LUISS

Dipartimento di Economia e Finanza

Corso di Laurea Magistrale in Economia e Finanza

Double Degree – MS in Global Finance at Fordham University

Cattedra di Finanza Aziendale Avanzato

Protocolli decentralizzati per il pricing delle IPO: analisi dell'integrazione Smart Contract su Algorand

RELATORE

Prof. Arturo Capasso

CORRELATORE

Prof. ssa Romina Guglielmetti

CANDIDATO

Alessandro Amelio 773491

Anno Accademico: 2024/2025

A mio Padre,
esempio di vita operosa ed attiva,
fonte inesauribile di energie e di idee.

Lisbona, febbraio 2025

Introduzione

Le offerte pubbliche iniziali nel panorama finanziario attuale, rappresentano un momento cruciale per le imprese che desiderano quotarsi sul mercato e ottenere quindi capitali attraverso una metodologia alternativa rispetto al finanziamento bancario, ovvero attraverso la vendita pubblica di titoli. Tuttavia, il tradizionale processo di *pricing* delle IPO è spesso criticato in quanto poco trasparente, fortemente dipendente dagli intermediari finanziari, organizzati di fatto in forma di oligopolio e dai fenomeni ricorrenti dell'*underpricing*. Questi fattori contribuiscono a penalizzare le società emittenti, favorendo d'altro canto gli investitori selezionati dagli stessi intermediari, che supportano il processo di quotazione. A fronte di queste inefficienze, lo sviluppo della tecnologia *blockchain* e quindi di protocolli decentralizzati sempre più accessibili e sicuri, si pongono come alternativa allo svolgimento tradizionale della quotazione delle imprese sul mercato primario. Gli aspetti più innovativi della disciplina riguardano nello specifico le modalità di allocazione e la determinazione del prezzo per le azioni di nuova emissione.

Questa tesi si propone di esplorare le potenzialità dei suddetti meccanismi decentralizzati per il *pricing* delle IPO. Il lavoro avrà una valenza sia teorica che pratica, dal momento che, da una parte, verranno analizzate nel dettaglio tutte le peculiarità dell'attuale IPO e della proposta innovativa di ICO, attraverso una disamina dei vantaggi e svantaggi corrispondenti, e dall'altra, verrà implementata una simulazione di offerta pubblica tramite asta decentralizzata. Questa verrà condotta mediante uno *smart contract* su Algorand, ossia una *blockchain* pubblica ad alte prestazioni in termini di sicurezza, scalabilità e velocità di esecuzione. La parte centrale del lavoro, infatti, si focalizzerà nella descrizione di un prototipo tecnico funzionante di *smart contract* su Algorand, in grado di raccogliere offerte, calcolare il prezzo marginale e distribuire automaticamente i *token* rappresentativi delle azioni. Lo *smart contract* realizzato, verrà testato tramite una simulazione e analizzato rispetto ai criteri di sicurezza, scalabilità e costi, caratteristiche fondamentali per una quotazione sul mercato primario. Infine le evidenze di *underpricing* ottenute tramite le simulazioni, verranno analizzate attraverso un modello econometrico multivariato al fine di studiare le variabili che impattano maggiormente sul fenomeno. In generale, il lavoro svolto all'interno di questo elaborato si pone come obiettivo quello di creare un *level playing field*, sfruttando quindi le potenzialità della *blockchain* per costituire una soluzione che possa migliorare l'efficienza, la trasparenza e l'equità nei mercati primari. I risultati ottenuti nelle simulazioni e nel *test* multivariato, dimostrano la validità tecnica del modello e suggeriscono che, con le dovute elaborazioni e specifiche, i protocolli decentralizzati potrebbero rappresentare un'evoluzione strutturale nella gestione delle offerte pubbliche nel prossimo futuro.

INDICE

CAPITOLO TERZO

Simulazione di offerta pubblica iniziale tramite Algorand

CAPITOLO QUARTO

Analisi econometriche dei risultati ottenuti tramite simulazione

Capitolo Primo

Funzionamento delle IPO tradizionali e le relative limitazioni del processo

Il presente capitolo, prettamente introduttivo e prodromico all'analisi del fenomeno e alle conclusioni verso cui si è giunti nella costituzione dell'elaborato, intende esporre e descrivere nel modo più esaustivo e particolareggiato possibile gli aspetti teorici e decisivi inerenti al funzionamento del mercato primario azionario, illustrando eventuali limitazioni ed aspetti supportati dalle evidenze empiriche.

1.1 Il quadro generale e le motivazioni alla base delle *Initial Public Offering*

Attraverso il termine *IPO* (*Initial Public Offering*), si intende un processo di finanza mobiliare di per sé molto articolato, attraverso il quale un'impresa definita *emittente*, dà avvio alla propria quotazione e contestualmente alla diffusione dei titoli azionari presso un mercato regolamentato. Questa decisione pertanto non coinvolge solo l'impresa, bensì anche soggetti esterni quali: intermediari finanziari, regolatori e pubblico risparmio nella forma di investitori[1]. La decisione di accedere al mercato primario, è presa in considerazione dall'apparato manageriale per diversi ordini di ragione, in primo luogo la scelta di attuare un'*IPO* può essere giudicata come la naturale evoluzione di un'impresa, con l'obiettivo di aumentare la propria riconoscibilità sul mercato finanziario[2] e dunque attirare quanti più investitori interessati. In effetti, uno tra i tanti scopi può fare riferimento alla ricerca di nuove forme di finanziamento, alternativo al contesto bancario, per espandere il proprio *business* attraverso le acquisizioni e finanziare i propri progetti con un costo del capitale relativamente più conveniente[3]. Oltre alle già menzionate ragioni, questa scelta viene ponderata anche per altri motivi, come: la necessità di stabilire un valore di mercato dell'impresa, migliorare la reputazione aziendale, allargare la base azionaria e contestualmente liquidare più facilmente gli azionisti già presenti all'interno dell'ambito societario. Nondimeno il primo approccio per una società all'interno di un sistema di negoziazione finanziario, richiede degli oneri particolarmente elevati per le imprese, a maggior ragione nei casi in cui le stesse sono di recente costituzione o non presentano un

[1] In tal senso, essendo l'offerta pubblica iniziale rivolta in modo indistinto verso gli investitori è da intendersi come incentivo al pubblico risparmio e come tale necessita di obbligatorie tutele da parte dei regolamentatori, in termini di trasparenza e rischio.
[2] R.A. Brealey, S. Myers, F. Allen, *Principles of Corporate Finance – 9th Edition*, McGraw-Hill, New York.
[3] In questa sede non si tiene in considerazione la presenza del *Tax Shield* che consente la deducibilità degli interessi passivi sul debito finanziario. In accordo con la *Pecking Order Theory* il debito finanziario è la seconda scelta tra le varie fonti di finanziamento aziendale, preceduta solo dall'autofinanziamento da parte dei soci.

apparato manageriale particolarmente interessato a fornire informazioni verso l'esterno, come accade nel caso delle imprese familiari. È dunque evidente come tale processo rappresenti una vera e propria rivoluzione per ogni aspetto aziendale, che dovrà a tal proposito uniformarsi con la regolamentazione sottesa al mercato e finalizzata alla divulgazione di informazioni finanziarie verso il pubblico di investitori. Proprio in riferimento a tale complessità e agli eventuali obblighi che ne derivano, è di significativa importanza che l'emittente sia consapevole e capace di poter apportare delle modifiche sostanziali e formali all'organizzazione, in modo tale da adeguarsi con tutti i requisiti richiesti dal mercato all'interno del quale si voglia procedere per la distribuzione del flottante.

Tra i differenti interventi di modifica si possono distinguere tre diverse aree di attività[4]:

- **Ambito patrimoniale**: riferito al soddisfacimento dei requisiti patrimoniali richiesti per ogni singolo mercato, questi possono variare molto a seconda della categoria di imprese a cui lo stesso mercato fa riferimento.
- **Ambito statuario/governativo**: adeguamento verso le normative definite all'interno del Testo Unico della Finanza, nonché alle direttive e regolamenti europei e per gli Stati Uniti alla regolamentazione fornita dalla SEC. Non di meno bisogna tenere in considerazione i cosiddetti codici di autodisciplina, che forniscono le *best practice* relative alla *corporate governance*, ricalcando gli articoli 25 e 126 del Testo Unico della Finanza[5], la composizione del collegio sindacale e l'eliminazione delle limitazioni alla circolazione degli strumenti finanziari.
- **Ambito manageriale**: presenza di un piano strategico industriale adeguato alla singola realtà, basato sulle metodologie di *forecasting* coerenti con il settore di riferimento. Fondamentale è anche di un sistema informativo e di *reporting* al fine di ampliare la trasparenza e il controllo di gestione, con un'adeguata *disclosure* verso l'esterno.

Come definito in precedenza, le operazioni di IPO, risultano essere molto complesse, all'interno del panorama finanziario si possono distinguere tre differenti categorie di offerte pubbliche iniziali[6], queste ultime differiscono in base all'obiettivo che l'azionariato ed il *management* si è imposto, ed al tempo stesso in base alla tipologia di azioni da collocare in seguito sul mercato:

[4] C. Iosio; "*IPO per le PMI italiane*", IPSOA Gruppo Wolters Kluwer, Volume 32, 2011, capitolo 1 e https://www.borsaitaliana.it/borsa/glossario/requisiti-di-ammissione.html
https://www.sec.gov/resources-small-businesses/going-public

[5] Consob, Decreto Legislativo 24 febbraio 1998, n.58; "*Testo unico delle disposizioni in materia di intermediazione finanziaria*", aggiornato con le modifiche apportate dal decreto legislativo n. 125 del 6/9/2024.

