura blockchain.
3. Token d'investimento: la categoria «token d'investimento» comprende token che rappresentano valori patrimoniali. Tali token possono rappresentare, in particolare, un credito ai sensi del diritto delle obbligazioni nei con- fronti dell'emittente oppure un diritto sociale ai sensi del diritto societario. Nel caso dei token d'investimento vengono promessi, per esempio, quote di ricavi futuri dell'azienda o flussi di capitale futuri. Secondo la funzione economica, il token rappresenta così, in particolare, un'azione, un'obbligazione o uno

[33] "*Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle Initial Coin Offering (ICO)"* FINMA, 16 febbraio 2018

strumento finanziario derivato. Nella categoria dei token d'investimento possono rientrare anche i token che mirano a rendere negoziabili sulla blockchain oggetti di valore materiali.

Queste due istituzioni, centrali per i rispettivi paesi in cui operano, riportano un punto di vista simile sebbene non speculare; ciò dimostra come vi sia bisogno di una convergenza istituzionale su larga scala per definire un regolamento chiaro e tracciare un percorso evolutivo "legale" per questi strumenti che in futuro otterranno sempre più importanza nel panorama finanziario mondiale. A livello internazionale il primo regolatore che riuscirà a portare un testo normativo adeguato e chiaro che tenga conto e permetta l'espressione delle potenzialità operative della tokenizzazione tutelando al contempo le esigenze e gli interessi degli investitori, fungerà da modello per gli altri e permetterò al proprio contesto di riferimento di ottenere un notevole vantaggio competitivo.

3.1 DeFi: Decentralized Finance

Dalla nascita delle prime blockchain e delle rispettive criptovalute si è generato un fenomeno di disintermediazione inizialmente degli scambi monetari e dei pagamenti, sebbene solo per un limitato numero di casi, e successivamente della finanza tradizionale. Questo fenomeno ha preso il nome di Decentralized Finance (DeFi) o finanza decentralizzata con cui si identifica l'organizzazione di servizi finanziari, comunemente offerti da intermediari specializzati, su strutture che operano in maniera decentralizzata, come la blockchain o le DLT, che non abbiano bisogno di una figura centrale, come una banca, per funzionare correttamente.

Lo sviluppo ed il propagarsi di strumenti come i tokens ha portato ad un aumento esponenziale di questo fenomeno cha ha acquisito, come detto, sempre più importanza negli anni. La generazione di token che rappresentano e vengono scambiati di fatto come se fossero degli strumenti finanziari, come i titoli azionari, ha rafforzato la visione generale secondo cui le criptovalute siano degli asset finanziari altamente rischiosi da valutare e gestire come tali. Questo punto di vista fu inizialmente condiviso dalla BCE che reputava le criptovalute come degli asset finanziari da valutare attentamente a causa del proprio rischio intrinseco dovuto alla volatilità dei prezzi, invece che come delle vere e proprie valute. Le argomentazioni riportate

dalla stessa BCE, all'interno di un'analisi sull'impatto delle criptovalute sulla stabilità del sistema finanziario europeo, riguardano il fatto che le stesse non rispettano nessuna delle funzioni della moneta legale, ovvero: (i) riserva di valore; (ii) mezzo di pagamento; (iii) unità di conto [34]. Queste argomentazioni, valide al tempo dell'analisi svolta (2019), sono state messe in discussione dalle recenti evoluzioni del mondo cripto. Nel giugno 2021 El Salvador è stato il primo paese ad ufficializzare l'adozione di bitcoin come moneta a corso legale, sebbene rappresenti un caso isolato, fornendo alla stessa la funzione di mezzo di pagamento. Contestualmente si può affermare che le monete virtuali abbiano raggiunto e soddisfino la funzione di mezzo di pagamento in quanto sono sempre di più le attività commerciali e le imprese che accettano le criptovalute come pagamento per i propri servizi o prodotti. A sostegno di questo trend, stabilizzatosi nel corso del tempo, vi è stata la creazione e diffusione di vere e proprie carte di credito, emesse da exchange centralizzati come Binance o Coinbase, che operando attraverso i tradizionali circuiti di pagamento (come Visa o MasterCard) permettono di pagare in qualsiasi contesto utilizzando il proprio wallet di criptovalute; il pagamento avviene tramite la conversione istantanea della valuta digitale in valuta in corso legale del paese in cui si effettua il pagamento esattamente come se si stesse pagando con una valuta legale estera.

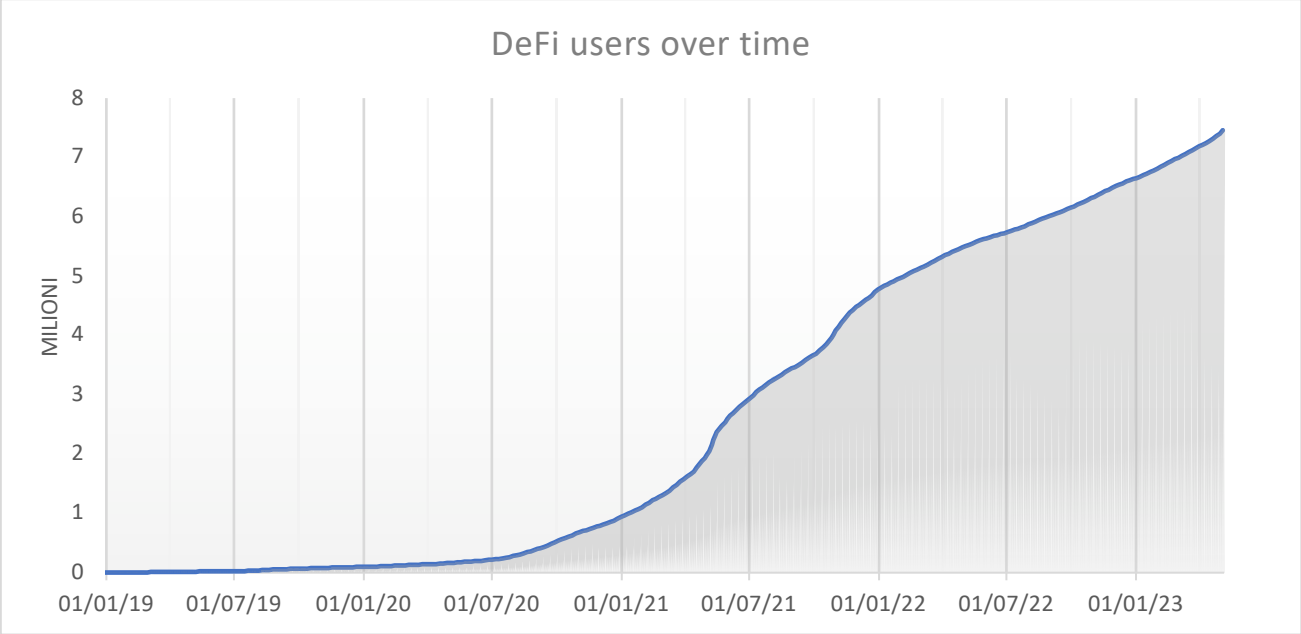
La tokenizzazione degli asset è un aspetto di centrale importanza per l'affermazione della finanza decentralizzata rispetto a quella tradizionale in quanto permette di sostituire completamente i servizi che ad oggi offrono gli intermediari finanziari; l'uso degli smart contract permette inoltre di ridurre la necessità della presenza di una terza parte che vigila sull'adempimento di un'obbligazione contratta dalle controparti rendendo per la maggior parte dei casi poco utile l'esistenza degli intermediari. Tuttavia, ad oggi, queste figure, centrali per il funzionamento e l'affidabilità del sistema finanziario, sono ancora necessarie e stanno apprendendo come reinventarsi e rimanere competitive in un mondo che sta seguendo un percorso diretto verso la disintermediazione finanziaria. Quello che è nato come un sistema per sostituire e rimpiazzare la dipendenza da figure centrali che regolassero il mondo finanziario,

[34] *"Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures"* ECB Crypto-Assets Task Force, ECB Occasional Paper Series No 223 / May 2019

può diventare per le stesse il più grande vantaggio competitivo nonché ispirazione per un ulteriore step evolutivo. Le più grandi banche di investimento stanno infatti testando questi sistemi cercando di internalizzare i processi di emissione di token con l'intento di creare persino delle proprie blockchain. In questo modo si assisterebbe ad una ri centralizzazione della finanza su un sistema che, però, permetterebbe di rendere più trasparente e accessibile il mondo delle operazioni finanziarie.

La crescita della DeFi negli ultimi anni è avvenuta a ritmi sorprendenti raggiungendo i 4,5 milioni di utenti attivi dal 2020 al 2022 fino ad attestarsi a più di 7 milioni ad aprile 2023[35]. L'altro dato che testimonia questa crescita riguarda il totale degli asset immobilizzati ed immessi nei protocolli e negli smart contract utilizzati dalle applicazioni di finanza decentralizzata, detto anche Total Value Locked (TVL). Il TVL è stato variabile lungo lo stesso periodo di tempo preso in considerazione per la crescita degli utenti marcando una crescita esponenziale che ha raggiunto il picco di 248.84 miliardi di dollari a novembre 2021 per poi oscillare e attestarsi intorno al valore di 50 miliardi nel primo trimestre del 2023 [36].

Il grafico seguente mostra il numero di utenti attivi nei protocolli DeFi nel corso del tempo



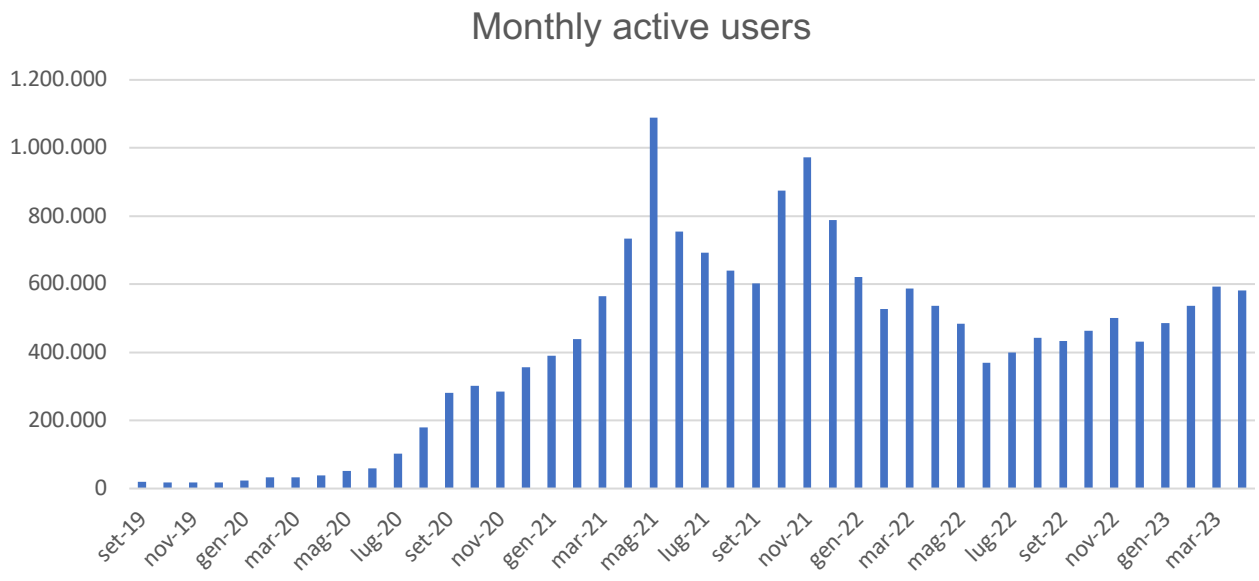
[37]

[35] Fonte dati: https://dune.com/queries/2972/5739 ; utilizzata nel seguente articolo del Sole 24 Ore: https://www.ilsole24ore.com/art/defi-come-funziona-finanza-pret-a-porter-basata-blockchain-AEJ3rj9

[36] Fonte dati: Statista "*TVL (total value locked) across multiple Decentralized Finance (DeFi) blockchains from November 2018 to April 24, 2023*"; https://www.statista.com/statistics/1272181/defi-tvl-in-multiple-blockchains/

[37] Elaborazione dati da database: https://dune.com/rchen8/defi-users-over-time

Il grafico che segue, invece, mostra il numero di utenti attivi mensilmente da settembre 2019 ad aprile 2023.



[38]

Questi dati dimostrano come l'adozione di soluzioni finanziarie decentralizzate siano state una scelta perseguita da un numero di utenti sempre maggiore ed in costante crescita negli ultimi quattro anni; nonostante il numero di utenti attivi mensilmente sia soggetto a delle oscillazioni, il trend rimane nettamente positivo sintomo che il numero l'utilizzo di applicazioni di finanza decentralizzata sarà sempre più comune in futuro.

3.2 Come avviene la tokenizzazione di asset reali

La tokenizzazione di asset è un processo volto a trasferire un bene reale in una sua rappresentazione digitale circolante su un registro distribuito, come la blockchain. Gli asset in questione, che verranno presi in considerazione in questo elaborato, sono di natura finanziaria o economica come, ad esempio, diritti di partecipazione a società, azioni, obbligazioni e tutti i titoli delle asset class finanziarie. L'unica precisazione deve essere fatta riguardo il mondo del real estate il quale, essendo caratterizzato da un elevato grado di burocratizzazione e di

[38] Elaborazione dati da database: https://dune.com/rchen8/defi-users-over-time

complessità normativa, deve essere trattato separatamente sebbene rappresenti una delle più grandi sfide e opportunità per generare liquidità in asset per loro natura illiquidi. Infatti, come si vedrà successivamente nel paragrafo 2.3, una delle implicazioni della tokenizzazione è la frazionabilità che in un contesto come quello immobiliare richiederebbe una serie di considerazioni aggiuntive rispetto a quelle che verranno fatte riguardo gli asset di natura finanziaria.