[6] J. Berk e P. DeMarzo; "*Corporate Finance – 4th Edition*", Pearson, Boston, 2016.

- Offerta pubblica di sottoscrizione (*OPS*): questa particolare offerta iniziale, si caratterizza per il fatto che i titoli oggetto della stessa sono emessi dalla emittente in modo totalmente *ex novo*. Lo scopo fondamentale di questa offerta è appunto l'allargamento dell'azionariato che caratterizza la proprietà della società attraverso la sottoscrizione da parte dei nuovi investitori. In questo caso infatti, le "neo-emesse" azioni contribuiscono ad accrescere il patrimonio societario, di modo che i proventi derivanti dal processo di *IPO* confluiscano direttamente nel capitale aziendale. Ovviamente così come nella altre tipologie di offerte iniziali anche nel caso dell'*OPS*, i titoli possono essere oggetto di offerte pubbliche, istituzionali oppure collocamenti privati. Nella prima fattispecie è importante ricordare che al fine di tutelare i risparmiatori *retail*, la società dovrà impegnarsi a rispettare degli obblighi informativi nei confronti dalla CONSOB, consegnando un prospetto dell'operazione, in conformità al TUF, questo poiché l'operazione viene categorizzata come sollecitazione all'investimento verso il pubblico[7].
- Offerta pubblica di vendita (*OPV*): nella fattispecie delle offerte pubbliche di vendita si riscontrano le medesime modalità di esecuzione rispetto alla *OPS*, tuttavia in questo caso la differenza più rilevante è dovuta alla presenza di azioni già emesse in precedenza dalla società emittente. Ovvero in questa tipologia di offerta pubblica, la parte di flottante messo in vendita sul mercato non fanno capo alla società bensì ai soci precedenti, con il risultato che i proventi generati, contrariamente alla *OPS* non verranno destinati al capitale aziendale bensì al ritorno personale dei precedenti soci. Questa modalità è dunque molto importante poiché consente la liquidazione dei soci precedenti e quindi l'ingresso dei nuovi investitori, inoltre questa è la modalità seguita nella operazioni di privatizzazione[8].
- Offerta pubblica di sottoscrizione e vendita (*OPSV*): in generale questa tipologia di operazione rappresenta un *mix* tra le precedenti due[9], in altre parole in occasione di questa operazione una parte del flottante viene emesso direttamente dalla società emittente, ossia risulta essere di nuova costituzione, mentre la parte rimanente deriva dalla vendita di azioni già in precedenza emesse ed acquistate dai in passato dai primi soci. Per quanto concerne le modalità di svolgimento dell'offerta, quest'ultime sono

[7] https://www.borsaitaliana.it/borsa/glossario/offerta-pubblica-di-sottoscrizione.html
[8] https://www.borsaitaliana.it/borsa/glossario/offerta-pubblica-di-vendita.html
[9] L.M. Benveniste e W.J. Wilhelm Jr.; "*Initial Public Offerings: Going by the Book*", in Journal of Applied Corporate Finance, n. 10, pp. 98-108, 1997.

analoghe alle precedenti, rispettando anche la normativa di base che caratterizza le emissioni societarie. In generale la maggior parte delle *IPO* risulta essere appunto un'operazione definita come *OPSV*[10].

Questa breve analisi può dimostrare la complessità del processo, il quale risulta rivoluzionario per il management e per le varie funzioni aziendali, tanto da essere particolarmente oneroso in termini di tempo, risorse ed informazioni che l'impresa deve necessariamente divulgare verso il pubblico. Dunque quali sono le motivazioni che fra tutte spingono le imprese verso un mercato aperto ad altri investitori?

A tal proposito, nel corso degli anni sono state condotte svariate analisi empiriche riguardo la *ratio* che sottende il comportamento delle figure manageriali e quindi delle ragioni che spingono le imprese a quotarsi. Tra tutti questi studi, molti hanno sottolineato come il mercato delle *IPO* sia ciclico[11], seguendo pedissequamente le fasi di espansione e di contrazione del ciclo economico[12]. Questo aspetto è di per sé molto rilevante, in quanto dimostra come il processo di quotazione viene influenzato non solo da fattori endogeni ma anche da fattori esogeni al contesto aziendale, che possono dipendere dal *market timing*, da congiunture economico-politiche oppure dall'andamento generale del mercato azionario.

Al fine di identificare le motivazioni che spingono una società a valutare la predisposizione di un'*IPO*, in primo luogo si ha intenzione di descrivere le *ragioni di tipo competitivo-commerciali*, tra queste vi sono: 1) raccolta di capitali a sostegno dello sviluppo; 2) visibilità e *brand awareness*; 3) moneta di scambio; 4) pressioni competitive; 5) attrarre e mantenere risorse qualificate. La teoria prevalente[13], evidenzia l'importanza di acquisire finanziamenti per sostenere gli investimenti delle imprese private, presentando quindi il processo di *IPO* come una fase essenziale nell'evoluzione di qualsiasi realtà economica. Il reperimento di risorse finanziarie è quindi giudicato come una delle ragioni fondamentali per pianificare un'*Initial Public Offering*, risorse che possono essere destinate al miglioramento dell'operatività e al finanziamento di attività innovative o di strategie volte ad espandere le quote di mercato. La raccolta di capitali e quindi la possibilità di poter ottenere una maggiore flessibilità nel reperimento delle risorse economiche, è di vitale importanza, specialmente nel caso in cui il

[10] J. Berk e P. DeMarzo, op. cit.
[11] J.R. Ritter, *Monthly number of IPOs and the average first-day return*, dec. 2020.
[12] M. Lowry, G. William Schwert; "*IPO Market Cycles: Bubbles or Sequential Learning?"* The Journal of Finance Vol. 57, No. 3 pp. 1171-1200 Jun. 2002.
[13] B. A. Jain, O. Kini; "*The Post Issue Operating Performance of IPO Firms*", Journal of Finance No. 49, 1699-1726, 1994.
W. H. Mikkelson, M. Partch, K. Shah; "*Ownership and operating performance of companies that go public*" Journal of Financial Economics Volume 44, 281-307, June 1997.

settore di riferimento sia particolarmente competitivo. L'impresa in questione potrà infatti fare riferimento sia al capitale di rischio, tramite l'emissione di titoli azionari sul mercato primario, presso la platea di investitori operanti al suo interno e sia al capitale di debito mediante il supporto di finanziamenti bancari ed istituti di credito, senza dimenticare il supporto del *private equity*, il quale a partire dal 2022 in Italia ha registrato una raccolta sempre più rilevante[14], ponendosi come una valida alternativa alla due precedenti, nel reperimento di risorse finanziarie.

Un altro tema è la visibilità, attraverso il processo di quotazione un'impresa può intercettare varie tipologie di investitori ed al tempo stesso suscitare l'interesse di un pubblico non solo interessato al finanziamento verso tale realtà, ma anche verso una platea più ampia, di modo che possa essere più riconoscibile e creare maggiore consapevolezza anche rispetto ai potenziali clienti.

Il processo di quotazione può inoltre generare una valorizzazione del capitale sociale, il quale non solo risulta essere maggiormente liquidabile, ma al tempo stesso si stabilisce un valore certo e riconosciuto sul mercato. Questo certamente si può definire un vantaggio nonché una motivazione al fine di avviare un processo di quotazione, d'altra parte il capitale sociale, ovvero le azioni, potranno essere sfruttate come moneta di scambio per eventuali operazioni straordinarie di *M&A*. Anche le società di piccole e medie dimensioni neo quotate, seppure in modo più difficoltoso, possono procedere alla pianificazione di operazioni finanziarie straordinarie, diventando dunque imprese *target* per future acquisizioni o alternativamente parte acquirente. In entrambe le alternative, la presenza di un' *acquisition currency* può aiutare l'impresa nella definizione dei propri obiettivi e nella conclusione dei vari *deals*.

Un'altra rilevante motivazione si può desumere della varie pressioni competitive alle quali un'impresa può essere esposta durante il corso della sua vita oppure in particolari fasi di espansione del mercato[15]. Pertanto la scelta di avviare un processo di quotazione, come menzionato in precedenza non deriva solamente da condizioni interne al contesto aziendale, ossia i fattori endogeni, tra cui: massimizzazione delle performance, supporto allo sviluppo aziendale, necessità di liquidazione dell'azionariato e cambio generazionale nella proprietà del capitale dell'emittente, bensì si può anche originare da fattori esterni non direttamente legati all'ambito operativo e gestionale dell'impresa. Le analisi di mercato, ed in particolare quelle relative alla struttura del capitale dei *competitors* sono fondamentali al fine di poter ottenere un

[14] M. D'Ascenzo, "*Private capital, 2022 miglior anno di sempre con 23,6 miliardi investiti"*, Il Sole24Ore.
[15] J. C. Brau, "*Why do firms go public?*", Marriott School Brigham Young University, 2010.

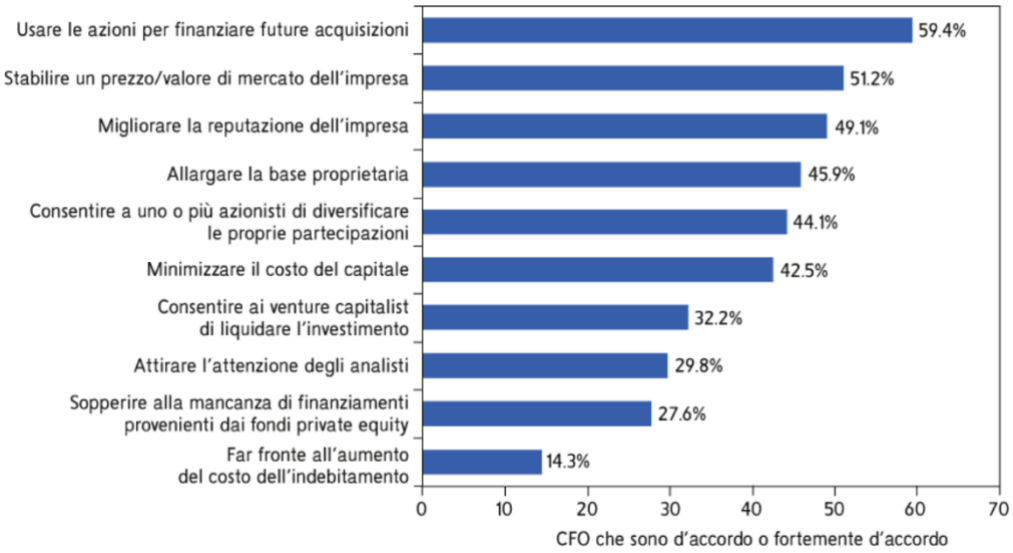
miglioramento ed efficientamento delle risorse aziendali, questo pertanto fa sì che le imprese a lungo termine possono soffrire la presenza di altre società quotante operanti nel medesimo settore. Questa posizione subordinata è dovuta molto spesso alla mancata diversificazione dei finanziamenti, i concorrenti in tal senso possono beneficiare di più alternative finanziarie, rendendo quindi il costo del capitale molto più economico ed in definitiva ottenendo un vantaggio competitivo molto rilevante, oltre all'avere un migliore o più rapido accesso a fonti di finanziamento generalmente più elevato rispetto ad una società non quotata.

Oltre alle pressioni competitive, un ulteriore fattore rilevante è la necessità di attrarre e mantenere risorse qualificate, è inutile affermare quanto quest'ultime possono essere fondamentali per il *business* aziendale, tuttavia similmente alla maggiore visibilità verso il pubblico, le risorse umane possono essere maggiormente attratte da una società quotata rispetto ad una realtà con flottante non presente sui mercati. Ciò si può ravvisare nei programmi di compensazione delle risorse più qualificate che prevedono una maggiore allineamento degli obiettivi tra *principal* ed *agent*, mediante incentivazioni tramite *stock option*, oggi non particolarmente condivise dagli azionisti oppure meccanismi di attribuzione di azioni, tendenzialmente collegati alle *performances* aziendali.

Ulteriori tipologie di motivazioni poi si possono ravvisare nelle ragioni collegate alla struttura organizzativo-societaria, piuttosto che alla valorizzazione delle partecipazioni degli azionisti preesistenti ed infine al rafforzamento della struttura patrimoniale dell'emittente. Il presente elaborato non ha la presunzione di fornire una formulazione dettagliata della totalità delle motivazioni che possono spingere una società a dare avvio ad un processo di *Initial Public Offering*, questo per due ragioni, in primo luogo l'obiettivo del lavoro non è quello di analizzare la totalità dei contesti empirici ed in seguito la seconda ragione è dovuto al fatto che ogni impresa presenta peculiarità organizzativo-manageriali differenti che possono definire situazioni del tutto differenti dai contesti empirici analizzati dalla dottrina economica. Tuttavia per quanto concerne i fini del presente elaborato le motivazioni in precedenza citate possono fornire un quadro generale delle situazioni che spingono il *management* ad affermare tale processo, evidenze osservate anche in ulteriori analisi condotte su un campione di 336 *CFO*[16] i quali hanno chiarito quali sono le principali ragioni, che spingono a quotarsi.

I risultati di questa analisi condotta possono essere sintetizzati attraverso la seguente tabella:

[16] J.C. Brau, S.E. Fawcett, "*Evidence on What CFOs Think about the IPO Process: Practice, Theory and Managerial Implications*", Journal of Applied Corporate Finance, n. 18, pp. 107–117, 2006.



Fonte: J. Berk e P. DeMarzo; "*Corporate Finance – 4th Edition*", Pearson, Boston, 2016.

1.2 Analisi del processo *go to public:* Requisiti, *Roadshow* e *Book building*

Il processo di *IPO* si articola in una serie di complesse fasi che possono richiedere molto tempo prima di procedere con l'effettiva quotazione, il tempo stimato in effetti si aggira in un *range* che va dai sei mesi fino ad un anno[17]. Ciò ovviamente può dipendere da differenti fattori, come ad esempio la dimensione dell'offerta primaria, della società emittente ed inoltre anche in base a quale tipologia di mercato la stessa impresa decide di quotarsi, questo perché ogni segmento presenta dei requisiti differenti in base alla finalità dello stesso. In Italia ad esempio, *Euronext* presenta differenti tipologie di mercato ognuno con elementi differenti che quotano imprese con diverse caratteristiche e finalità, tra questi si distinguono[18]:

- *Euronext Growth Milan*: un mercato dedicato alle *PMI* dinamiche e competitive che punta alla loro quotazione tramite un percorso equilibrato e graduale, che tiene conto delle strutture finanziarie delle imprese e le supporta tramite la figura in un *Advisor*.
- *Euronext Milan*: conosciuto anche in passato come *MTA* (Mercato Telematico Azionario), è il segmento più importante nel mercato italiano, che accoglie le imprese italiane a grande capitalizzazione , offrendo loro la visibilità verso gli investitori internazionali.

[17] M. B. Lowry, R. Michaely, E. Volkova, "*Initial Public Offerings: A Synthesis of the Literature and Directions for Future Research*", Forthcoming Foundations and Trends in Finance, 2017.
[18] https://www.borsaitaliana.it/azioni/mercati/mercati-landingpage/mercati.htm.

- *Euronext STAR Milan*: questo è il segmento che al suo interno presenta prestigiose *PMI*, che aderiscono a stringenti requisiti imposti dal regolatore, su temi come: trasparenza, governance e liquidità, in sintesi un campione di società dalle quali gli investitori si aspettano una forte crescita.
- *Euronext MIV Milan*: è un mercato di riferimento per i veicoli ed i fondi d' investimento nazionali o esteri che operano nell'economia reale.

Nel presente elaborato da qui in avanti si farà riferimento specialmente hai primi due mercati, poiché presentano un campione di imprese più numeroso e inoltre la procedura risulta essere maggiormente standardizzata. Come riferito in precedenza, tutte le imprese necessitano di requisiti al fine di potersi quotare, tali requisiti sono fondamentali ed imposti dal regolatore al fine di assicurare maggiore trasparenza in relazione ad una più ampia tutela del risparmio pubblico e quindi degli investitori che sottoscrivono i titoli di nuova emissione.

Procedendo con ordine alla descrizione dei suddetti requisiti, ci si vuole soffermare in primo lugo sul mercato *Euronext Milan*, lo stesso come specificato è il mercato che accoglie le grandi imprese, pertanto i requisiti risultano essere particolarmente elevati in termine di capitalizzazione, infatti il minimo stabilito si attesta a 40 milioni di euro, inoltre i principi contabili dovranno seguire le disposizioni internazionali in base agli IFRS, si necessita inoltre di almeno tre bilanci certificati e di una quota di flottante almeno al 25%. Inoltre il numero di componenti indipendenti del CdA deve attenersi alle norme stabilite nel TUF, così come la predisposizione di un prospetto informativo necessario per potersi quotare. Oltre a questi, si hanno poi altri requisiti informativi sia dal punto di vista semestrale che trimestrale in merito ai *report* contabili della società. Nel caso invece dell'*Euronext Growth Milan* il flottante si attesta al 10%, oppure il 7,5% dovrà essere detenuto da almeno cinque investitori istituzionali, una differenza rispetto al precedente mercato si ritrova nel numero di bilanci consolidati, che si attesta ad uno anziché tre, ed inoltre il CdA presenta solo un singolo amministratore indipendente. Vi è inoltre la permanenza degli obblighi informativi infra annuali, tuttavia non si hanno disposizioni in materia di minima capitalizzazione oppure di obblighi nella definizione della contabilità, che potrà seguire in questo caso i principi nazionali oppure internazionali[19].