Il processo di rappresentazione on- chain di un asset finanziario o di un diritto di partecipazione richiede una serie di passaggi di diversa natura e complessità che necessitano di competenze che variano dall'informatica avanzata alla finanza, da legali a manageriali. Questo processo non è univoco e può differenziarsi a seconda del paese in cui viene implementato, questo a causa delle varie regolamentazioni (laddove ve ne siano) o degli obiettivi che si vogliono raggiungere.

Considerando una prospettiva generale, non esaustiva, si possono identificare sette passaggi fondamentali da affrontare per tokenizzare un asset reale [39]:

1. Deal origination: creazione dell'operazione e definizione degli obiettivi
2. Structuring: strutturazione dell'operazione secondo i parametri e le necessità dell'emittente, definizione dei termini di offerta del token, aspetti legali e tecnici (come la struttura e stesura degli smart contracts)
3. Subscription: sottoscrizione da parte dei primi investitori ai quali vengono offerti un determinato numero di token in relazione al taglio minimo di investimento scelto dall'emittente
4. Minting and distribution of tokens: i token vengono creati e distribuiti agli investitori tramite la blockchain trasferendo i fondi raccolti direttamente all'emittente
5. Asset servicing and custody: la piattaforma attraverso cui sono stati generati i token può, eventualmente e non obbligatoriamente, comportarsi come custode dei token replicando a tutti gli effetti le funzioni della Borsa tradizionale

[39] Questi passaggi sono riportati dall'analisi contenuta all'interno del paper *"Relevance of on-chain asset tokenization in 'crypto winter' "*, S. Kumar, R. Suresh, D. Liu, B. Kronfellner, A. Kaul; Boston Consulting Group e ADDX (più grande private market exchange dell' Asia)

6. Secondary trading: dopo l'emissione il token è disponibile sul mercato secondario fornito e rappresentato direttamente dalla blockchain. Inoltre, lo stesso token può essere listato su exchange centralizzati o decentralizzati accendendo così ad un mercato ancora più ampio
7. Maturity and burning of tokens: nel caso in cui il progetto di tokenizzazione prevedesse una scadenza specifica programmata, come nel caso di un token rappresentante un'obbligazione, al raggiungimento di tale scadenza i token vengono "bruciati" ovvero eliminati dalla circolazione a seguito della restituzione del denaro, sottoforma di valuta virtuale o fiat con cui sono stati acquistati, all'investitore

Si tratta di una visione di insieme, all'interno di ogni passaggio occorre risolvere diverse problematiche non scontate che possono essere più o meno grandi a seconda del progetto che si vuole realizzare. Da un punto di vista tecnico la programmazione degli smart contract, la definizione delle regole di funzionamento e distribuzione di token richiedono notevoli sforzi applicativi e delle capacità specifiche non facilmente individuabili sul mercato del lavoro odierno.

3.2.1 Impostazione funzionamento dei token: token standard

Per circolare correttamente e per essere compatibili con vari tipi di blockchain esistenti, i token hanno bisogno della definizione ed impostazione di una serie di regole di funzionamento definite e codificate appositamente per il tipo di funzione che il token deve adempiere. Vista l'esistenza di un vastissimo numero di blockchain ed un numero ancora più grande di token esistenti e potenzialmente generabili, gli sviluppatori, al posto di definire singolarmente da zero tutte le regole, si avvalgono dei cosiddetti ''standard'' ovvero insiemi di regole e convenzioni configurate e progettate con lo stesso schema che definiscono le principali funzionalità e proprietà dei token. In questo modo è possibile rendere i nuovi token compatibili con le blockchain e gli exchange decentralizzati già esistenti.

Questi standard possono essere progettati da ogni sviluppatore e la loro adozione non è soggetta ad accordi o vincoli, ma è semplicemente dovuta alla qualità del codice programmato

e alle funzioni che lo stesso permette di assolvere. Anche in questo caso la scelta di un accordo sulla rete non è subordinata alla presenza di un'autorità centrale, ma è la rete che autonomamente converge verso la propria preferenza. Infatti, nel momento della nascita di un nuovo progetto e della generazione di un nuovo token, l'emittente può scegliere di adottare un qualsiasi tipo di standard o di scrivere autonomamente da capo le regole di funzionamento del proprio token, la scelta di adottare uno standard già esistente, però, consente di avere una maggiore sicurezza e scalabilità per il proprio strumento.

Gli standard token più diffusi ed utilizzati sono generati e presenti nell'ecosistema di Ethereum, dato che non sorprende vista la capacità operativa[40] che la rete mette a disposizione nonché la sua compatibilità con le altre blockchain esistenti, e di Binance, il quale essendo il più grande exchange al mondo agevola le operazioni nel proprio network con l'adozione dei propri standard.

I token standard più utilizzati su Ethereum sono [41]:

- ERC – 20: "Ethereum Request for Comment" 20, creato nel 2015, è lo standard più diffuso ed utilizzato per la creazione di token fungibili come token di staking o valute virtuali
- ERC – 721: creato nel 2018, è lo standard utilizzato per la creazione di NFT o token non fungibili come atti relativi ad opere d'arte digitali
- ERC – 777: creato nel 2017, è lo standard che consente di creare extra-funzionalità sui token come l'invio degli stessi per conto di un altro (indirizzo, contratto o account), o una funzione di recupero di emergenza nel caso di smarrimento delle chiavi private
- ERC – 1155: creato nel 2018, consente scambi e aggregazioni di transazioni più efficienti permettendo di risparmiare sui costi. Permette, inoltre, di creare token utility e non fungibili

Un ulteriore tipo di token standard, operativo nel network di Binance, è il BEP – 20 che sia dal nome sia dalle funzioni che permette di realizzare, è molto simile all' ERC – 20. È lo standard utilizzato per la creazione di diverse tipologie di token sulla Binance Smart Chain (BSC),

[40] generazione DApps di vario genere e progetti di finanza decentralizzata
[41] Fonte: portale Ethereum https://ethereum.org/it/developers/docs/standards/tokens/

blockchain implementata da Binance, che sono compatibili con Ethereum ed altre blockchain e con i token con standard ERC – 20.

Nel momento in cui si volesse creare la rappresentazione on-chain di uno strumento finanziario, come un titolo azionario o obbligazionario, la scelta migliore sarebbe lo standard ERC – 20 in quanto, vista la sua diffusione e ampio utilizzo dagli utenti nella rete, risulterebbe il più efficiente e semplice da utilizzare. Qualora però si volessero rispettare dei requisiti regolamentari altamente stringenti, o se tra gli obiettivi del progetto di tokenizzazione vi sia quello di rendere più regolare e sicuro, da un punto di vista legale, lo scambio, la scelta potrebbe ricadere su uno standard non estremamente diffuso noto come ERC – 1400. Questo standard consente di prevedere dei meccanismi di KYC (Know Your Customer) e AML (Anti Money Laundering) che possono tutelare l'emittente dal rischio di controparte rendendo l'intero progetto *compliant* con le normative che un regolatore prevede in termini di scambio di titoli finanziari, o potrebbe prevedere per le transazioni di token.

Un passo in avanti decisamente molto importante è stato fatto a marzo 2023 quando è stato ufficialmente implementato lo standard ERC – 4804 con cui si gettano le basi per la rivoluzione del funzionamento di internet e dei normali siti web. Questo standard, infatti, avvicina ulteriormente il passaggio definitivo al Web 3.0 consentendo di accedere al front-end di un normale sito web attraverso uno smart contract che richiama un URL predefinito[42] e archivia i dati del sito direttamente sulla blockchain con cui interagisce attraverso l'Ethereum Virtual Machine (EVM). In questo modo l'utente interagisce direttamente con la EVM per richiamare direttamente delle applicazioni decentralizzate senza più dover passare su server centralizzati, come quelli di Amazon Web Services (AWS). Al momento sono pochi il numero di siti raggiungibili in questo modo e non sono ancora pienamente operativi per la maggior parte; pertanto, si tratta al momento solamente di un'alternativa attraente al normale internet ma nel lungo periodo potrebbe diventare la nuova normalità per accedere ad internet.

[42] "web3://" e non più "https://"; fonte: https://w3url.w3eth.io/#/

3.3 Implicazioni della tokenizzazione e possibili use case

Da un primo impatto la tokenizzazione potrebbe apparire come una semplice alternativa all'odierno sistema finanziario permettendo lo scambio di titoli o denaro in maniera diretta tra utenti, peer-to-peer, sostituendo di fatto l'utilità e la funzionalità degli intermediari. Scendendo più nel profondo e apprendendo quelle che sono le vere potenzialità della tecnologia blockchain e dei sistemi di tokenizzazione, si può arrivare a concepire un sistema ben più vasto con capacità applicative eterogenee e senza limiti di utilizzo.

La tokenizzazione di asset reali può diventare, e con tutta probabilità diventerà, il nuovo approdo della finanza e non solo permettendo di risolvere alcune delle problematiche più rilevanti che il sistema e i regolatori cercano di affrontare da tempo.

Inoltre, la tokenizzazione non deve necessariamente essere vista come nemica del sistema finanziario o degli intermediari che vi operano, ma dovrebbe piuttosto essere vista come un'opportunità, una sfida concreta con dei possibili risvolti evolutivi di grandissimo impatto.

Di seguito verranno affrontate una serie di implicazioni riguardo l'utilizzo della tokenizzazione e della sua possibile applicazione su larga scala anche da parte degli intermediari stessi, alcune delle quali analizzate e studiate da istituzioni importanti nel panorama mondiale.

La prima considerazione, probabilmente quella più immediata che si può fare, riguardo i vantaggi che l'adozione di asset tokenizzati comporterebbe riguarda la liquidità.

3.3.1 Rendere liquidi asset illiquidi

Il meccanismo di tokenizzazione, come osservato nei paragrafi precedenti, consente ad un qualsiasi tipo di asset, finanziario e non, di accedere ad un mercato secondario dove un gran numero di investitori possono agire e negoziare liberamente.

In questo modo, nel momento in cui oggetto di tokenizzazione fossero degli asset difficilmente liquidabili all'interno del sistema finanziario tradizionale, sarebbe possibile comprare o vendere gli stessi in tempi estremamente brevi senza dover applicare sconti eccessivi al prezzo del bene e rendendoli perciò liquidi.

Con liquidità si intende *"l'attitudine di un bene mobile o immobile a essere convertito in moneta legale. Quanto più rapidamente e a costi contenuti questo avviene, tanto più il bene può essere considerato liquido."* [43] ovvero trasformare un titolo in denaro circolante prontamente utilizzabile. Ad oggi vi sono diversi esempi di beni la cui liquidazione richiede tempistiche estremamente elevate e processi non esattamente rapidi e trasparenti; basti pensare anche ad un normale investimento azionario o obbligazionario, titoli definiti liquidi, che può essere venduto liberamente in qualsiasi momento, a patto che la Borsa in cui sono listati sia aperta. Tipicamente per un normale investitore retail il disinvestimento di un portafoglio azionario, o di una parte dei titoli presenti in esso, richiede fino ad un massimo di 15 giorni con dei valori medi che si aggirano intorno alla settimana. Queste tempistiche, considerate brevi per vedersi depositati i propri soldi disinvestiti, potrebbero essere azzerate e ridotte in un arco di secondi o al massimo minuti se il portafoglio in questione fosse composto da token, rappresentanti la partecipazione in una società, piuttosto che da titoli azionari. La dematerializzazione di questi ultimi ha consentito di velocizzare la circolazione ed il trasferimento di essi concentrando gli scambi all'interno di sistemi di autorità centrali, come Euronext Securities Milano [44]; la tokenizzazione consentirebbe di incrementare esponenzialmente la circolazione degli stessi permettendo scambi quasi istantanei. Le blockchain richiedono tempi di approvazione variabili ma estremamente inferiori per l'approvazione delle transazioni e per permettere di fatto il trasferimento di fondi o token da un utente all'altro. La variabilità dipende dalla congestione della rete e dalle commissioni che la stessa richiede per far approvare le transazioni, in media ci vogliono circa 5-10 minuti ma a seconda della blockchain utilizzata vi possono essere tempi di elaborazione anche istantanei. Ethereum, ad esempio, permette oggi di realizzare 100.000 transazioni al secondo che visti i volumi giornalieri si tradurrebbe in circa 14 minuti di attesa; altre blockchain come Ripple o Internet Computer Protocol (ICP) richiedono solo una manciata di secondi.

Pensare questi sistemi applicati a quelli tradizionali consentirebbe di accelerare drasticamente lo scambio di titoli, la Borsa virtuale rappresentata dalla blockchain non avrebbe

[43] Definizione "Liquidità" Borsa Italiana: https://www.borsaitaliana.it/notizie/sotto-la-lente/liquidita.htm
[44] Ex Monte Titoli S.p.A., unica società autorizzata da Banca d'Italia e Consob a gestire servizi di regolamento titoli

orari o limiti e questo si tradurrebbe in un possibile immobilizzo o smobilizzo di fondi, di qualsiasi entità, in maniera rapida, sicura e trasparente.

Se si ampliasse questo ragionamento, la tokenizzazione potrebbe essere coinvolta nel processo di raccolta fondi o di investimento di società persino non quotate. Non occorrerebbe emettere azioni su Borse nazionali ma basterebbe tokenizzarle e distribuirle nei protocolli di finanza decentralizzata per avere un bacino di possibili investitori di simili dimensioni e con minori costi di transazione. Le partecipazioni in start-up, PMI così come in tutte le società non quotate sui mercati, ovvero gli asset definiti per loro natura illiquidi, potrebbero essere tokenizzate e vendute ad investitori sia privati che istituzionali permettendo agli stessi di superare i problemi legati alla reperibilità di denaro liquido circolante. Anche da un punto di vista aziendale vi potrebbe essere un notevole decremento del ricorso al debito prediligendo una forma di equity tokenizzato con un costo intrinseco inferiore dovuto all'efficienza del mercato su cui è negoziato e alla facilità di smobilizzo. La stessa OECD vede come una delle possibili applicazioni quella di rappresentare sottoforma di token fondi di Venture Capital così come di Private Equity [45]; una previsione prudenziale effettuata da Boston Consulting Group vede possibile il raggiungimento di un valore complessivo degli asset tokenizzati pari a 16 trilioni di dollari, 16 milia miliardi di dollari (16.000.000.000.000$), equivalenti a circa il 10% del PIL mondiale entro il 2030 [46]. La stessa vede un potenziale ottimistico complessivo di circa 68 trilioni entro lo stesso anno, l'intero mercato azionario mondiale (global equity market) è stato stimato essere pari a 85 trilioni [47] ad inizio 2023. Una visione simile, sebbene più modesta, la riporta una delle più importanti banche di investimento al mondo, Citi, la quale prevede che questo mercato possa raggiungere un valore complessivo di 4-5 trilioni di dollari entro il 2030 [48].

[45] OECD (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, OECD Blockchain Policy Series, https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm

[46] *"Relevance of on-chain asset tokenization in 'crypto winter' "*, S. Kumar, R. Suresh, D. Liu, B. Kronfellner, A. Kaul; Boston Consulting Group e ADDX,

[47] Fonte Reuters: https://www.reuters.com/markets/europe/outsized-us-share-world-equity-may-revert-norm-2023-02-07/#:~:text=According%20to%20Datastream%2C%20global%20market,%24100%20trillion%20in%20late%202021.

[48] *"MONEY, TOKENS, AND GAMES Blockchain's Next Billion Users and Trillions in Value",* Citi GPS: Global Perspectives & Solutions, Marzo 2023

3.3.2 Vantaggi di costo e problemi di prezzo

La scelta di inserire all'interno del proprio portafoglio dei token al posto di titoli azionari o obbligazionari, come visto, permette di risparmiare e ottenere notevoli vantaggi in termini di costi di transazione ed intermediazione nonché di tempo.

L'acquisto o la vendita di token comporterebbe, infatti, costi di transazione legati semplicemente alle fee della blockchain che variano a seconda della rete utilizzata e in linea generale sono minori di quelli richiesti dai normali intermediari. Inoltre, sono completamente abbattuti i costi di intermediazione in quanto la finanza decentralizzata non richiede la presenza di intermediari che gestiscano i portafogli e chiedano delle commissioni per questo genere di servizi.

Il problema che questo meccanismo comporta riguarda il prezzo dell'asset in cui si investe che, a causa della facilità di speculazione, potrebbe discostarsi eccessivamente dal valore dell'asset reale. Per comprendere meglio questa dinamica si può prendere ad esempio un'azione ed il suo corrispettivo tokenizzato emesso come security token rappresentante il diritto di partecipazione in una società. L'azione in quanto tale circola su mercati regolamentati, gli scambi e le transazioni sono vigilati e permessi da un'entità centrale che funge da garante per il corretto funzionamento del sistema nonché per avere un quadro completo generale degli investitori coinvolti. Il token rappresentante l'azione tokenizzata circola sulla blockchain che garantisce autonomamente la trasparenza e l'affidabilità del sistema iscrivendo nei propri blocchi gli indirizzi degli investitori che effettuano le transazioni. Gli investitori sono in questo modo anonimi o pseudo anonimi vista l'elevata difficoltà con cui si può risalire da un indirizzo al suo proprietario. L'anonimità, sebbene per l'adozione delle criptovalute abbia rappresentato un valore aggiuntivo, potrebbe risultare uno svantaggio importante che potrebbe in particolari situazioni scoraggiare una certa categoria di investitori, come quelli istituzionali, ad operare in questo sistema. La facilità e velocità di circolazione e di scambio del token da un investitore all'altro potrebbe generare facilmente delle dinamiche speculative che porterebbero nel breve termine suscitare spirali inflattive o deflattive risultato di un'estrema volatilità dei prezzi che, come risultato finale, condurrebbe ad un significativo scostamento del prezzo del titolo in questione rispetto al suo valore finale. Si creerebbero così delle considerevoli opportunità di

arbitraggio dovute al discostamento dei prezzi del titolo circolante nel mercato tradizionale e del token circolante su blockchain.

Inoltre, i token sono frazionabili e divisibili a differenza delle azioni che per legge, in quanto rappresentano il diritto di partecipazione ad una società di capitali, possono essere suddivise o scambiate solo unitariamente e interamente.

Infine, l'investimento in token al posto di un'azione potrebbe essere percepito dagli investitori come più rischioso e pertanto questi si aspetterebbero un rendimento maggiore; essendo però la rappresentazione virtuale di un'azione, il token non dovrebbe (a livello teorico) prospettare o offrire un rendimento maggiore in quanto la fonte dell'emissione sarebbe sempre la medesima società il cui valore è dato dalla sua capacità di generare utili e ricchezza per gli azionisti, tra cui rientrerebbero gli investitori in token. Per questo motivo la percezione di rischio maggiore, che si potrebbe palesare inizialmente, dovuta alla poca conoscenza della tecnologia blockchain e dei meccanismi di tokenizzazione da parte degli investitori, potrebbe portare all'aumento di domanda di copertura e di ricerca di assicurazione per l'esposizione all'investimento in un'azienda. Ciò porterebbe ad un incremento di diffusione di credit default swap (CDS) come assicurazione sul rischio di default dell'emittente delle azioni e token; l'acquisto di CDS comporterebbe un rischio maggiore per l'azienda emittente in quanto vengono utilizzati come proxy per misurare il rischio di fallimento di un emittente di un titolo [49].

Tutto questo ragionamento, che per attuarsi richiederebbe il verificarsi di una serie di eventi e condizioni, e le problematiche sollevate dallo stesso potrebbero risolversi attraverso una serie di considerazioni.

In primo luogo, il token emesso da una società avrebbe, a livello teorico, lo stesso valore di un'azione emessa dalla stessa; il token potrebbe rappresentare e surrogare pienamente l'azione garantendo la titolarità dei diritti di partecipazione attraverso vari meccanismi. Uno di questi è rappresentato dai già diffusi KYC ed AML ovvero dei processi attraverso cui si può verificare l'identità di un investitore ed evitare il riciclaggio di denaro. Ad oggi in Italia questi meccanismi sono adottati anche dagli intermediari finanziari e dalle banche e possono essere

[49] Parte delle considerazioni fatte in questo passaggio sono riprese dall'analisi svolta nel paragrafo 3.3 "Pricing Implications" del paper: OECD (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, OECD Blockchain Policy Series, www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential- Implications-for-Financial-Markets.htm.

implementati anche su blockchain codificandoli all'interno di uno smart contract. In questo modo, qualora si volesse investire in token invece che in azioni, si può chiedere al proprio investitore di verificarsi ed autenticarsi attraverso lo smart contract con il risultato di avere una lista completa, trasparente e affidabile di chiunque detenga la partecipazione in una società, il tutto circolante in maniera decentralizzata ed automatizzata.

Una soluzione più originale, per ovviare in parte ai problemi di prezzo, potrebbe essere l'implementazione di un nuovo meccanismo denominato "Proof-of-Knowledge" con cui si verifica e si permette l'accesso a questo particolare strumento finanziario (i token) solo ad investitori consapevoli che dimostrano di avere le conoscenze di base riguardo materia finanziaria e blockchain; come una specie di questionario MIFID per gli investimenti in attività on chain.

3.3.3 Problemi di custodia: sarà necessaria un'autorità centrale?

Dai problemi di prezzo appena descritti deriva l'aspetto principale che può minare lo sviluppo e l'adozione su larga scala di questi strumenti nonché rappresentare la soluzione finale: la custodia.

Con custodia si intende *"La detenzione e l'amministrazione, da parte di un ente incaricato, di titoli e altri strumenti finanziari di proprietà di terzi."* [50]. Questa funzione viene svolta da una sola entità centrale che, in maniera esclusiva, garantisce non solo l'esistenza del titolo ma anche la sua circolazione corretta. Il soggetto predisposto a svolgere l'attività di custodia è detto "custodian" ovvero *"Soggetto preposto alla custodia del patrimonio di un fondo e al controllo della gestione al fine di garantire il criteri di separatezza contabile e i principi di correttezza e di trasparenza amministrativa."* [51]

Si tratta perciò di un'attività centrale per il corretto funzionamento dei mercati finanziari tradizionali e che potrebbe, invece, rappresentare un paradosso per la finanza decentralizzata.

[50] Traduzione definizione "Custody" BCE: https://www.ecb.europa.eu/services/glossary/html/glossc.en.html
[51] Definizione "Custodian" Borsa Italiana: https://www.borsaitaliana.it/borsa/glossario/custodian.html#:~:text=Definizione,correttezza%20e%20di%20trasparenza%20amministrativa.

Come visto più volte la forza della blockchain su cui si basano tutte le operazioni di DeFi è proprio la sua capacità di non dover dipendere da un solo operatore centrale su cui tutti gli utenti devono obbligatoriamente fare affidamento.

Il problema nella finanza decentralizzata si pone in quanto, vista la facilità di creazione di un token il cui numero emesso può essere potenzialmente illimitato, vi possono essere dei casi in cui si presenta un netto discostamento del titolo "reale" rispetto a quello tokenizzato generando in tal modo caos tra gli investitori. Per ovviare a questo problema vi è bisogno che il titolo tokenizzato sia strettamente correlato, quasi sotto forma di un gemello digitale, al titolo reale. Ad oggi questo problema non è direttamente risolto dalla blockchain e pertanto vi è la necessità di creare un'autorità centrale che faccia da ponte tra il mondo on e off-chain. Uno dei compiti che questa autorità sarebbe chiamata a svolgere è quello di controllare che lo stesso titolo non venga tokenizzato su più piattaforme e circoli, di conseguenza, su diverse blockchain dando vita ad una possibile infinità di token diversi che rappresentino tutti lo stesso titolo; dovendo perciò garantire la copertura del token da parte di un unico asset reale [52].

È proprio su tale aspetto su cui stanno lavorando fortemente le autorità di regolamentazione onde evitare che il passaggio da finanza tradizionale a finanza decentralizzata si trasformi in una nuova bolla e crisi finanziaria. Essa, infatti, può giocare un ruolo importante per lo sviluppo di questi meccanismi imponendo regole che disciplinano la generazione di security token; in Svizzera, ad esempio, esiste già da anni una bozza di regolamentazione che detta quali sono i passaggi necessari da dover seguire per generare un token e realizzare un'Initial Coin Offering.

Tuttavia, diverse imprese operanti in questo settore, sebbene esse non siano ancora molte e nessuna di grandezza rilevante, stanno studiando diverse soluzioni per ovviare a questo problema senza dover necessariamente ricorrere all'istituzione di un'autorità centrale; lo scoglio più grande rimarrà comunque quello della regolamentazione in quanto le istituzioni governative avranno inevitabilmente l'ultima parola per far si che la tokenizzazione diventi la nuova realtà nel mondo finanziario.

[52] Parte delle considerazioni fatte in questo passaggio sono riprese dall'analisi svolta nel paragrafo 3.5 "The possible need for a central authority in a decentralised, tokenised world: the relevance of custodianship " del paper: OECD (2020), *The Tokenisation of Assets and Potential Implications for Financial Markets*, OECD Blockchain Policy Series, www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential- Implications-for-Financial-Markets.htm.

3.4 Come generare un token: le ICO

Il processo di creazione di una criptovaluta, ovvero il modo in cui questa viene distribuita sulla blockchain è detto Initial Coin Offering (ICO). Si tratta di un processo concettualmente semplice da comprendere ma nella pratica piuttosto complesso da realizzare in quanto le competenze richieste per realizzarlo sono diverse e con diversi gradi di specificità. In questo contesto verranno considerate solo le ICOs efficienti e supportate da un progetto reale e che pertanto non hanno come obiettivo quello di realizzare truffe. Negli ultimi anni questa pratica è stata notevolmente diffusa causando danni e perdite ingenti agli utenti e agli investitori. I motivi di queste perdite sono legati maggiormente alla scarsa sicurezza informatica e alla natura stessa del progetto di offerta delle criptovalute.

Gli step da seguire per realizzare un'Initial Coin Offering assomigliano fortemente a quelli che devono essere svolti per quotare una società nei mercati tradizionali, ovvero un'Initial Public Offering (IPO). Di seguito verranno elencati ed analizzati i passaggi necessari per realizzare entrambe le offerte iniziali per poi evidenziarne similitudini e differenze.