Appare evidente come le due tipologie di mercato siano essenzialmente differenti e la logica è dovuta in special modo a quelli che sono gli investitori finali ai quali tali mercati si rivolgono, se infatti è vero che nel primo caso i requisiti sono particolarmente stringenti, questa ragione è dovuto al fatto che il legislatore ha pesato di proteggere maggiormente la componente *retail*

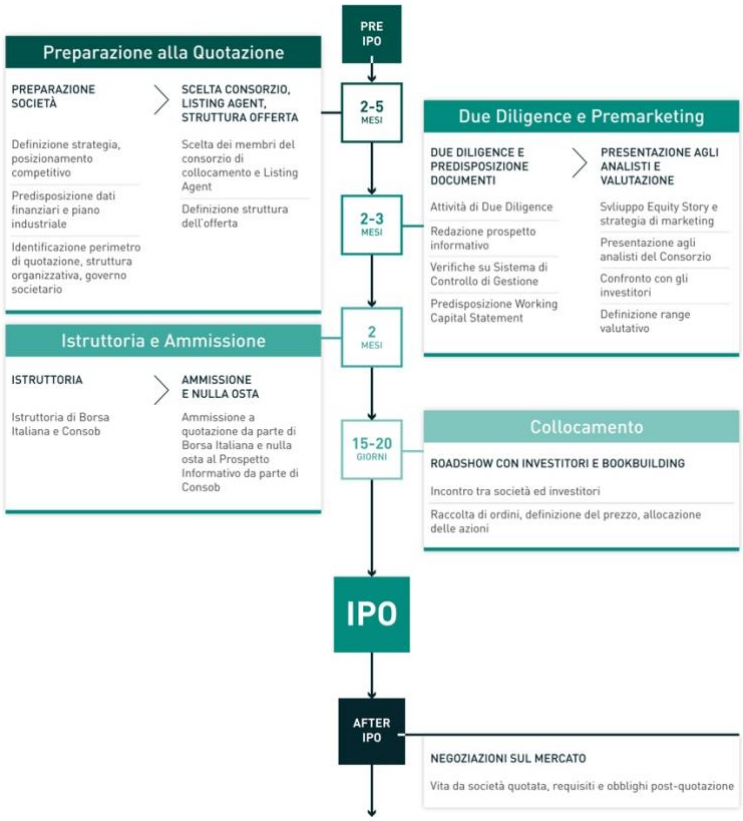
[19] https://www.borsaitaliana.it/azioni/mercati/euronext-growth-milan/requisiti/come-accedere.htm

che si approccia all'investimento verso appunto società molto grandi e bene conosciute presso il pubblico. Nel caso dell'*Euronext Growth Milan*, composto principalmente da PMI, gli investitori maggiormente attratti da questo segmento, e che presentano le competenze per poter valutare la fattibilità dell'investimento, sono essenzialmente investitori istituzionali, i quali hanno tutte le conoscenze in materia di rischio e dunque necessitano di una minore tutela da parte delle istituzioni.

Un'altra differenza molto più elevata si riscontra tra i requisiti richiesti nel segmento *STAR*, in questo mercato infatti, le caratteristiche sono molto più stringenti rispetto ai due segmenti in precedenza citati, questo poiché le imprese in questione sono definite come altamente profittevoli ed inoltre ci si aspetta una forte crescita dalle stesse durante il corso degli anni successivi. Le differenze quindi si possono osservare i primo luogo per la percentuale di flottante che raggiunge almeno il 35%, inoltre la capitalizzazione è fissata in un range che va da 40 milioni fino ad 1 miliardo di euro, gli ulteriori requisiti sono molto simili al segmento *Euronext Milan*.

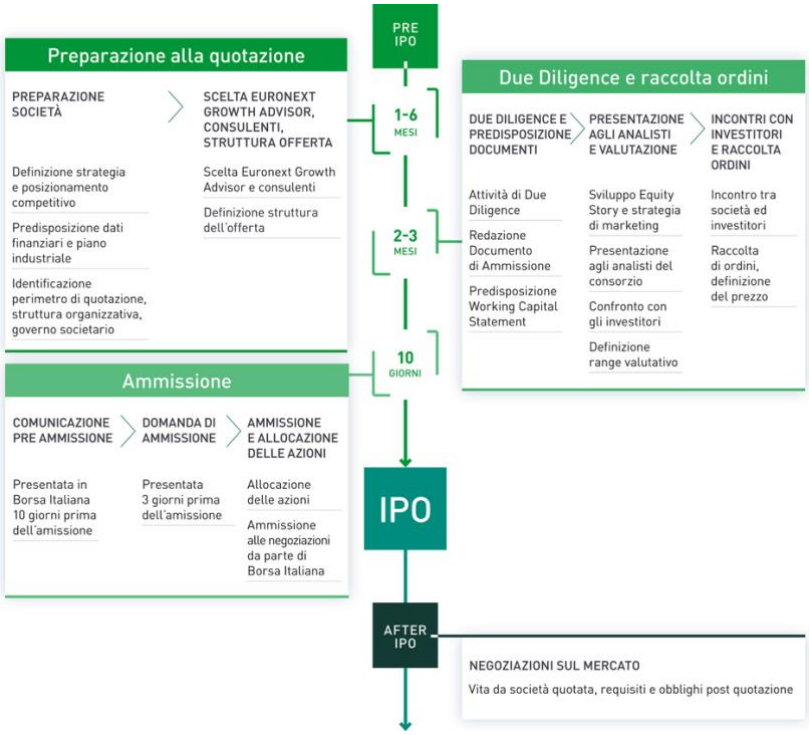
Nei grafici seguenti sono illustrate le fasi con le relative tempistiche che caratterizzano il processo di quotazione sui due mercati precedentemente descritti.

Schema del processo di quotazione sul mercato Euronext Milan:



Fonte: www.borsaitaliana.it

Schema del processo di quotazione sul mercato Euronext Growth Milan:



Fonte: www.borsaitaliana.it

Da questi grafici si possono notare differenti fasi che possono essere più o meno lunghe, molte delle quali relative a processi di tipo burocratico o di *due diligence*, necessari per far luce su eventuali problematiche che possono compromettere l'esito del processo di emissione in una fase già di avvio. Tuttavia al fine di rispettare lo scopo fondamentale della presente analisi, l'elaborato si concentrerà maggiormente sulle fasi di *roadshow* e *bookbuilding*, ed in generale sul ruolo attivo che gli intermediari finanziari svolgono al fine di condurre e supportare la gestione dell'*Initial Public Offering.*

Procediamo con ordine descrivendo ora il ruolo degli intermediari finanziari coinvolti all'interno del processo di quotazione. In generale le mansioni che gli intermediari o le banche d'investimento devono svolgere, si possono sintetizzare in tre macro categorie[20]: consulenza legale e finanziaria, sottoscrizione e vendita al pubblico. Solitamente il processo di quotazione viene affrontato per la prima volta dalle imprese, soprattutto nel caso in cui esse presentano una dimensione ridotta. Nel momento in cui il *management* ha selezionato i sottoscrittori (*underwriters*), gli stessi dovranno confrontarsi in modo molto diretto con l'impresa, in maniera tale da poterla guidare senza ulteriori problemi verso l'obiettivo stabilito, nel caso dell'*IPO* appunto la vendita dei titoli agli investitori. È chiaro quindi, che il ruolo delle banche

[20] R.A. Brealey, S. Myers, F. Allen, op. cit.

d'investimento non si limita soltanto ad apportare capitali e dunque sottoscrivere l'intera emissione, ma soprattutto il loro ruolo, almeno nella parte iniziale, si concretizza nel consigliare e definire un programma strutturato al fine di evitare le problematiche più comuni che possono incorrere. La consulenza legale e finanziaria è finalizzata a definire lo scopo della società emittente, ossia come questo processo di *IPO* debba impattare sulla struttura del capitale aziendale, possibilmente andandola a rafforzare, ed inoltre quali sono le conseguenze dello stesso sulla base azionaria dell'impresa. Tutte queste informazioni vengono sintetizzate in un documento chiamato *registration statement* o prospetto informativo, da consegnare alle autorità garanti per la concorrenza del mercato, in modo tale da poter giudicare la validità e l'adeguatezza dell'offerta dei titoli al pubblico.

Nella scelta dei sottoscrittori le società emittenti devono tenere conto del ruolo che le banche d'investimento hanno sia in fase *ex ante* che *ex post* dell'emissione. Non è raro infatti che i sottoscrittori in seguito alla vendita, si impegnano a sostenere il prezzo dei titoli attraverso la produzione dei *report*, in seguito al *quiet period* di quaranta giorni, oppure svolgendo il ruolo di *market maker*, tutte iniziative affermate in modo da evitare il fenomeno di *underpricing*[21].

Nel caso delle società particolarmente grandi gli intermediari investiti nel ruolo di sottoscrittori, sono affiancati da altri attori finanziari, generalmente altre banche, che riunendosi prendono il nome di consorzio di sottoscrizione, dove tuttavia la banca capofila presenta un ruolo preminente, poiché solitamente quest'ultima negozia tra il 40% e il 60% del volume scambiato sull'azione nei primi 60 giorni dopo la quotazione[22].

In seguito alla consulenza legale e finanziaria, si procede quindi con la fase di sottoscrizione dei titoli. I sottoscrittori, ovvero il consorzio di banche che supporta l'emittente nella quotazione, ha come obiettivo quello di sollevare la stessa dalla collocazione dei titoli sul mercato. In questa fase, i sottoscrittori assumono il rischio legato alla vendita delle azioni presso gli investitori, in altre parole la capofila si accorda con la società al fine di acquisire l'intera emissione, per poi al procedere al collocamento dei titoli sul mercato ad un prezzo maggiore. Questo differenziale tra prezzo di vendita e di acquisto è chiamato *spread*, che rappresenta il guadagno che i sottoscrittori ricevono per assumersi il rischio di quotare una società. Ovviamente questa appena descritta è la fattispecie più semplice e generale, ci sono infatti moltissime clausole che possono essere apportate negli accordi, e questo accade

[21] L. Krigman, W.H. Shaw e K.L. Womack, "*Why Do Firms Switch Underwriters?*", in Journal of Financial Economics, n. 60, pp. 245-284, 2001.

[22] K. Ellis, R. Michaely e M. O'Hara, "*When the Underwriter is the Market Maker: An Examination of Trading in the IPO Aftermarket*", in Journal of Finance, n. 55, pp. 1039-1074, 2000.

soprattutto nel momento in cui l'emissione risulta essere particolarmente rischiosa o altresì particolarmente apprezzata dal mercato. I sottoscrittori come specificato in precedenza si accollano il rischio che l'emissione non abbia successo, ritrovandosi quindi in una situazione in cui il proprio bilancio contiene dei titoli sopravvalutati, non attrattivi per gli investitori. Tra le clausole più comuni vi è ad esempio la *all or none*, che viene scelta soprattutto per le emissioni ad alto rischio. Con questa clausola i sottoscrittori hanno il diritto di rinunciare e quindi annullare la sottoscrizione dell'offerta pubblica iniziale nel momento in cui non dovessero riuscire a collocare la totalità dei titoli, le conseguenze negative pertanto ricadono sulla società che da questa operazione non riuscirà ad ottenere nulla. Un'altra clausola comune è la *best effort*, ovvero il migliore risultato, in questo modo i sottoscrittori si impegnano a collocare il maggiore numero possibile di azioni sul mercato senza tuttavia assicurare la totalità del collocamento. Esistono altre clausole che hanno lo scopo di stabilizzare il prezzo dei titoli al fine di evitare il fenomeno dell'*underpricing*; questo è il caso della *green shoe*, ovvero una clausola che prevede un'opzione di acquisto nel caso in cui la domanda di titoli risulti particolarmente elevata. Questa opzione ha una durata generalmente di trenta giorni ed è associata al meccanismo dell'*over allotment*, ovvero di vendita allo scoperto, che il *global coordinator* può prevedere per stabilizzare il prezzo dell'offerta pubblica nei giorni successivi all'effettiva quotazione. Generalmente la portata del numero di azioni di nuova emissione prevista dalla *green shoe* è pari a quella della vendita allo scoperto (*over allotment*), e si aggira solitamente tra il 10 ed il 15% del totale. Questa strategia ha l'obiettivo di evitare le perdite ed impedire la speculazione sui titoli neo-emessi, si possono presentare infatti due scenari; il primo relativo al caso in cui la domanda supera l'offerta dei titoli, una situazione in cui il prezzo può crescere a dismisura nel giro di pochi giorni ed il secondo viceversa in cui le quotazioni del titolo scendono sotto la soglia di emissione. Nel primo caso quindi il consorzio di collocamento può vendere allo scoperto i titoli tramite l'*over allotment*, realizzando un guadagno e modificando di conseguenza il flottante della società attraverso l'incremento di azioni. Nel caso il prezzo risultasse maggiore rispetto a quello del collocamento, i sottoscrittori possono esercitare la *greenshoe*, al fine di restituire le azioni ai soci prestatori. La remunerazione è comunque assicurata, poiché i sottoscrittori vengono pagati in misura maggiore in base ai titoli che gli stessi collocano sul mercato. Nel secondo scenario, ossia nel caso in cui l'offerta è maggiore della domanda, il prezzo tenderà a scendere; dunque, il consorzio otterrà comunque un guadagno derivato dalla vendita allo scoperto, ma al tempo stesso stabilizzerà il prezzo relativo ai titoli andando a riacquistare le azioni sul mercato per restituirle ai soci e sostenendo quindi la domanda dei titoli.

All'interno degli accordi contrattuali tra società e *global coordianator*, ci possono essere ulteriori clausole più o meno *standardizzate* che possono prendere in considerazione differenti obiettivi rispetto a quelle già citate. Tra queste le più importanti sono la *clawback provision*, *lock-in period*, e *lockbox mechanism.* La prima è una clausola molto importante nel caso in cui le IPO prevedono una categorizzazione degli investitori, questa consiste nella redistribuzione dei titoli azionari in base alla domanda effettiva. Ad esempio, se la domanda degli investitori istituzionali risulta particolarmente elevata, mentre quella degli investitori *retails* e dei *HNWI* è bassa, una parte delle azioni destinate alle precedenti categorie può essere spostata verso gli istituzionali. Riguardo al *lock-in period*, si tratta di un periodo stabilito negli accordi di vendita in cui gli investitori istituzionali oppure le figure manageriali si impegnano a non procedere immediatamente con la dismissione delle azioni, questa clausola è necessaria per stabilizzare i prezzi. A causa dell'ingente quantitativo di titoli acquistato dagli investitori istituzionali la stessa si rende necessaria poiché una vendita improvvisa può causare un tracollo del prezzo. *Lockbox mechanism*, è un accordo presente soltanto in alcuni mercati al fine di verificare la trasparenza dell'emittente, i proventi vengono infatti bloccati su un conto vincolato fino al completamento di tutte le verifiche regolatorie necessarie per l'accesso ad un determinato mercato finanziario.

Si procede ora con la descrizione del processo di vendita dei titoli azionari, in modo particolare per le fasi di *roadshow* e di *bookbuilding*. Nel momento in cui la società ha redatto il prospetto informativo con il supporto della banca capofila, il documento necessita dell'approvazione delle autorità, in questo arco temporale quindi, l'emittente ed il sindacato di sottoscrizione si impegnano effettuare le dovute analisi per definire al meglio il prezzo dei titoli oggetto dell'*IPO*. La metodologia di analisi del prezzo e quindi del valore dell'impresa si basa sui modelli di valutazione mediante i flussi di cassa, come accade con il modello DCF, oppure basato sul modello DDM. Una volta giunti alla formulazione del prezzo, si procede con gli incontri in cui l'emittente ed i sottoscrittori presentano la quotazione sul mercato, questo processo prende il nome di roadshow, e viene realizzato principalmente presso i mercati dove la società intende quotarsi. In questa fase gli incontri sono indirizzati principalmente verso gli investitori istituzionali, i quali esprimono un giudizio sul prezzo e sulla validità dell'offerta, solitamente i sottoscrittori realizzano anche un book degli ordini, ovvero nel caso in cui gli investitori istituzionali siano realmente interessati all'offerta questi potranno esprimersi sulla quantità di azioni oppure sul prezzo che saranno disposti a pagare. Tutte queste indiscrezioni risultano fondamentali poiché ci si può confrontare fin da subito con la reazione del mercato, pertanto i sottoscrittori e gli emittenti potranno adeguare il prezzo e la quantità offerta in base

a tali giudizi. Il processo in questione prende il nome di bookbuilding, ed è fondamentale per capire l'esito di un'offerta pubblica iniziale, inoltre gli investitori non possono adottare comportamenti scorretti nei confronti dei sottoscrittori poiché sono consapevoli che in futuro potranno non beneficiare di questi privilegi, ossia nel poter avere un'anteprima di un'IPO. Per questa ragione il track record del sottoscrittore è di fondamentale importanza, maggiore potere contrattuale possiede e più le analisi saranno corrette in tal senso. In seguito alle suddette fasi si può avere un quadro generale più chiaro, capita infatti che molti investitori che si possono esprimere in modo favorevole acconsentendo ad acquistare un quantitativo fisso di azioni a prescindere dal prezzo di riferimento, ciò quindi può permettere all'impresa di innalzare il prezzo di vendita. Questa è anche una fase di estrema cautela, in effetti nel caso in cui si voglia innalzare il prezzo questo potrebbe essere un problema per altri investitori non coinvolti nelle fasi iniziali di presentazione tramite roadshow, e dunque potrebbero giudicare l'offerta sopravvalutata, finendo così per non acquistare. In sostanza tutte queste fasi devono essere analizzate in modo scrupoloso, andando a capire il *sentiment* del mercato ma più importante è condurre delle valutazioni accurate per stabilire il reale valore dell'impresa in base a ciò che la stessa potrà fornire in futuro agli investitori.

1.3 Aspetti problematici e svantaggi per le società emittenti

Tra i differenti temi, che si pongono in evidenza nel momento in cui una società decide di intraprendere il processo di quotazione, ve ne sono alcuni di fondamentale importanza relativi ai costi ed agli svantaggi derivanti da una maggiore *disclosure* verso il mercato ed in generale verso gli *stakeholders*. Molto spesso, infatti, alcune aziende scelgono di rimanere private perché gli obblighi informativi richiesti dai mercati pubblici possono essere onerosi per il *management*. Questo è particolarmente vero quando si tratta di delineare strategie o piani industriali complessi; in tali circostanze, è essenziale non solo informare gli investitori, ma anche assicurarsi che essi abbiano una percezione positiva delle iniziative proposte. La necessità di divulgare informazioni dettagliate, può quindi rappresentare un ostacolo significativo, trattenendo le aziende dal quotarsi sui mercati pubblici. Negli ultimi anni in effetti la quantità di società quotate è drasticamente diminuita, circa il 50% rispetto ai massimi registrati nel 1996[23] e con esse anche il numero di offerte pubbliche iniziali. Questa tendenza si è registrata in tutti i Paesi occidentali, ma in particolare negli Stati Uniti, dove secondo la

[23] R.A. Brealey, S. Myers, F. Allen, op. cit.

maggioranza dei *top managers* questa situazione si è creata a fronte di un aumento degli oneri burocratici in seguito all'implementazione del *Sarbanes-Oxley Act* (*SOX*). Questo provvedimento legislativo, ha fatto si che molte imprese, soprattutto quelle di piccola dimensione rimanessero fuori dal contesto del mercato finanziario. A tal proposito il *SOX* è stato previsto proprio per aumentare i requisiti di trasparenza e gli sforzi informativi di una realtà economica verso gli investitori, proprio per evitare ulteriori scandali finanziari come quelli accaduti nei primi anni del duemila[24]. Questo provvedimento ha colpito in primo luogo le piccole imprese come le *startup*, che non hanno ritenuto proficuo procedere con il *going to public*, in tal senso molti unicorni come SpaceX, OpenIA oppure Stripe presentano una struttura del capitale interamente privata.