Un'Initial Coin Offering viene realizzata in sei passaggi fondamentali:

1. White paper: una sorta di business plan con cui viene redatto e spiegato il progetto che si vuole realizzare attraverso la creazione del token. In questa fase possono essere presenti accenni riguardo la "tokenomics", economia del token, e le specifiche degli smart contract che verranno utilizzati (necessarie competenze business e informatiche).
2. Legal opinion e fundrasing terms: fase in cui si analizza e stabilisce la compliance del progetto con i requisiti legali internazionali e specifici del paese in cui questo viene realizzato. Nei termini di emissione vengono invece indicati l'offerta totale di token generati nonché il loro valore unitario (necessarie competenze legali in collaborazione con quelle informatiche)
3. Marketing e investors list: in questa fase vengono raccolte le richieste dei primi investitori che vogliono aderire al progetto ed acquistare i token emessi, spesso con uno sconto applicato per favorirne la vendita. Sempre in questa fase il progetto ha preso forma e vengono svolte le attività di marketing per pubblicizzarlo sia ad investitori istituzionali che retail

4. Creazione smart contract: una volta stabiliti i termini di creazione del progetto, resi conformi con i requisiti normativi richiesti, vengono creati gli smart contract e progettati secondo le linee guida previste nel white paper. Queste sono verificabili liberamente dagli utenti in quanto nella maggior parte dei casi si utilizzano smart contract e token standard già esistenti oppure, nel caso di una nuova creazione, attraverso un'analisi più attenta che non richiede particolari sforzi in quanto il codice è open-source. (necessarie abilità informatiche avanzate)
5. Rilascio del token: una volta generati gli smart contract ed ultimata la prima revisione tecnica generale del progetto, il token viene rilasciato e diventa circolante sulla blockchain
6. Aggiornamenti e revisioni del software e token listing: in questa fase continuano periodici aggiornamenti e revisioni della componente del progetto legata al software e all'informatica, soprattutto riguardo il corretto funzionamento degli smart contract. Una volta ultimate le ulteriori verifiche il token può essere listato su exchange sia centralizzati che decentralizzati; in questo modo il mercato di riferimento si amplia e il token è messo a disposizione di un maggior bacino di investitori.

Che si tratti di una moneta virtuale, criptovaluta, o di un token, security/utility, i passaggi generali da dover seguire rimangono sempre questi. Il processo di emissione di un token security, frutto del processo di tokenizzazione di un asset finanziario, è detto Security Token Offering (STO) e segue esattamente gli stessi passaggi con l'unica differenza che i requisiti legali richiesti possono essere più o meno stringenti a seconda del paese in cui si vogliono creare [53]. La differenza tra coin e token risiede nella loro natura e nel loro scopo di utilizzo: i token, come visto precedentemente, sono la rappresentazione digitale di un bene o asset esistente nel mondo reale a cui pertanto può essere attribuito un valore e hanno una funzione specifica; le coin, o più genericamente criptovalute, sono monete elettroniche circolanti su

[53] Ad esempio, in Svizzera la FINMA ha previsto un requisito minimo di informazioni necessarie per poter realizzare un'ICO attraverso l stesura di una vera e propria guida pratica in modo da minimizzare il rischio di generazione di trufe e attività illecite: *"Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle initial coin offering (ICO)"* FINMA, 16 febbraio 2018

blockchain che rappresentano la valuta digitale nativa con cui vengono attribuite le ricompense generate dal corretto funzionamento della blockchain.

Il meccanismo con cui invece vengono quotate le società sui mercati tradizionali è quello delle Initial Public Offering; anch'esso scomponibile in sei fasi:

1. Predisposizione prospetto informativo: redazione di un documento apposito in cui inserire e spiegare chiaramente tutti i termini del progetto
2. Nulla osta CONSOB: l'autorità di vigilanza preposta analizza e giudica il prospetto informativo deliberando sulla possibile accettazione o rifiuto della proposta di quotazione
3. Sottoscrizione: fase detta di "underwriting" in cui viene individuato l'intermediario incaricato di promuovere e intrattenere i rapporti tra la società di prossima quotazione e i primi investitori istituzionali
4. Definizione termini di emissione: vengono definite il numero di azioni da emettere ed il relativo prezzo a cui quotarle inizialmente. Il processo di formazione del prezzo è continuo e non si esaurisce in un'unica fase e richiede spesso tempo e analisi apposite (due diligence) per individuare il fair value della società
5. Definizione tempistiche e modalità di collocamento: viene effettuato un road show per completare il processo detto di "book building", ovvero di annessione all'operazione da parte degli investitori iniziali. Vengono così definite le modalità di collocamento nonché il prezzo finale della quotazione
6. Collocamento sul mercato: le azioni vengono listate sui mercati tradizionali e possono essere liberamente scambiate

Le IPO sono solitamente più complesse e richiedono genericamente mesi per essere realizzate, l'elenco riportato sopra non è da considerarsi esaustivo ma deve essere interpretato come di carattere generale.

Come si può però notare i due procedimenti di offerta iniziale, che si tratti di un token o di un'azione, sono in linea di massima simili e raggiungo entrambi lo stesso risultato. Lo scopo per cui le aziende decidono di quotarsi è quello di raccogliere fondi sotto forma di capitale di rischio per finanziare progetti e sviluppi futuri; inoltre, permette alle quote di partecipazione di una società di essere scambiate su un mercato secondario il che comporta notevoli benefici

per la società emittente e per gli investitori. Allo stesso modo la generazione di un token attraverso un'ICO o STO permette ad una società già quotata di reperire nuovi capitali, diminuendo in prospettiva il costo del capitale, e ad una società non quotata di ottenere finanziamenti da parte di un maggior numero di investitori che normalmente non potrebbero accedere a questo genere di investimenti.

3.4.1 ICO o IPO preventiva

Come visto l'ICO/STO permette di generare il token rappresentante parte della quota di partecipazione in una società. Nella fattispecie in cui l'emittente di token fosse una società non quotata, l'ICO potrebbe rappresentare una specie di offerta pubblica preventiva ovvero effettuata prima di realizzare la vera quotazione sui mercati tradizionali.

Le differenze tra ICO e IPO riguardano maggiormente l'obbligo di assoggettarsi, da parte della società emittente, alla vigilanza di un'istituzione preposta che ha il compito di verificare i requisiti di legge e garantire che l'offerta pubblica non rappresenti un rischio di truffa per gli investitori. Sebbene la fase di controllo legale non manchi tra le fasi di offerta iniziale del token (ICO/STO), non si può affermare che questa sia equivalente al controllo che viene riservato alle operazioni di offerta pubblica iniziale di titoli azionari. Un'autorità garante e di vigilanza è di fatto mancante nel mondo blockchain e la sua istituzione rappresenterebbe un paradosso per lo sviluppo di questa tecnologia. È proprio su questi punti che si sta soffermando la regolamentazione e su cui vengono destinati i maggiori sforzi.

Nel caso di una società grande, sebbene non quotata, l'emissione autonoma di token per finanziare progetti di sviluppo potrebbe rappresentare una prova generale in vista di una possibile quotazione. Gli sforzi operativi richiesti da un'ICO sono inevitabilmente minori rispetto a quelli richiesti da un'IPO e possono essere sfruttati dalla società come base per l'intrapresa di un percorso diretto verso la quotazione in borsa. L'ICO o IPO preventiva, permetterebbe alla società emittente di testare anticipatamente il processo di offerta pubblica raccogliendo comunque dei fondi necessari per lo sviluppo. Da un punto di vista della regolamentazione, l'introduzione di adeguate norme potrebbe aiutare a generare una proxy del possibile successo della quotazione delle società permettendo di ottenere dati ed informazioni importanti prima

ancora dell'avviamento del processo di quotazione finale. Ad esempio, l'IPO preventiva, ovvero la tokenizzazione di una parte delle quote societarie attraverso un'ICO, potrebbe ridurre essenzialmente i tempi di definizione del prezzo di quotazione, aiutando sia la società emittente che gli intermediari preposti a realizzare una quotazione ad un prezzo che rispecchi il valore o fair value della società, evitando le forti correzioni del prezzo dei titoli subito dopo la quotazione in borsa a causa di una sopravvalutazione/sottovalutazione degli stessi [54] . Gli scambi dei token, infatti, possono fornire importanti informazioni riguardo le valutazioni e il sentiment degli investitori riguardo la possibile emissione di un titolo prima della sua futura quotazione, permettendo al mercato di valutare il titolo prima ancora della sua ufficiale emissione.

I problemi più grandi si verificherebbero nel momento in cui fossero società medio-piccole o addirittura start-up a voler emettere token per finanziare il proprio sviluppo e la propria crescita; per limitare questo rischio e il dilagare di strumenti rischiosi sulla blockchain è essenziale una figura già osservata all'inizio di questo documento: i Venture Capital.

3.5 Mera speculazione o slancio per l'innovazione?

Fino a questo punto la tokenizzazione è stata vista come un'alternativa dall'alto potenziale dell'odierno sistema finanziario, come una Borsa alternativa sulla quale effettuare scambi più velocemente e in maniera più diretta e semplice. Questa concezione avrebbe un limite concettuale riferito ad una semplice sostituzione di un meccanismo già esistente il cui sviluppo comporterebbe vantaggi e svantaggi già osservati.

Il potenziale della tokenizzazione, però, non si esaurisce qui; un meccanismo di scambio virtuale di valore, rappresentato non solo da monete virtuali o titoli digitalizzati, potrebbe avere un ambito applicativo estremamente ampio portando soluzioni innovative ad alta tecnologia ed efficienza in contesti diversi da quelli strettamente finanziari. Numerose aziende o attività che in generale richiedono un grande bacino di liquidità potrebbero trovare un forte beneficio nell'usufruire di questa tecnologia, permettendo nel futuro la realizzazione di progetti complessi

[54] fenomeno che si manifesta non raramente in seguito alle quotazioni in borsa il cui prezzo di emissione non rispecchia le valutazioni del mercato.

e con grandi barriere realizzative. In questo modo si amplierebbe la concezione della tokenizzazione aprendo le porte all'evoluzione del processo innovativo.

3.5.1 Come un Venture Capital può sfruttare la tokenizzazione per evolvere il proprio business ed accelerare l'innovazione

Uno dei settori in cui l'utilizzo della tokenizzazione comporterebbe un notevole incentivo e beneficio è quello dei Venture Capital.

Nel primo capitolo è stato descritto il funzionamento del settore, gli attori coinvolti, i meccanismi di investimento e di tutela dei rischi; la tokenizzazione avrebbe un impatto significativo in ognuno di essi.

Un Venture Capital, infatti, può sfruttare la tokenizzazione come metodo di raccolta dei capitali da investire nelle start-up o prendere in considerazione l'idea di aprire un'apposita business unit volta a tokenizzare le partecipazioni direttamente della start-up. Si tratta di due soluzioni all'apparenza simili ma con dei risvolti operativi diversi.

Nel primo caso un VC può tokenizzare una parte delle proprie quote di partecipazione, rivenderle agli investitori tramite blockchain raccogliendo in appositi round capitale da investire in una o più start-up. In questo modo potrebbe ottenere capitali non solo da investitori istituzionali o grandi investitori privati, come avviene nella normale prassi, ma potrebbe raccoglierli anche da piccoli investitori retail riducendo il rischio di investimento di capitale proprio e iniettando maggiore liquidità nel sistema. Questo meccanismo non sarebbe privo di rischi ma permetterebbe di bilanciarli attraverso l'intermediazione del processo di investimento, l'investitore infatti presterebbe i propri capitali al VC ricevendo in cambio token emessi dallo stesso e ottenendo in questo modo la possibilità di venderli ad altri investitori e liquidare la propria posizione in ogni momento senza dover interagire con l'emittente. Il VC sarebbe il solo autorizzato a decidere come investire i fondi raccolti scegliendo, in base alle logiche viste nel paragrafo 1.2, in quali attività o società investirli. L'utilizzo della blockchain permetterebbe in questo caso di ridurre anche i rischi di azzardo morale o quantomeno di rendere le decisioni prese dal VC più trasparenti e a disposizione degli investitori che potrebbero in ogni momento tracciare il flusso di denaro e osservare direttamente come questo viene gestito e indirizzato

verso i vari progetti. I vantaggi principali risiederebbero nella possibilità per gli investitori di riottenere liberamente e rapidamente i propri fondi o di speculare su essi; considerando il valore aggregato dell'acquisto e vendita di questi token si creerebbe un andamento storico del valore di questo strumento che, sotto un'ottica di valutazione, potrebbe rappresentare una proxy del consenso degli investitori riguardo le decisioni di investimento del VC e dei rischi che questo decide di sopportare. Allo stesso tempo questo processo potrebbe risultare simile all'attività di un fondo comune di investimento a gestione attiva, con l'unica differenza che i capitali raccolti sarebbero indirizzati a società più piccole e rischiose non quotate sul mercato tradizionale. Il processo appena descritto rappresenterebbe, ancora una volta, la sostituzione di un meccanismo già esistente e pienamente operativo, di semplice comprensione e con il quale gli investitori nel settore sono già familiari.

Il carattere rivoluzionario dei meccanismi di tokenizzazione troverebbe maggiore spazio nella seconda soluzione proposta ovvero l'apertura di un'apposita unità di business che si occupi di tokenizzare le partecipazioni delle start-up.