Questa ipotesi legislativo-burocratica appena evidenziata è solo una delle possibili spiegazioni alla decrescita delle *IPO*, parte della letteratura infatti, sottolinea come il problema della diminuzione di offerte pubbliche iniziali sia dovuto soprattutto alle strategie di finanziamento delle *PMI*. Le piccole e medie imprese, presentano infatti una maggiore flessibilità rispetto alle grandi realtà, un vantaggio di certo non trascurabile per lo sviluppo ed il dinamismo industriale. Dunque, la necessità di mantenere questo *status* e quindi evitare ulteriori costi di finanziamento, porta le *PMI* ad affidarsi a strumenti alternativi rispetto ai mercati tradizioni, come ad esempio il *crowdfunding*, il prestito *peer-to-peer*, il *private equity* e *venture capital*[25]. Gao, Ritter e Zhu hanno analizzato questo fenomeno notando che, nel contesto di un mercato in rapido cambiamento, diventa sempre più difficile per queste imprese rimanere competitive, sostenendo che per queste realtà, può essere più facile essere acquisite da entità più grandi piuttosto che affrontare i costi e le complessità di avviare un processo di quotazione.

A tal proposito, una delle sfide più importanti in una quotazione pubblica sono le elevate spese dirette e indirette, come i costi legali, di conformità e amministrativi. Queste spese non sono particolarmente problematiche solo per le piccole realtà, ma anche per le imprese già mature e avviate, molti studi[26] evidenziano infatti come nelle *IPO* solo le commissioni per il consorzio dei sottoscrittori si aggirano in un *range* che va dal 7% al 10% della totalità dell'emissione.

A fronte della sistematicità di questi costi, molti studi hanno pubblicamente dubitato circa la concorrenzialità del mercato dei sottoscrittori, ritenendo infatti che le autorità dovrebbero

[24] In questo senso il Congresso statunitense ha voluto fornire una maggiore protezione per gli investitori, i quali in seguito allo scoppio della bolla Dot-com ed al fallimento di importanti realtà come Enron avevano perso fiducia verso il mercato e verso le istituzioni incaricate al controllo dello stesso.

[25] X. Gao, J.R. Ritter e Z. Zhu, "*Where have all the IPOs gone?*" in Journal of Financial and Quantitative Analysis, n. 48, pp. 1663–1692, 2013.

[26] R.S. Barden, J.E. Copeland, J.R. Hermanson, e R.H.L. Wat, "*Going public—what it involves: A framework for providing advice to management*", Journal of Accountancy 1984.

verificare se questo *spread* fissato al 7% non costituisca una prova di tacito accordo tra gli intermediari finanziari[27].

Altri ritengono invece che il mercato sia perfettamente concorrenziale e dunque la percentuale richiesta sia in linea con gli sforzi richiesti per seguire un processo di quotazione ed offrire allo stesso tempo un servizio di consulenza particolarmente complesso[28]. Una prova a supporto di questa tesi sta nel fatto che secondo alcuni studi, il mercato delle *IPO* è caratterizzato da una bassa concentrazione e da una facile entrata di nuovi attori, questo indica un ambiente competitivo dove non è necessaria una collusione per mantenere gli spread al 7%. Hansen avanza un'ulteriore ipotesi, ossia che i sottoscrittori competono sul prezzo delle IPO basandosi su reputazione e servizi offerti, piuttosto che fissando i prezzi. Questo ragionamento supporta l'idea che il mercato risulti competitivo e che le banche di investimento si sforzano di offrire il miglior servizio possibile per attrarre clienti, nonostante ciò, però molti dubbi permangono in merito a questa evidenza sui prezzi e l'idea di concorrenzialità del mercato. Non a caso infatti nonostante la tesi di Hansen la maggioranza, altri studi dimostrano che la maggioranza delle IPO viene sottoscritta dei medesimi intermediari finanziari, andando di fatti a creare una sorta di oligopolio, sfatando appunto le prove in merito ad una mancanza di barriere nel settore finanziario e quindi di un'elevata concorrenzialità nel processo.

Di seguito si riportano i dati relativi ai sottoscrittori delle principali emissioni azionarie statunitensi[29]:

Underwriter	Number of IPOs	Average First-day Return	Average 3-year Buy-and-hold Return		
			IPOs	Market-adjusted	Style-adjusted
Goldman Sachs	272	27.6%	6.5%	-22.3%	-33.9%
JPM	224	25.7%	20.9%	-7.8%	5.6%
Morgan Stanley	218	26.9%	31.3%	3.0%	2.5%
BOA-Merrill	133	24.5%	15.0%	-15.8%	-8.5%
Jefferies	91	24.3%	-2.1%	-32.2%	-33.5%
Citigroup	82	8.0%	21.9%	-10.5%	-27.7%
UBS/Credit-Suisse	89	10.9%	16.8%	-17.3%	-16.2%
Barclays	46	16.7%	28.9%	0.7%	10.9%
Cowen	29	26.1%	-43.4%	-74.0%	-100.3%
Deutsche Bank	19	11.7%	44.4%	12.7%	-1.8%
Stifel	18	12.3%	44.8%	11.7%	25.3%
Others (regionals)	118	11.1%	9.8%	-24.5%	-16.3%
Others (lower tier)	140	38.2%	-42.3%	-67.4%	-28.1%
2012-2021	1,479	23.6%	10.4%	-19.3%	-15.6%

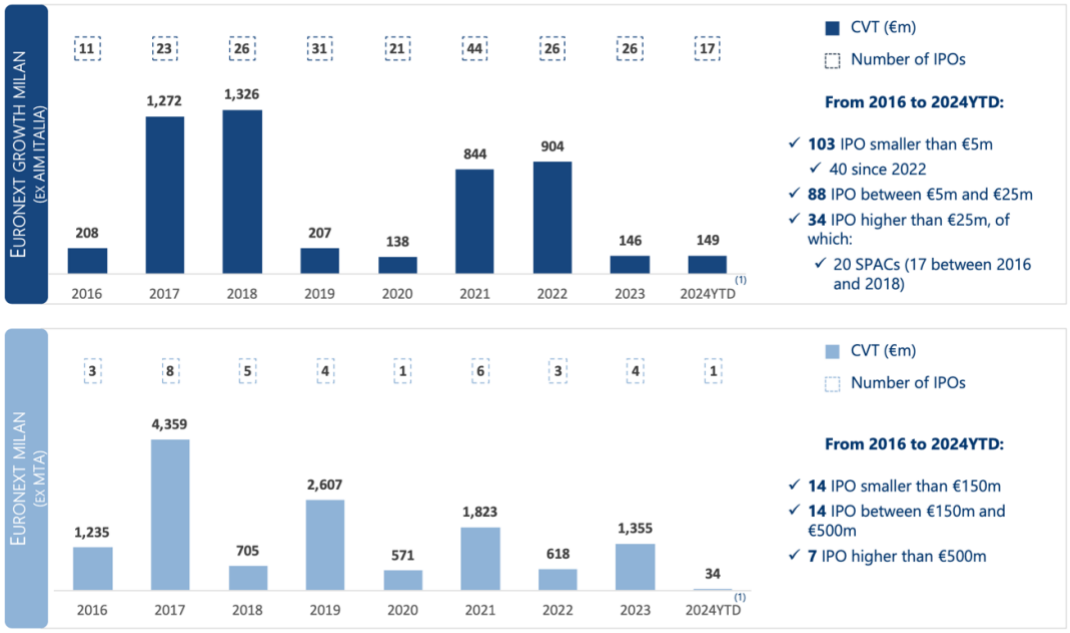
[27]H.C. Chen e J.R. Ritter, "*The Seven Percent Solution*", in Journal of Finance, n. 55, pp. 1105-1132, 2000.
[28] R. Hansen, "*Do Investment Banks Compete in IPOs?: The Advent of the Seven Percent Plus Contract*", in Journal of Financial Economics, n. 59, pp. 313-346, 2001.
[29] J. R. Ritter, "*Initial Public Offerings: Underwriting Statistics Through 2024*", Warrington College of Business, University of Florida, 27 Jan 2025.

In seguito un ulteriore aspetto considerato da Gao, Ritter e Zhu risiede nella necessità di adattamento più rapido in settori più tecnologicamente avanzati, questo proposito infatti richiede un livello di flessibilità operativa che le politiche relative alla quotazione non consentono di ottenere. Al contrario imprese finanziate mediante *venture capital* presentano maggiori pressioni per una rapida espansione e quindi consentono maggiore flessibilità operativa e agilità per rispondere e adattarsi alle condizioni di mercato, senza obblighi particolarmente gravosi in termini reputazionali, rendendo difatti la quotazione meno attraente.
Analizzando poi la situazione del mercato primario italiano, i numeri sono perfettamente concordi con le evidenze del mercato statunitense. Anche in Italia si è assistito ad una forte diminuzione delle *IPO* in sostanza per le medesime ragioni in precedenza esplicitate, ovvero per i costi diretti ed indiretti, eccessiva burocrazia e mancanza di flessibilità di azione. Oltre a ciò, bisogna poi aggiungere che il tessuto economico-sociale italiano differisce profondamente da quello degli USA. In effetti in Italia la circa l'80% delle imprese appartiene alla categoria di *PMI*, in aggiunta a ciò, molto spesso il legame che è presente tra i soci delle imprese è di stampo famigliare, il che complica ulteriormente le procedure relative alla quotazione. Molto spesso il *management* fa fatica a seguire tutte le regole imposte dal processo, a maggior ragione nel caso in cui l'impresa fino a poco tempo prima era totalmente assoggettata nelle mani di un solo proprietario oppure di una singola famiglia[30].
I dati relativi ai recenti sviluppi sul mercato primario italiano, sia *Euronext Milan* che *Growth*, supportano appunto queste evidenze di debolezza intrinseca nello strumento soprattutto in seguito al 2022, anno aveva fatto registrare un record per il numero di operazioni e di capitale raccolto sin dal 2018.
In seguito si riportano delle elaborazioni che descrivono la situazione del marcato primario azionario in italiana a partire dal 2016, prendendo in considerazione i dati del *MTA* (Mercato Telematico Azionario), ovvero l'attuale *Euronext Milan* e i dati relativi *AIM* Italia (*Alternative Investment Market*) cioè l'attuale *Growth*.
Risulta evidente soprattutto per l'anno 2024 come sia in termini di raccolta che di operazioni, gli intermediari finanziari abbiano faticato a registrare dei risultati soddisfacenti, nello specifico sul totale delle sottoscrizioni, nell'arco di circa otto anni, soltanto due volte si è

[30] M. Gonzalez, A. Guzman, C. Pombo, e M. Trujillo, "*Family firms and financial performance: the cost of growing*", *Emerging Markets Review*, Vol. 13 No. 4, pp. 626-649, 2012.

registrato un risultato superiore al miliardo di euro, numeri che confrontati con il *fundraising* attuato dai fondi di *VC* e PE, sono essenzialmente infinitesimi[31].

Evoluzione delle IPO sui mercati azionari di Borsa Italiana[32]:



Fonte: EQUITA ufficio studi

1.4 Fenomeno dell'*underpricing*: serie storiche ed evidenze in altri mercati

Un ulteriore problematica che la società deve tenere in considerazione nel momento in cui decide di avviare un processo di quotazione è il fenomeno dell'*underpricing*. Questo si caratterizza come un costo indiretto, definito come differenziale tra il prezzo di emissione e il prezzo delle azioni raggiunto alla fine del primo giorno di negoziazione sui mercati[33]. Nel caso in cui il prezzo raggiunto dai titoli è maggiore rispetto al prezzo concordato tra la società ed i sottoscrittori; significa che vi è una perdita per l'emittente poiché è come se avesse sottovalutato i propri titoli, danneggiando gli azionisti preesistenti e precludendosi al tempo stesso l'opportunità di ottenere maggiori risorse finanziarie.

Questo fenomeno è molto più comune nei mercati meno efficienti, ossia nei contesti finanziari dove si hanno alte asimmetrie informative, che permettono quindi di poter approfittare di questa discrepanza di informazioni e quindi realizzare maggiori profitti. Generalmente la teoria

[31] M. D'Ascenzo, "*Private capital, 2022 miglior anno di sempre con 23,6 miliardi investiti"*, Il Sole24Ore.
[32] Equita - LUISS Report: "*Recent trend of IPOs on Italian markets"*, Ottobre 2024.
[33] Rathnayake, Nawadali, Louembé et Al., *"Are IPOs underpriced or overpriced? Evidence from an emerging market*," Research in International Business and Finance, vol. 50, pages 171-190, 2019.

dell'asimmetria informativa non si applica soltanto ai mercati finanziari nei quali s'intende avviare il processo di quotazione, bensì anche ai settori di riferimento delle imprese. Molti studi[34], supportati da analisi econometriche evidenziano che nei paesi emergenti questo fenomeno risulta si può osservare molto spesso, rispetto ai mercati più efficienti, tuttavia le conclusioni definite per questi mercati possono essere usate anche per descrivere un quadro generale di questo fenomeno, andando a prendere in considerazione quali sono i fatti che maggiormente influenzano un'*IPO*.

In un particolare studio[35], si fa riferimento a due tipi di modelli econometrici basati sugli *OLS*, al fine di stimare due variabili dipendenti, ossia l'*Initial Return* (*IR*) ed il *Market-Adjusted Abnormal Return* (*MAAR*). Il primo modello permette di valutare il rendimento immediato, ovviamente sottoforma di percentuale, che gli investitori ottengono dopo il primo giorno di contrattazione del titolo, mentre il secondo definisce la differenza tra il rendimento effettivo dell'azione ed il rendimento atteso, basandosi sul movimento generale del mercato durante lo stesso periodo, fornendo una visione dell'efficacia dell'*underpricing* rispetto alla performance generale del mercato.

Di seguito si riportano le formule usate per definire e calcolare tali variabili:

$$IR_i = \frac{P_{i1} - P_{i0}}{P_{i0}} \times 100$$

$$MAAR_i = [(1 + R_{m1})(1 + IR_{i1}) - 1] \times 100$$

Dove P_{i1} è il prezzo di chiusura nel primo giorno di trading dell'azienda *i*, mentre P_{i0} è il prezzo di offerta. Invece nel caso del *MAAR*, R_{m1} è il ritorno del mercato nel primo giorno di trading, ossia: $\frac{P_{m1}-P_{m0}}{P_{m0}} \times 100$, dove P_{m1} e P_{m0} sono i valori dell'indice di mercato alla chiusura nel primo giorno di trading e al giorno dell'offerta pubblica iniziale.

I modelli *OLS*, si caratterizzano per avere differenti coefficienti, circa undici per l'*IR* e dodici per il *MAAR*, queste si configurano come variabili indipendenti che secondo gli autori possono essere significativamente rilevanti per spiegare questo fenomeno di *underpricing.* Di seguito si riportano i modelli analitici usati per definire la regressione lineare, tuttavia è ben sottolineare

[34] T. Loughran, J. R. Ritter e K. Rydqvist, "*Initial Public Offerings: International Insights*", in Pacific-Basin Finance Journal, n. 2, pp. 165–199, 1994, aggiornato al febbraio 2021: bear.cba.ufl.edu/ritter.

[35] Rathnayake, Nawadali, Louembé et Al., *"Are IPOs underpriced or overpriced? Evidence from an emerging market*," Research in International Business and Finance, vol. 50, pages 171-190, 2019.

che gli autori hanno ritrovato delle evidenze significative, il un *range* che va dal 10% fino all'1% di significatività[36]:

- *lnSIZE*: Il coefficiente dimensionale dell'impresa sul scala logaritmica; β = -0.12 ***
- *lnLAG*: *log* del tempo tra l'annuncio dell'IPO e l'effettiva quotazione; β = 0.36 **
- *SENT* : la variazione percentuale del sentimento di mercato; β = 0.21 ***
- *RISK*: rischio associato, il reciproco del prezzo nominale dell'offerta; β = 0.53 *
- *HOT*: coefficiente del ciclo favorevole alle offerte pubbliche (hot issue); β = 0.59 *

$$IR_{it} = \beta_0 + \beta_1 \ln(\text{AGE}) + \beta_2 \ln(\text{SIZE}) + \beta_3 \ln(\text{LAG}) + \beta_4 \text{SENT} + \beta_5 \ln(\text{VOL}) + \beta_6 \text{MVL} + \beta_7 \text{RISK} + \beta_8 \text{PRC} + \beta_9 \text{BRD} + \beta_{10} \text{PRIV} + \beta_{11} \text{HOT} + \beta_{12} \text{IND} + \epsilon_{it}$$

$$MAAR_{it} = \beta_0 + \beta_1 \ln(\text{AGE}) + \beta_2 \ln(\text{SIZE}) + \beta_3 \ln(\text{LAG}) + \beta_4 \text{SENT} + \beta_5 \ln(\text{VOL}) + \beta_6 \text{MVL} + \beta_7 \text{RISK} + \beta_8 \text{PRC} + \beta_9 \text{BRD} + \beta_{10} \text{PRIV} + \beta_{11} \text{HOT} + \beta_{12} \text{IND} + \epsilon_{it}$$