L'unità di business in questione avrebbe un business model simile a quello di diverse società che stanno nascendo, anche sotto forma di start-up, in questo periodo [55]. L'obiettivo è quello di permettere ad investitori retail così come ad investitori istituzionali o ad intermediari finanziari di inserire all'interno del proprio portafoglio la partecipazione diretta in start-up attraverso l'acquisto di un token emesso da un VC o dalla start-up stessa. L'attività principale svolta dal VC in questo contesto sarebbe quella di valutazione della start-up, secondo le proprie logiche[56], per stabilire un prezzo equo a cui vendere inizialmente il token, e successivamente svolgere un'attività di due diligence periodica con cui monitorare la crescita della società, esattamente come avviene nella sua attività normale. Dal punto di vista della start-up, quest'ultima otterrebbe accesso ad un maggior volume di capitali, reperibili in minor tempo e provenienti da una più vasta gamma di investitori con obiettivi diversi. In tal modo si ridurrebbe il costo del capitale e limitando l'ingresso di investitori all'interno della propria cap-table [57] ottenendo una minore diluizione delle partecipazioni. Il token emesso potrebbe rappresentare sia delle azioni/quote con diritto di voto, prassi più complicata da realizzare e da gestire a causa

[55] Come Seed Venture, Tokeny, Polymath, BlockInvest o società più affermate in Asia come ADDX
[56] Vedi paragrafo 1.2 *"Strategie di remunerazione di un VC e metriche di valutazione delle Start-up"*
[57] Tavola dei capitali: suddivisione delle quote di partecipazione societarie

dei requisiti legali che verrebbero richiesti, sia delle azioni/titoli senza diritto di partecipazione. In entrambi i casi l'emissione dei token genererebbe un mercato secondario dove ogni singola start-up può "quotarsi" e dove investitori di vario tipo possono scambiare i titoli eliminando i rischi di arbitraggio in quanto non esisterebbe un altro mercato dove scambiare questi strumenti. Il problema di custodia si potrebbe risolvere grazie alla presenza dei VC che permettono la generazione dei token e gestiscono i titoli sottostanti. Inoltre, il VC potrebbe, per rimanere in linea con il suo core business, ottenere una quota di partecipazione all'interno della start-up in cambio del servizio di tokenizzazione o in alternativa selezionare le start-up a cui permettere la quotazione on-chain e inserirle nel proprio portafoglio di gestione.

Attraverso questo meccanismo i progetti più complessi, idee di business o attività di ricerca che richiedono un ingente quantità di capitale, possono reperire i fondi di cui hanno bisogno senza dover ricorrere all'accentramento presso un unico grande investitore. Il beneficio per l'intero sistema economico così come per lo sviluppo scientifico sarebbe notevole in quanto, attraverso la tokenizzazione, si ridurrebbero significativamente le barriere all'entrata dovute al bisogno di capitali. Inoltre, investitori piccoli, ad oggi esclusi dalla possibilità di investire in società non quotate o in progetti troppo grandi, potrebbero diversificare i propri portafogli e i propri obiettivi di investimento. Allo stesso modo i grandi investitori, come quelli istituzionali, potrebbero beneficiare dell'ampliamento del volume di utenti attivi nel mercato attraverso la possibilità di generazione di liquidità in investimenti fino ad oggi considerati illiquidi.

I Venture Capital hanno l'opportunità di diventare il fulcro di questo meccanismo fungendo da leva ed impulso per l'innovazione generando un impatto reale, non solo sull'economia, ancora più grande di quello osservato fino ad oggi [58].

3.6 Regolamentazione Europea: MiCA

La prima proposta di regolamentazione in Europa riguardo il settore delle cripto-attività viene presentata dalla Commissione Europea il 24 settembre 2020 come parte di un più ampio pacchetto riguardante la finanza digitale volto a promuovere lo sviluppo tecnologico garantendo la stabilità finanziaria e la tutela dei consumatori. Il Consiglio Europeo ha adottato il mandato

[58] Vedi capitolo 1

negoziale sul regolamento dei mercati delle cripto attività, Markets in Crypto Assets Regulation (MiCA o MiCAR), il 24 Novembre 2021 raggiungendo un accordo provvisorio il 30 giugno 2022. L'Iter legislativo si è concluso in data 16 maggio 2023 con l'approvazione unanime del regolamento da parte del Consiglio Europeo in seguito ad una precedente approvazione del Parlamento Europeo avvenuta in data 24 aprile 2023. Il prossimo passo riguarda l'entrata in vigore di tale regolamento con l'inserimento all'interno della gazzetta ufficiale previsto intorno alla metà del 2024.

Come si evince dal comunicato stampa del 16/05/2023 delle ore 10:30 del consiglio europeo[59], l'obiettivo del MiCA è quello di assoggettare alla pratica comune, regolata attraverso le direttive MiFID, l'emissione di strumenti finanziari sottoforma di token circolanti su blockchain. In tal modo si vuole supportare l'evoluzione del contesto tecnologico all'interno del settore finanziario limitando i rischi per gli investitori ed evitando che questi si espongano a rischi dei quali non possono comprendere la vera entità.

Un altro obiettivo del regolamento è quello di regolare l'emissione di questi strumenti assoggettando ad una particolare disciplina le società che sono in grado di generarli; vengono inoltre imposti dei requisiti minimi di trasparenza standardizzati che il processo di emissione dovrà riportare. Il regolamento impone anche agli investitori attirati da questi strumenti di doversi identificare attraverso processi di KYC ed AML onde evitare il riciclaggio di denaro. Le informazioni dovranno pertanto circolare con lo strumento stesso e le controparti dovranno obbligatoriamente tenerne traccia e conservarle. Nello specifico il regolamento fornisce regole uniformi, da dover adottare da tutti gli operatori all'interno della comunità europea, riguardo:

- Emissione e negoziazione dei crypto assets
- Autorizzazione e supervisione dei fornitori di crypto assets e degli emittenti di token
- Protezione dei consumatori per l'emissione, negoziazione, scambio e custodia dei crypto assets
- Prevenzione degli abusi di mercato e la garanzia dei mercati delle cripto attività

Per garantire queste misure il regolamento prevede l'istituzione di un registro pubblico da parte dell'autorità europea degli strumenti finanziari e dei mercati (ESMA, European Securities

[59] Comunicato Stampa del Consiglio Europeo in seguito all'approvazione del regolamento MiCA, 16 maggio 2023 https://www.consilium.europa.eu/it/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/

and Market Authority) per i fornitori di servizi finanziari sottoforma di cripto attività che operano nell'Unione Europea.

3.6.1 Tipologie di asset e regole per gli emittenti

I cripto asset su cui il regolamento impone delle regole comuni da rispettare sul territorio europeo sono divisi in tre categorie principali:

1. Asset-referenced token (ART): crypto asset che si propone di mantenere un valore stabile nel tempo in riferimento ad un altro valore o diritto, o combinazione tra i due, come una valuta ufficiale di un paese sovrano; rientrano tra queste le Stablecoin
2. Electronic money token (EMT): crypto asset il cui scopo principale è quello di essere utilizzate come mezzo di pagamento che basa il suo valore in riferimento ad una moneta ufficiale di un paese sovrano
3. Utility token: crypto asset fungibile destinato a fornire accesso ad un bene o servizio fornito dall'emittente del token

Il MiCA verrà applicato a tutti i soggetti che si identificano negli emittenti e nei fornitori di servizi di cripto attività; in sostanza chiunque generi asset basati e circolanti su blockchain e chiunque offra qualsiasi tipo di servizio ad essi legato.

L'emissione di ART richiederà un'autorizzazione specifica e degli appositi obblighi di informazione, che verranno in seguito definiti dall'Autorità Bancaria Europea (EBA), e la costituzione di un "asset reserve" che servirà a sostenere il diritto di rimborso obbligatorio che gli investitori avranno nei confronti dell'emittente. Gli emittenti di ART hanno inoltre l'obbligo di detenere un capitale di vigilanza sottoforma di liquidità pari ad un minimo di 350.000€ o al 2% del valore degli asset detenuti come riserve. Questi avranno, inoltre, l'obbligo di adottare regole di condotta e governance pari a quelle degli istituti finanziari ed il white paper del progetto di emissione sarà soggetto a requisiti più stringenti.

Gli EMT, invece, potranno essere offerti solo da istituti di credito e di moneta elettronica autorizzati dalle leggi comunitarie e dalle rispettive normative nazionali. Anche in questo caso è presente un diritto di rimborso obbligatorio che l'emittente deve concedere agli investitori.

Per i fornitori di servizi di cripto attività (CASPs, crypto assets service providers) le regole imposte sono simili a quelle che la direttiva MiFID prevede per i soggetti che offrono servizi di investimento. Queste entità dovranno essere autorizzate ed iscritte in un registro tenuto dall'ESMA che permetterà, attraverso una procedura di "passporting", di fornire i propri servizi in tutta l'Unione Europea. I tempi di rilascio di queste autorizzazioni saranno più brevi rispetto a quelle per poter emettere ART, con una tempistica media che dovrebbe aggirarsi intorno ai tre mesi.

A livello generale si può dire che il MiCA segua la falsa riga della direttiva MiFID applicando le regole previste per il settore finanziario "tradizionale" a quello decentralizzato espandendo il regime di competenza non solo alla blockchain ma a tutte le soluzioni basate su registri distribuiti decentralizzati (DLT). [60]

[60] Fonti delle informazioni e risorse per possibili approfondimenti:
https://www.econopoly.ilsole24ore.com/2023/04/24/mica-crypto-regolamento-europa/#_ftn3
"Regolamento sui mercati delle cripto-attività (MiCA)", Consiglio Europeo, 16 maggio 2023
https://data.consilium.europa.eu/doc/document/PE-54-2022-INIT/it/pdf

4. CASE STUDY: The DAO & Seed Venture

La raccolta fondi tramite blockchain è una delle opzioni nate grazie allo sviluppo dell'ecosistema di Ethereum e alla sua capacità di dar vita a progetti ed iniziative raccolti dentro delle organizzazioni autonome decentralizzate (DAO: Decentralized Autonomus Organizations). Ad oggi esistono diversi progetti on chain che hanno come obiettivo quello di offrire servizi finanziari, ma la raccolta fondi intesa come investimento diretto in una società è una possibilità che è stata già testata in passato con un risultato fortemente negativo e lasciando scorie piuttosto importanti.

In questo capitolo verranno analizzati due case study scelti appositamente di cui il primo verterà su fatti accaduti in passato con l'intento di mostrarne le fragilità e sottolineare quali sono state le lezioni impartite e cosa fare per evitare che possano accadere di nuovo. Il secondo, invece, verterà sull'analisi di un'azienda nata negli ultimi anni che opera nel settore della tokenizzazione con lo scopo di permettere alle start-up di raccogliere fondi tramite blockchain.

4.1 The DAO: "boom and bust" del primo progetto on chain per raccogliere capitali

Prima di introdurre il caso di studio occorre specificare cosa sia una DAO e che differenza vi sia con il caso in questione. Una DAO, Decentralized Autonomus Organization o organizzazione autonoma decentralizzata, è un'organizzazione, intesa anche come impresa, che opera su blockchain in maniera decentralizzata senza la presenza di una figura centrale che dirige le operazioni. Sul portale di Ethereum riferito alle DAO [61] si può capire facilmente come queste siano pensate per essere delle vere e proprie aziende i cui dipendenti e dirigenti operano senza la presenza di un supervisore, come un CEO o CFO, in maniera democratica servendosi di regole programmate all'interno di smart contract e prendendo decisioni tramite votazioni effettuate direttamente sulla blockchain. Si tratta perciò di una sorta di cooperativa digitale che persegue una missione comune in accordo tra tutti gli stakeholders, *"Hanno*

[61] https://ethereum.org/en/dao/

tesorerie integrate a cui nessuno ha l'autorità di accedere senza l'approvazione del gruppo. Le decisioni sono regolate da proposte e votazioni per garantire che tutti i membri dell'organizzazione abbiano voce in capitolo, e tutto avviene in modo trasparente on-chain." [62]

The DAO, invece, è il nome del progetto, nato sottoforma di organizzazione autonoma decentralizzata, creato da alcuni sviluppatori di Ethereum con lo scopo di operare come un fondo di Venture Capital per il mondo cripto. Il nome originale di tale progetto era Genesis DAO passato alla storia come "The DAO" per gli avvenimenti che verranno di seguito descritti.

The DAO nasce nel 2016 come progetto pioneristico e rivoluzionario nel mondo blockchain, prima ancora che le criptovalute diventassero l'oggetto dei dibattiti quotidiani del mondo finanziario con lo scalpore che oggi tutti conosciamo. Questa organizzazione è stata sviluppata esclusivamente attraverso smart contract, per raccogliere capitali con lo stesso meccanismo di funzionamento del crowdfunding. Gli investitori potevano scegliere arbitrariamente quale progetto supportare scambiando i propri ether (ETH), valuta digitale della blockchain di Ethereum, con il token generato dal protocollo dell'organizzazione dal nome DAO (per evitare confusione e fraintendimenti d'ora in avanti il token generato da The DAO verrà chiamato all'interno di questo documento "DAO-T")[63], con un rapporto di cambio di 1 a 100. La piattaforma permetteva a chiunque di presentare il proprio progetto o la propria idea alla comunità, formata sia da investitori che soggetti privati, e ricevere potenzialmente dei finanziamenti direttamente da The DAO. Chi acquisiva i token DAO-T otteneva il diritto di votare quale progetto supportare, e quindi a quale idea destinare finanziamenti, e di ricevere ricompense nel caso in cui il progetto votato avesse ottenuto successo e realizzato profitti.

The DAO raccolse subito grande successo stimolando gli utenti ad utilizzare le criptovalute in un modo alternativo che potesse generare valore non solo per loro stessi. Nel periodo di lancio, 30 aprile 2016-28 maggio 2016, raccolse un totale di 12,7 milioni di Ether (ETH) da circa 11.000 investitori, per un valore stimato all'epoca pari a 150 milioni di euro. Questo valore è anche cresciuto a causa della volatilità di Ether raggiungendo un picco di 250 milioni di euro quando ETH ha raggiunto il prezzo di 20$; ad oggi, grazie alla crescita del prezzo di Ether (ETH) quella somma sarebbe intorno ai 20 miliardi di euro.

[62] Traduzione dal portale Ethereum per le DAO: https://ethereum.org/en/dao/
[63] DAO-T: nome fittizio utilizzato solo all'interno di questo documento per identificare il token generato da The DAO

[64]

Le premesse erano pertanto ottime: il progetto sembrava essere promettente, gli investitori avevano assunto un atteggiamento positivo e scommesso nel complesso un'ingente somma di denaro, la più grande mai raccolta in così breve tempo da un unico soggetto, e i DAO-T potevano inoltre essere scambiati su exchange decentralizzati aprendo lo spazio al mercato secondario.

Il successo di questa piattaforma cresce alla stessa velocità che la stessa ha impiegato per fallire e passare alla storia come uno dei progetti più controversi del mondo blockchain minando irreparabilmente la fiducia degli utenti. Il 17 giugno 2016, dopo neanche tre mesi dal lancio, The DAO subisce un attacco hacker che causa la perdita, nell'arco di poche ore, di 3,6 milioni di Ether (ETH), pari a quasi il 30% del totale dei fondi raccolti; il controvalore in euro di questa perdita era di circa 70 milioni.

Il caso attirò l'attenzione non solo degli utenti ma anche delle istituzioni di vigilanza; la Securities and Exchange Commission (SEC), istituzione statunitense di vigilanza sui mercati, indagò sull'accaduto. Il caso fu trattato allo stesso modo e con gli stessi principi che regolano la quotazione in borsa delle società e terminò, come si evince dal report della SEC, con la

[64] Andamento del valore di Ether (ETH): valori settimanali

constatazione che The DAO, così come gli investitori coinvolti, ha violato le leggi federali sui titoli mobiliari e sull'emissione di strumenti finanziari [65].

Prima della pronuncia della SEC, pubblicata in data 25 luglio 2017, il token DAO-T era stato delistato dai principali exchange e la sua vendita repentina causò il fallimento di The DAO.

4.2 Implicazioni e cause del fallimento

Sulla pagina web di The DAO appariva la scritta "*The DAO is code"* (The DAO è codice) ad indicare cosa fosse veramente l'organizzazione e quale fosse veramente il suo punto di forza. Il codice, però, è risultato essere anche la più grande vulnerabilità dimostrando come la sicurezza informatica, come ci si poteva aspettare da un sistema basato su scambi ed interazioni virtuali, fosse l'aspetto centrale da dover considerare nella creazione di un progetto basato su blockchain.

L'hacker fu in grado di sfruttare un malfunzionamento (bug) del codice con cui era stata progettata la piattaforma e in particolare gli smart contract che la governavano; un errore di programmazione che era stato segnalato dalla stessa comunità e sul quale il team di sviluppo di The DAO non fece in tempo ad intervenire. Lo stesso codice dello smart contract, però, si rivelò essere l'unico appiglio a cui gli investitori potettero aggrapparsi: tra i termini dello smart contract vi era una "clausola" che imponeva a chi voleva ritirare i fondi, un holding period di 28 giorni all'interno di un wallet controllato da The DAO. Gli hacker non furono perciò in grado di sottrarre la somma derubata che venne pertanto restituita agli investitori non senza conseguenze.

Per restituire il denaro sottratto durante l'attacco furono proposte diverse soluzioni provenienti da diversi utenti, una di queste persino dal creatore di Ethereum Vitalik Buterin che propose di bloccare il wallet su cui erano stati depositati i fondi. Il gruppo di hacker, sebbene non ancora identificato, spedì una lettera alla comunità di Ethereum affermando di aver ottenuto quel denaro in maniera "legale" dichiarando di aver operato seguendo i termini codificati all'interno dello smart contract. A livello puramente teorico, se lo smart contract contiene le

[65] *"Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO";* Release No. 81207 / July 25, 2017

"leggi" con cui si può interagire con la piattaforma e queste leggi presentano un errore che pregiudica gli interessi di terze parti, a doverne rispondere sarebbe il "legislatore" ovvero colui il quale ha creato le regole codificate nello smart contract (quindi in questo caso The DAO)? Allo stesso tempo, però, bisogna riconoscere che gli investitori erano consapevoli del rischio a cui andavano incontro essendo il codice dello smart contract pubblico e consultabile da chiunque; sarebbe pertanto giusto che gli stessi paghino per una loro disattenzione? Chi risponderebbe se una sentenza di un giudice, che favorisce ampiamente una controparte a scapito della/e altre, fosse stata emanata sulla base di un errore di ortografia presente all'interno del contratto che regola gli obblighi assunti dalle controparti?

A completare il quadro vi è però l'intenzione con cui l'azione è stata perpetrata, ovvero quella di trarre ingiusto vantaggio a scapito di una moltitudine di investitori; l'errore era stato infatti individuato ed era prossimo ad essere corretto, l'operato degli hacker è quindi senza dubbio da condannare in quanto hanno ingiustamente giovato di una condizione avversa che gli altri utenti hanno contribuito ad individuare senza però volerne approfittare.

La situazione, che evidenziò non solo problemi tecnici ma anche l'esistenza di aspetti morali ed etici nell'operare tramite blockchain, venne risolta attraverso un hard fork[66] della blockchain di Ethereum. Dopo lunghi dibattiti che questionarono i principi fondanti su cui era stata creata la tecnologia blockchain e più in generale dei registri distribuiti, il 20 Luglio 2016 al blocco 192.000 Ethereum si aggiorno permettendo ai nodi di scegliere se accettare o meno questo nuovo aggiornamento che prevedeva, tra le altre cose, lo spostamento dei fondi, in quel momento bloccati sul wallet di The DAO gestito dallo smart contract "malato", su uno smart contract "sano" permettendo agli investitori originali di recuperare i propri fondi. Non tutti i nodi aderirono al fork e perciò si crearono da quel momento due blockchain distinte: (i) Ethereum: quella aggiornata in cui confluirono tutti i nodi favorevoli all'aggiornamento, la maggior parte di quelli esistenti; (ii) Ethereum Classic: nella nuova blockchain generata dall'hard fork confluirono tutti i nodi che erano contro all'aggiornamento dando vita ad una nuova criptovaluta nativa: Ethereum classic (ETC).

[66] Vedi paragrafo 2.1.2

4.2.1 Considerazioni sul caso

La vicenda di The DAO ha sollevato notevoli dubbi e perplessità tra gli utenti di Ethereum e di tutto il mondo blockchain ed ha per certo cambiato la storia di questa tecnologia. Si tratta di un caso all'apparenza semplice ma solleva un certo numero di considerazioni che potrebbero essere fatte e lascia dietro di sé una scia di insegnamenti che mostrano cosa non deve essere fatto se si vuole creare un progetto su blockchain.

In prima istanza si potrebbe discutere sul business model di The DAO, sui suoi punti di forza, di debolezza nonché sulla validità del progetto e se questo potesse essere un vero aiuto per lo sviluppo di idee ingegnose ed innovative, o un mero strumento di speculazione. Di certo quello che rimane sono solamente gli aspetti negativi ed i punti critici di questa organizzazione che aveva iniziato forse in modo troppo promettente offuscando le capacità di valutazione dei rischi a cui gli investitori andavano incontro. Tra questi bisogna inevitabilmente considerare alcuni aspetti oltre a quelli tecnici e di sicurezza già ampiamente osservati. Vi sono alcune lacune riguardo la capacità ed il metodo con cui The DAO avrebbe rimborsato i propri investitori, vi sono dubbi sulla valutazione dei progetti, sui requisiti che questi avrebbero dovuto rispettare e sull'affidabilità degli imprenditori dietro gli stessi. The DAO non presentava alcun meccanismo di valutazione del valore effettivo dei progetti che ottenevano capitali sulla piattaforma, prometteva di restituire ricompense basate sulla crescita degli stessi ma non forniva strumenti per valutarli accuratamente lasciando gli investitori scoperti ad un rischio sia di azzardo morale, in quanto i prenditori di fondi non fornivano assicurazioni ma una semplice idea di business, sia di successiva sottovalutazione/ sopravalutazione della propria partecipazione. Inoltre, non essendo definito un meccanismo di ricompensa standard, il valore della partecipazione al progetto avrebbe potuto subire forti oscillazioni dovute alla volatilità del prezzo di ETH a cui era ancorato, con un rapporto di cambio fisso, il valore del token DAO-T.

Queste ed altre considerazioni potrebbero essere fatte ma sfortunatamente, a causa degli eventi descritti, non vi sono sufficienti informazioni per valutare correttamente l'idea di business portata da The DAO; ogni tipo di giudizio o considerazione sarebbe basata su ipotesi e su previsioni di un possibile scenario che si è rivelato, però, nefasto. Gli insegnamenti che The DAO lascia sono estremamente importanti per chiunque volesse creare progetti basati su tecnologia blockchain o per chiunque volesse lanciare una propria organizzazione

decentralizzata. Anche gli stessi regolatori possono imparare molto da questa vicenda intuendo come gestire e come regolare i punti nevralgici di debolezza di The DAO.

Sicuramente il tema della sicurezza informatica è centrale, ma si potrà mai intervenire per raggiungere un livello di garanzia del 100%? La tecnologia è in continuo sviluppo e il prossimo step evolutivo sembra essere alle porte; l'unico modo per limitare i rischi provenienti dall'informatica e dalla programmazione è conoscerle. Occorre apprendere e padroneggiare le competenze necessarie, competenze e capacità che ogni giorno diventano sempre più specifiche. In un prossimo futuro, con l'avvento dell'intelligenza artificiale sarà ancora più complesso apprendere il funzionamento di questi meccanismi e affidarsi ai propri mezzi potrebbe non essere sufficiente.

Dal punto di vista dell'utente quello che oggi si può fare è valutare, quanto più precisamente possibile, i rischi provenienti da progetti on-chain. Tra le cose a cui guardare per prime vi è il piano strategico; The DAO ha destato tanto scalpore per le conseguenze e per l'impatto che il suo fallimento ha avuto perché gli investitori sono stati attratti dalla foga del momento guardando solo al fascino che aveva senza osservarlo nel complesso. Per capire tutte le caratteristiche di un progetto e l'affidabilità dello stesso bisogna, come minimo, verificare la presenza di un white paper e valutare l'organizzazione (centralizzata o decentralizzata che sia) che lo pone in essere. Proprio su questi punti si stanno facendo grandi passi in avanti sia per consapevolizzare gli investitori sia per tutelarli legalmente; l'approvazione del MiCA[67] imporrà parametri stringenti e standardizzati per la realizzazione di questi progetti e ci si auspica, pertanto, che casi come The DAO non si ripetano in futuro.

[67] Vedi paragrafo 3.6

4.3 Seed Venture: l'innovazione made in Italy

Prima di analizzare il caso relativo ad una delle start-up italiane più promettenti operanti nel panorama blockchain e web3, si vuole ringraziare il team di Seed Venture[68] e in particolare il CTO Gabriele Soranzo per aver concesso l'analisi di questo caso fornendo direttamente le informazioni durante una serie di interviste.

Seed Venture è una start-up italiana nata nel 2018 a Londra dall'idea dei due founder originari, Sergio De Prisco e William Pividori, di creare un ponte che collegasse l'economia reale alla finanza decentralizzata. Il progetto si basa sul meccanismo di tokenizzazione, accessibile tramite piattaforma web, che permette agli investitori ed utenti attivi del mondo crypto di accedere ad una più vasta tipologia di asset class rappresentata dalle partecipazioni in start-up e idee di business.

Simile ad una piattaforma di crowdfunding, Seed Venture permette da un lato alle imprese di raccogliere fondi e capitali attraverso la blockchain totemizzando una parte delle proprie partecipazioni; dall'altro, permette agli investitori interessati, e non solo, di allocare i propri capitali a sostegno di idee e progetti innovativi che possano generare un impatto futuro e generare un ulteriore flusso di rendita.

Ciò che contraddistingue Seed Venture dagli altri competitor sul mercato, e che rappresenta un carattere forse unico o quantomeno molto raro in questo settore, è la volontà ferrea di rimanere compliant con le normative nazionali ed europee. Come visto in precedenza la maggior parte dei progetti sviluppati su blockchain negli ultimi anni contenevano grandi punti di vulnerabilità e agivano sfruttando le lacune regolamentari, trasformandosi in molti casi in truffe o scandali finanziari di cui si è anche sentito molto parlare nell'arco del biennio 2022-2023 [69]. Seed Venture si differenzia nettamente collaborando direttamente con le istituzioni italiane, come Consob e Banca d'Italia, per rispettare i requisiti ed ottenere le autorizzazioni necessarie prima di lanciare sul mercato la sua piattaforma.