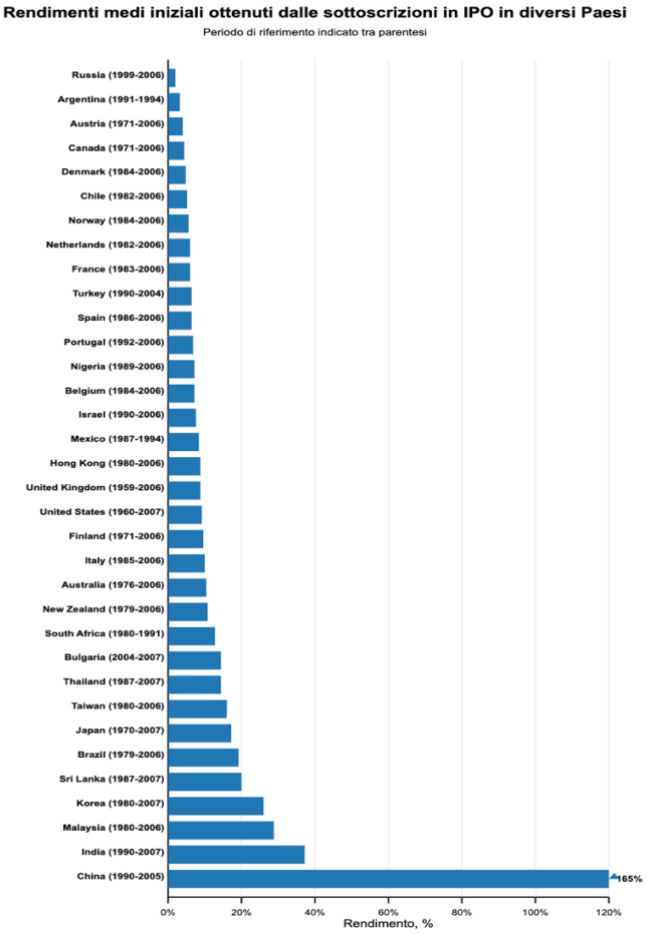
In sintesi, lo studio dimostra come questi coefficienti da soli riescono a spiegare tra il 21% ed il 28% dell'*underpricing* osservato nelle *IPO* per i mercati emergenti, ovviamente descrivendo tali risultati in termini di R^2 *adjusted*, visto che lo studio ha impiegato una metodologia *OLS*. Il campione non di meno risulta essere particolarmente vasto, racchiudendo infatti 148 offerte pubbliche iniziali, avvenute in Paesi emergenti, in un arco temporale dal 1997 al 2017, coprendo quattordici settori industriali, con un'enfasi particolare sul settore bancario, finanziario e assicurativo, che rappresenta circa il 28% del totale. Fino al settore della tecnologia e dell'informazione che rappresenta il 16,5%, inferiori sono poi le quote dei restanti settori come: manifattura, servizi, trasporti e agricoltura. ciò quindi può significare che seppur con differenze indubbiamente più rilevanti questi fattori sono ugualmente significativi anche per il mercato occidentale, il quale di certo presentando minori asimmetrie informative, risulta più efficiente in tal senso, sulla determinazione dei prezzi.

[36] In questa sede si vuole usare la notazione econometrica standard, ovvero tre asterischi (***): significatività all'1%; (**): significatività al 5%; (*): significatività al 10%.

Queste ipotesi sono dimostrate anche in altri studi, come accade con l'analisi di Ritter[37], quest'ultimo prendendo in considerazione un campione di Paesi con mercati finanziari avanzati ed altri con mercati meno efficienti.

La conclusione a cui giunge è identica rispetto a quanto sopra, i medesimi fattori sono fondamentali per spiegare la fenomenologia di prezzi molto più bassi rispetto alla quotazione, riscontrando maggiori inefficienze nei Paesi con asimmetrie più elevate.

Di seguito si riporta un grafico che definisce i rendimenti medi iniziali in un campione di Paesi eterogenei, con relative serie temporali.



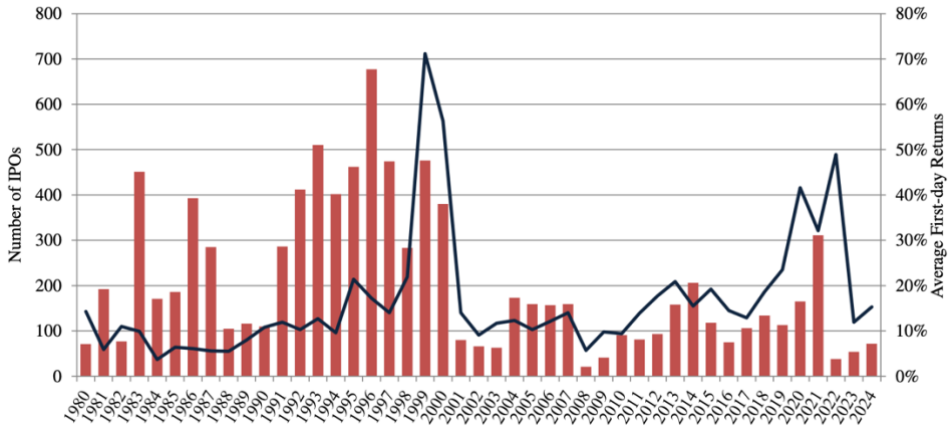
Fonte: elaborazione propria sui dati di J.R Ritter; bear.cba.ufl.edu/ritter.

Analizzando poi altre serie storiche, si può notare come l'*underpricing* segue pedissequamente le fasi cicliche del mercato delle offerte pubbliche iniziali, confermando quindi le osservazioni e le analisi econometriche sul fattore *Hot Issue*, in altri termini negli anni in cui si registrano maggiori presenze di *IPO*, l'*underpricing* è tendenzialmente maggiore, ciò risulta vero soprattutto in seguito ai primi anni duemila. Non a caso infatti esistono degli studi che hanno

[37] T. Loughran, J. R. Ritter e K. Rydqvist, op. cit.

evidenziato come le imprese assoggettate ad un business di tipo *tech* abbiano maggiore probabilità di incorrere nel fenomeno di *underpricing*[38]. Ciò è dovuto appunto all'incertezza da parte dei sottoscrittori, ossia nel momento in cui si ritrovano a dover collocare l'intera emissione sul mercato, gli stessi cercano di concordare un prezzo più basso di modo che possano liberarsi più facilmente di azioni di fatto più rischiose, poiché il settore presenta molte incertezze ed asimmetrie informative. In effetti gli investitori, non conoscendo in modo meticoloso il modello di *business* della società decidono di evitare di acquistare azioni con prezzi molto elevati, proprio per eludere la *winner's curse.*

Numero di IPO e rendimenti medi del primo giorno per anno, 1980-2024



Fonte: J.R. Ritter:bear.cba.ufl.edu/ritter.

Quest'ultimo si può tradurre come "maledizione del vincitore", ossia un fenomeno in base al quale un compratore si aggiudica un *asset* soltanto perché questi ha sovrastimato l'effettivo valore, finendo quindi per pagare un prezzo troppo elevato.

Gli investitori quindi saranno maggiormente esposti alla maledizione del vincitore soltanto quando non hanno i mezzi per riconoscere: l'effettivo valore dell'impresa, il business di riferimento e l'attrattività di un'emissione sul mercato.

Una parte della letteratura ritiene infatti che un minimo di *underpricing* sia un aspetto positivo per la società emittente, poiché nel lungo termine gli investitori potranno finanziare più facilmente un'impresa che in passato si è dimostrata al di sopra delle aspettative, tuttavia ciò non toglie la perdita di opportunità. Ma al tempo stesso l'emissione sarà più attrattiva presso il pubblico *retail*, poiché gli investitori consapevoli di un possibile *underpricing* potranno chiudere le proprie posizioni più o meno in pareggio.

[38] D. Salerno, G. Sampagnaro, V. Verdoliva, "*Fintech and IPO underpricing: An explorative study*", University of Naples Parthenope, 2022.

Questa fenomenologia è stata osservata anche in altri studi, attraverso degli esperimenti controllati, gli investitori con l'obiettivo di acquisire un'impresa, sperimentavano gli effetti della maledizione del vincitore, sopravvalutando l'affare. Ciò era dovuto alla mancanza di informazioni e all'ascolto di messaggio fuorvianti che poco si riferivano all'effettivo valore dell'impresa, tuttavia la situazione cambiava nel momento in cui i soggetti acquisivano esperienza e pertanto osavano inserirsi nella contrattazione nel momento in cui vi erano delle opportunità di guadagno, in altre parole la presenza di un *underpricing*[39].

Un altro studio si è poi focalizzato sulle evidenze empiriche del mercato nipponico, infatti a partire dal 1989, il Giappone ha sperimentato in media sui mercati primari, un *underpricing* molto più basso rispetto al periodo successivo al 1995, ossia in seguito all'introduzione del *bookbuiding*[40]. Ciò è pertanto dovuto alla modalità di contrattazione delle *IPO*, similmente a come accade con i titoli del tesoro statunitense ed i buoni poliennali del tesoro in Italia, in Giappone anche le offerte pubbliche iniziali venivano contrattate seguendo un'asta marginale, che consentiva di attutire gli effetti della maledizione del vincitore, consentendo agli investitori non informati di fare offerte non competitive, in cui viene indicata una quantità, ma non il prezzo. Il campione dello studio è appunto molto ampio, ovvero 321 *IPO*, che dimostrano appunto come questa alternativa possa rendere più efficienti i mercati e quindi andare a favore di tutti i soggetti convolti nell'ambito di un'emissione primaria.

Quest'ultimo esempio presentato risulta una chiara evidenza che mette in discussione l'attuale procedura di quotazione sul mercato primario, che in base alle affermazioni esposte in precedenza nell'attuale elaborato, non è esente da inefficienze che si dimostrano persistenti nell'arco degli anni.

[39] D. Di Cagno, W. Guth, N. Pace, L. Pannaccione, "*Experience and Gender Effects in an Acquiring-a-Company Experiment Allowing for Value Messages*", Luiss Guido Carli University, 2015.
[40] F. Kerins, K. Kutsuna