I primi anni di sviluppo, sostenuti da un importante network di finanziatori ed investitori provenienti dal mondo del Angel Investing e Venture Capital, si sono concentrati sulla costruzione dell'infrastruttura tecnologica e sulla creazione di un team valido e competente che

[68] https://www.seedventure.io/contributors/

[69] Vedi fallimento di FTX, exchange centralizzato fallito in maniera fraudolenta che ha generato molto scalpore nell'ultimo anno.

potesse portare all'interno di Seed Venture le risorse tecniche ed il know-how necessario. Tra il 2019 ed il 2020 vengono realizzate le operazioni preliminari necessarie per il corretto sviluppo futuro, viene implementato il primo MVP, istituiti accordi con partner professionali e viene completata la creazione del proprio ERC – 20 token "SEED", distribuito attraverso la blockchain di Ethereum. Nel biennio successivo, 2021-2022, viene realizzata la piattaforma e l'interfaccia web con un design intuitivo ed user-frinedly; viene inoltre raggiunto un ulteriore traguardo importante ovvero l'aggiunta del Polygon layer, che permetterà di operare su una struttura blockchain meno costosa, più rapida ed efficiente basata sulla sicurezza di Ethereum.

L'obiettivo più importante che Seed Venture vuole raggiungere nell'arco del 2023 è l'ottenimento delle licenze necessarie per operare in Europa e nell' UK ed entrare inizialmente nel mercato italiano per poi espandersi a tutta l'Unione Europea.

4.3.1 Business model e processo di tokenizzazione

Il business model di Seed Venture si fonda su alcuni concetti legati prevalentemente al funzionamento del mondo crypto e di alcune pratiche note e con cui gli utenti sono già familiari. Il funzionamento di questo modello è piuttosto articolato e verrà presentato nel suo complesso con una particolare attenzione alla tokenizzazione delle partecipazioni delle start-up.

Un aspetto centrale, intorno a cui ruota parte del modello di ricavi ed incentivi proposto da Seed Venture, è costituito dalla criptovaluta "SEED" ovvero un token ERC – 20 circolante sulla blockchain di Ethereum e sul suo layer secondario Polygon. Si tratta di un token emesso direttamente da Seed Venture con una total supply di 300 milioni di cui un terzo, pari a 100 milioni, detenuti esclusivamente da Seed Venture[70] e al momento non listato su alcun exchange centralizzato. Il possesso di questi token permette ai proprietari di poter sia speculare sul prezzo sia di incassare delle ulteriori fee date dallo staking degli stessi.

Lo staking consiste in un meccanismo attraverso cui l'investitore invia i token SEED ad uno smart contract, appositamente generato da Seed Venture, che restituisce una quantità uguale di token wrappati che rappresentano il diritto di poter riottenere l'ammontare immesso

[70] Maggiori informazioni su questo token disponibili sulla piattaforma Etherscan in grado di mostrare in tempo reale i movimenti delle criptovalute che circolano sulla blockchain di Ethereum: https://etherscan.io/token/0xc969e16e63ff31ad4bcac3095c616644e6912d79

più le fee maturate dagli scambi sul mercato secondario. Detenendo un terzo di tutti i SEED messi in staking, Seed Venture potrà sempre incassare la stessa proporzione delle fee generate da tutto il sistema.

Entrando più nello specifico del business model, i ricavi principali nonché il principale apporto innovativo sviluppato ed offerto da Seed Venture è fornito dal meccanismo che permette alle start-up di raccogliere fondi in maniera decentralizzata.

Quando una start-up vuole finanziarsi in maniera alternativa, può rivolgersi al portale di Seed Venture[71] che funziona in modo simile a quelli delle piattaforme di crowdfunding[72] in cui viene disposta una vetrina di progetti con le rispettive campagne di raccolta di capitali tra cui gli investitori possono scegliere di investire. La piattaforma progettata da Seed Venture non è aperta a tutti i progetti, ma occorre superare alcuni step di selezione per potervi avere accesso. La start-up manda la richiesta di accesso alla piattaforma compilando un modulo online in cui inserisce una serie di informazioni preliminari; queste informazioni vengono valutate inizialmente da un gruppo di valutatori inviati dal team di Seed Venture, composto da professionisti del settore Venture Capital e Private Equity, che rappresenta un primo filtro nella verifica dell'adeguatezza del progetto e la consistenza delle informazioni onde evitare che i progetti possano contenere truffe o caratteri di illegalità.

Una volta terminato l'intero processo di verifica, il risultato viene mandato direttamente alla start-up e qualora l'esito fosse positivo si avrebbe accesso allo step successivo. Si tratta di un passaggio "tecnico" in cui la start-up deve creare un'istanza su un server, che può essere fornito da Seed Venture in collaborazione con Amazon Web Services (AWS), in cui inserire tutte le informazioni che andranno a riempire la campagna di raccolta fondi. Le informazioni richieste in questa fase sono standardizzate in modo da obbligare tutti i vari progetti a fornire lo stesso set informativo e rendere più trasparente la scelta di investimento dei futuri investitori. Si ricorda che, trattandosi per la maggior parte dei casi di start-up innovative ancora in fase di creazione/crescita, le informazioni a cui un investitore può avere accesso sono limitate e di vitale importanza sia per poter stabilire un valore approssimativo del progetto, sia per poter prendere accuratamente una decisione sul proprio investimento.

[71] In attesa delle necessarie autorizzazioni per essere lanciato al pubblico e diventare pienamente operativo
[72] Vedi ad esempio Mamacrowd: https://mamacrowd.com/it/

Ultimata questa fase la start-up, avvalendosi facoltativamente della consulenza di Seed Venture, effettua il deploy del proprio smart contract sulla blockchain che contengono i token che gli investitori potranno acquisire. Questa fase, ricordando anche l'esempio di The DAO, è estremamente delicata e richiede un certo livello di competenza. Per questo gli smart contract che verranno distribuiti sono sviluppati internamente da Seed Venture e sottoposti a forti stress test da parte di aziende terze. I test sono detti anche di "penetrazione" e si focalizzano sia sull'analisi dinamica che statica in modo da misurare e valutare il grado di sicurezza del codice ed evitare che attori malevoli possano sfruttare dei bug a scapito della comunità come successo con The DAO.

Superate tutte le fasi di verifica la campagna di raccolta fondi della start-up viene pubblicata sulla piattaforma online di Seed Venture e gli investitori possono arbitrariamente scegliere presso quale progetto allocare i propri fondi. Quando un investitore decide di puntare su un progetto ed investirci può acquistare direttamente il token della start-up (da qui SUP-token) sulla piattaforma sottoponendosi ad un processo di verifica. Questo processo, noto con il nome di KYC (know your customer), è fornito da terze parti e serve per constatare e verificare l'identità dell'investitore il quale dovrà, inoltre, rispondere obbligatoriamente al questionario per l'antiriciclaggio di denaro, AML (anti-money laudering), e fornire gli estremi dell'indirizzo (address) del proprio wallet blockchain da cui verrà effettuato il pagamento e su cui verranno depositati i token. In tal modo l'intero procedimento di investimento ha raccolto tutte le informazioni necessarie e richieste dalle autorità di vigilanza ed è pertanto reso compatibile con le normative europee. Il riconoscimento dell'investitore è essenziale e non può essere evitato o eluso in quanto gli smart contract distribuiti dalle start-up sono progettati per accettare ed effettuare transazioni solo con indirizzi verificati che hanno superato il processo di KYC.

L'investimento, e quindi il pagamento allo smart contract per ottenere i SUP-token, può essere effettuato solo attraverso Stablecoin e non tramite valuta fiat [73]. Una volta inviati i token di pagamento (Stablecoin come USDT) allo smart contract, l'investitore riceverà il corrispettivo di SUP-token secondo il rapporto di cambio prestabilito dalla start-up che permetterà all'investitore di dimostrare la propria partecipazione nella società. La garanzia del

[73] Su questo aspetto Seed Venture sta lavorando per inserire un plug-in nella piattaforma che consenta la conversione istantanea, secondo i prezzi di mercato, dalla valuta fiat alla rispettiva Stablecoin (ad esempio da EUR a USDT)

funzionamento di questo meccanismo è data da due fattori: (i) l'emissione del token da parte della start-up si configura legalmente come uno strumento di finanza partecipativa (SFP); (ii) l'emissione di questo strumento viene iscritta, con apposita clausola, all'interno dello statuto della società e pertanto si legittima il fatto che chiunque dimostri il possesso di questo strumento, quindi del SUP-token, ha diritto ad ottenere una quota prestabilita della rispettiva società.

Al termine della campagna di raccolta fondi la start-up riceverà i fondi investiti dagli investitori diminuiti di una percentuale, compresa tra l'1% ed il 5%, che rappresenta una specie di costo del servizio corrisposto a Seed Venture. Questa piccola porzione dei fondi raccolti, formata sempre da Stablecoin, viene indirizzata non nelle casse di Seed Venture, che altrimenti opererebbe come una normale piattaforma di crowdfunding, ma verso uno strumento che rappresenta il vero fattore chiave per la scalabilità di questo business model.

La fee corrisposta a Seed Venture è destinata alla creazione di una liquidity pool presso un exchange decentralizzato, come Uniswap, attraverso cui i fornitori di liquidità può incassare le commissioni di trading sugli scambi che vengono effettuati su questo bacino di liquidità[74]. Si verranno a formare in futuro tante liquidity pool quante le società che si finanziano attraverso questo meccanismo.

Le liquidity pool funzionano attraverso la fornitura di liquidità attraverso il deposito di una coppia di valute; in questo caso l'accoppiamento, in gergo tecnico chiamato "pair", di valute avviene tra il SUP-token wrappato (da ora WSUP-token) e la Stablecoin con cui è stato fatto il pagamento. Un token si dice wrappato quando il suo valore viene ancorato a quello di un altro asset, in questo specifico caso la necessità di "wrappare" il SUP-token è data dal processo di KYC effettuato dall'investitore. Quando il token circola sul mercato secondario, lo farà sottoforma di WSUP-token in modo tale da obbligare il futuro possessore, che vorrà riscuotere la propria partecipazione nella start-up, a sottoporsi al processo di verifica KYC e ottenere il SUP-token e perciò il suo diritto partecipativo.

[74] Si possono trovare approfondimenti sul funzionamento delle liquidity pool nella Binance Academy: https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi

La scommessa che Seed Venture fa per rendere il suo revenue model altamente scalabile è che si generi un forte movimento speculativo nella liquidity pool che generi a sua volta un grande ammontare di commissioni.

Ogni volta che viene effettuata uno scambio sulla liquidity pool il fornitore di liquidità, ovvero lo smart contract che ha depositato la coppia di valute (Stablecoin e WSUP-token), incassa una commissione. Questa commissione potrà essere reclamata da coloro i quali hanno messo in staking i token SEED e pertanto un terzo di queste spetterà sempre a Seed Venture. Chi fa il claim del reward generato dallo staking dei SEED riceverà in parti proporzionali sia la Stablecoin che il WSUP-token permettendo in questo modo a Seed Venture di ottenere un guadagno diretto, dato dal valore della Stablecoin, e la partecipazione diretta nella start-up che si è finanziata.

Infine, tutto questo meccanismo permette a Seed Venture di basare i propri ricavi in funzione dei movimenti che si generano sulla liquidity pool superando i limiti di scalabilità che devono sopportare le piattaforme di crowdfunding. Come per i normali Venture Capital, non occorre che tutte le start-up che si finanziano ottengano successo, ma basta che anche solo una di queste diventi un unicorno per generare un ritorno esponenziale per Seed Venture.

4.4 Possibili sviluppi futuri

Questi due case study dimostrano come l'intero panorama blockchain e web3 debba fare ancora passi in avanti ma che tuttavia si trova sulla strada giusta. The DAO ha evidenziato alcune delle principali fragilità e punti di debolezza che l'evoluzione del settore finanziario può presentare mentre Seed Venture dimostra come queste possano essere eliminate rimanendo compliant con le normative vigenti. Ciò che emerge maggiormente è la necessità dell'intervento del regolatore e la definizione di regole d'ingaggio comuni non solo nel panorama europeo ma nel mondo intero. Essendo la tecnologia blockchain di fatto senza limiti territoriali ed essendo essa raggiungibile ed azionabile da ogni parte del mondo, la soluzione migliore per il più efficiente e sicuro sviluppo futuro sarebbe un'omogeneità di trattamento a livello normativo diffusa e condivisa da tutti i paesi e dai rispettivi governi. Chiaramente si tratta di un'utopia in quanto è altamente improbabile, per non dire impossibile, che vi sia, quantomeno nel breve-medio termine, una visione condivisa di trattamento di questo tipo di tecnologia e delle sue applicazioni pratiche.

Le decisioni dei legislatori mondiali saranno la determinante principale per segnare il percorso evolutivo ed i conseguenti risvolti nonché l'adozione della tecnologia blockchain e web3. La sensazione ad oggi è che si tratti di un mondo complesso che si è affermato rapidamente e senza un preciso controllo, un settore particolare governato solamente dalle azioni dei singoli utenti in cui l'ordine viene stabilito "democraticamente". Un mondo creatosi alle spalle della finanza tradizionale dalla quale trae però inevitabilmente ispirazione con l'intento di provare a risolverne le principali inefficienze.

Un futuro in cui la finanza sarà totalmente decentralizzata appare oggi molto lontano ma un'integrazione/cooperazione con la finanza tradizionale potrebbe essere una realtà molto prossima. Le più grandi banche di investimento stanno sviluppando, testando ed investendo nei propri dipartimenti di DEFI e allo stesso tempo l'attenzione di sempre più investitori è diretta nella stessa direzione. Si sta pian piano superando il concetto di mera speculazione legata alle criptovalute e Seed Venture ne è la dimostrazione.

La tokenizzazione in particolare rappresenta una possibilità concreta di creazione di un legame solido e stabile tra le due tipologie di finanza innovando nella soluzione delle problematiche più complesse. Gli stessi Venture Capital dovrebbero cogliere l'occasione non

solo per aumentare i propri profitti ma per dare un ulteriore slancio all'innovazione. L'impatto reale che l'adozione di questa pratica e più in generale che la collaborazione tra finanza tradizionale e decentralizzata può generare ha una portata immensa ed incalcolabile. Basti pensare a progetti di ricerca, idee di business originali e complesse che ad oggi non riescono a trovare i giusti finanziamenti, che possono avere l'opportunità di essere sostenuti non solo da grandi istituzioni ma da un'intera comunità decentralizzata. Tutti attori che possono intervenire in ogni momento calcolando i rischi in maniera trasparente e senza dover fare necessariamente affidamento ad intermediari riducendo le notevoli asimmetrie informative del settore.

Le fasi da dover superare affinché tutto ciò diventi realizzabile sono ancora tante ma ci sono tutti i presupposti per far si che esse vengano affrontate nel miglior modo possibile. Ci troviamo oggi agli albori di una nuova era, vedremo se e tra quanto questa prospettiva di futuro diventerà realtà.

CONCLUSIONI

Nel corso di questo elaborato si è cercato di analizzare come si potesse incentivare l'innovazione attraverso l'uso delle nuove tecnologie. Nello specifico è stato preso in considerazione il binomio Venture Capital e Blockchain come possibile soluzione applicabile ed è risultato essere effettivamente un'alternativa concreta per incentivare e supportare il processo innovativo.

I Venture Capital sono i soggetti che più di tutti permettono alle piccole realtà, ad i progetti avveniristici e alle idee di business più innovative di raggiungere il successo che meritano. I dati, riportati all'interno del primo capitolo, mostrano i risultati ottenuti fino ad ora ed evidenziano l'impatto reale che le società cresciute con l'aiuto di VC hanno avuto nell'economia. È pertanto inevitabile che i soggetti che più possono influire nel successo di una start-up sono quelli che più possono beneficiare dell'avvento delle nuove tecnologie.

La tecnologia blockchain è stata individuata come principale mezzo attraverso cui si possono sia risolvere alcune delle problematiche relative alla finanza tradizionale, sia efficientare il processo di investimento di un VC rendendolo più trasparente e dinamico.

Attraverso la tokenizzazione, processo analizzato nel terzo capitolo, si può offrire l'acceso ad una nuova ed inedita asset class, fino ad oggi destinata solo agli investitori istituzionali o a pochi grandi imprenditori facoltosi. La tokenizzazione permettere di rendere digitale e circolante su blockchain una qualsiasi tipologia di asset reale[75] permettendo allo stesso di accedere ad un ampio mercato secondario. Investitori di qualsiasi tipo potranno in questo modo avere accesso, ed investire direttamente in quote di partecipazione di società medio piccole e addirittura start-up. Il tutto fruibile on-chain e con possibilità, di particolare utilità, di liquidare in qualsiasi momento la propria partecipazione rendendo liquido un settore fino ad oggi considerato per sua natura illiquido. L'utilizzo da parte di un VC della tokenizzazione delle partecipazioni delle proprie partecipate permetterebbe di dare uno slancio importante all'innovazione permettendo agli investitori, anche retail, di finanziare un progetto in cui credono. Il ruolo dei Venture Capital in questo settore sarebbe estremamente importante per

[75] In questo documento vengono trattate principalmente i beni di natura finanziaria con particolare riferimento alle azioni o quote di partecipazione di una società o di una start-up.

quanto riguarda la definizione di un valore intrinseco di base delle start-up, in quanto soggetti esperti in questa pratica; il proprio business non cambierebbe radicalmente ma otterrebbe un grande beneficio potendo diventare estremamente scalabile.

Questo meccanismo cela tante opportunità quante insidie soprattutto per chi non è esperto e non conosce questo particolare tipo di tecnologia. Per questo viene più volte sottolineata la necessità di un intervento legislativo e la centralità che i regolatori avranno nell' indirizzare lo sviluppo di questo settore. In merito alla regolamentazione è presente un apposito paragrafo (3.6) riguardo il MiCA ovvero il regolamento europeo sui mercati delle cripto attività, recentemente approvato[76] dal Consiglio Europeo che entrerà in vigore dalla metà del 2024.

Da quanto emerso in questo elaborato, e come dimostrano i due case study analizzati nel quarto capitolo, è evidente che il futuro della finanza dovrà necessariamente fare i conti con la tecnologia blockchain e con la prossima frontiera di internet, il web3.0. La tokenizzazione sarà il ponte tra beni reali e rappresentazioni virtuali che permetterà il raggiungimento di una nuova frontiera per la creazione e generazione di valore.

[76] 16 maggio 2023

BIBLIOGRAFIA E SITOGRAFIA

Zider, B. (1998). "How Venture Capital works." *Harvard Business Review*.

Gornall, W., & Strebulaev, I. A. (2015). The Economic Impact of Venture Capital: Evidence from Public Companies. *Social Science Research Network*. https://doi.org/10.2139/ssrn.2681841

Kaplan, S. A., & Strömberg, P. (2002). Characteristics, Contracts and Actions: Evidence from Venture Capitalist Analyses. *National Bureau of Economic Research*, *Working Paper 8764*. http://www.nber.org/papers/w8764

Janeway, W., Nanda, R., & Rhodes-Kropf, M. (n.d.). Venture Capital Booms and Startup Financing. *Harvard Business School*, *Working Paper 21-116*.

Howell, S. T. (2018). Reducing Information Frictions in Venture Capital: The Role of New Venture Competitions. *National Bureau of Economic Research*, *Working Paper 23874*. http://www.nber.org/papers/w23874

Van Pottelsberghe De La Potterie, B., & Romain, A. (2004). The Economic Impact of Venture Capital. *Deutsche Bundesbank*, *Paper Series 1, No. 2004,18*. https://doi.org/10.2139/ssrn.2785063

Ed-dafali, S., Chakir, A., & Bouzahir, B. (2016). Value-adding and Monitoring Activities of Venture Capital: a Synthesis Literature Review. *Research Journal of Finance and Accounting*, *Vol.7, No.22*, ISSN 2222-1697.

Harris, R. M., Jenkinson, T., & Kaplan, S. A. (2013). Private Equity Performance: What Do We Know? *Social Science Research Network*. https://doi.org/10.2139/ssrn.1932316

Banca d'Italia. (2022). Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività. *Comunicazione Banca D'Italia*. https://www.bancaditalia.it/media/approfondimenti/2022/cripto/Comunicazioni-della-Banca-d-Italia-DLT-cripto.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin Org*. https://bitcoin.org/bitcoin.pdf

ECB - Crypto-Assets Task Force. (2019). Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures. *ECB Occasional Paper Series*, *No 223*.

European Central Bank. (2020). *"Report on a digital euro."* https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

Burlon, L., Montes-Galdón, C., Muñoz, M., & Smets, F. (2022). The Optimal Quantity of CBDC in a Bank-Based Economy. *Social Science Research Network*, *Working Paper Series, No 2689*. https://doi.org/10.2139/ssrn.4175853

Hileman, G., & Rauchs, M. (2017). 2017 Global Blockchain Benchmarking Study. *Cambridge Centre for Alternative Finance*. https://doi.org/10.2139/ssrn.3040224

Carrière, P., De Luca, N., De Mari, M., Gasparri, G., & Poli, T. N. (n.d.). "Tokenizzazione di azioni e azioni tokens". *Quaderni Giuridici Consob*.

Caponera, A., & Gola, C. (2019). Aspetti economici e regolamentari delle «cripto-attività». *Questioni Di Economia E Finanza (Occasional Papers)*, *Numero 484*, ISSN 1972-6643. https://www.bancaditalia.it/pubblicazioni/qef/2019-0484/QEF_484_19.pdf

FINMA. (2018). Guida pratica per il trattamento delle richieste inerenti all'assoggettamento in riferimento alle Initial Coin Offering (ICO)". *Guida Pratica FINMA*.

Kumar, S., Suresh, R., Liu, D., Kronfellner, B., & Kaul, A. (1999). "Relevance of on-chain asset tokenization in 'crypto winter' "*Boston Consulting Group*. BCG & ADDX. https://web-assets.bcg.com/1e/a2/5b5f2b7e42dfad2cb3113a291222/on-chain-asset-tokenization.pdf

OECD (2020), The Tokenization of Assets and Potential Implications for Financial Markets, OECD Blockchain Policy Series, https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm

Citi. (2023). MONEY, TOKENS, AND GAMES Blockchain's Next Billion Users and Trillions in Value. *Citi GPS: Global Perspectives & Solutions*.

European Central Bank & Bank of Japan. (2018). Securities settlement systems: delivery-vs-payment in a distributed ledger environment. *STELLA - a Joint Research Project of the European Central Bank and the Bank of Japan*. ECB & BoJ.

Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why do businesses go crypto? An empirical analysis of initial coin offerings. *Journal of Economics and Business*, *100*, 64-75. https://doi.org/10.1016/j.jeconbus.2018.04.001

Howell, S. T., Niessner, M., & Yermack, D. (2020). Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales. *Review of Financial Studies*, *33*(9), 3925–3974. https://doi.org/10.1093/rfs/hhz131

Sitografia

Enciclopedia Treccani. (n.d.-c). *"Token."* https://www.treccani.it/enciclopedia/token/#:~:text=In%20informatica%2C%20termine%20con%20cui,l%27accesso%20a%20un%20servizio

Borsa Italiana. (n.d.-e). *Venture Capital - Glossario Finanziario - Borsa Italiana*. https://www.borsaitaliana.it/borsa/glossario/venture-capital.html#:~:text=Glossario%20finanziario%20%2D%20Venture%20Capital&text=Attivit%C3%A0%20di%20investimento%20istituzionale%20in,un%20elevato%20potenziale%20di%20sviluppo.

Borsa Italiana. (n.d.-c). *Due Diligence - Glossario Finanziario - Borsa Italiana*. https://www.borsaitaliana.it/borsa/glossario/due-diligence.html#:~:text=Glossario%20finanziario%20%2D%20Due%20Diligence&text=Attivit%C3%A0%20di%20acquisizione%20delle%20informazioni,di%20emissione%20di%20strumenti%20finanziari.

Borsa Italiana. (n.d.-e). *Private Equity - Glossario Finanziario - Borsa Italiana*. https://www.borsaitaliana.it/borsa/glossario/private-equity.html

SHA256 Online. (n.d.). https://emn178.github.io/online-tools/sha256.html

Borsa Italiana. (n.d.-d). *Nonce - Glossario Finanziario - Borsa Italiana*. https://www.borsaitaliana.it/borsa/glossario/nonce.html#:~:text=Il%20nonce%20%C3%A8%20un%20parametro,di%20contratti%20creato%20dall%27account.

Academy, Binance. (2023). Cos'è lo Staking? *Binance Academy*. https://academy.binance.com/it/articles/what-is-staking

Ethereum. (n.d.). *Introduzione alle dapp | ethereum.org*. ethereum.org. https://ethereum.org/it/developers/docs/dapps/

tokenizzazione - Parole nuove - Accademia della Crusca. (n.d.). https://accademiadellacrusca.it/it/parole-nuove/tokenizzazione/23537#:~:text=Definizione,tradizionali%20sotto%20forma%20di%20token.

DeFi TVL history 2018-2023 | Statista. (2023, April 24). Statista. https://www.statista.com/statistics/1272181/defi-tvl-in-multiple-blockchains/

Ethereum. (n.d.-b). *Standard token | ethereum.org*. ethereum.org. https://ethereum.org/it/developers/docs/standards/tokens/

Borsa Italiana. (n.d.-b). *Cos'è la Liquidità economica e finanziaria di uno strumento? - Borsa Italiana*. https://www.borsaitaliana.it/notizie/sotto-la-lente/liquidita.htm

McGeever, J. (2023, February 8). Column: Outsized U.S. share of world equity may revert to norm. *Reuters*. https://www.reuters.com/markets/europe/outsized-us-share-world-equity-may-revert-norm-2023-02-07/#:~:text=According%20to%20Datastream%2C%20global%20market,%24100%20trillion%20in%20late%202021.

European Central Bank. (2023, April 12). *All glossary entries glossary*. https://www.ecb.europa.eu/services/glossary/html/glossc.en.html

Borsa Italiana. (n.d.-c). *Custodian - Glossario Finanziario - Borsa Italiana*. https://www.borsaitaliana.it/borsa/glossario/custodian.html#:~:text=Definizione,correttezza%20e%20di%20trasparenza%20amministrativa.

Econopoly. (2023, April 24). *L'avvento del MiCA mette davvero fine al Crypto Far West in Europa?* Econopoly. https://www.econopoly.ilsole24ore.com/2023/04/24/mica-crypto-regolamento-europa/#_ftn3

Ethereum. (n.d.-a). *Decentralized autonomous organizations (DAOs) | ethereum.org*. ethereum.org. https://ethereum.org/en/dao/

Academy, Binance. (2022). Cosa sono le pool di liquidità nella DeFi e come funzionano? *Binance Academy*. https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi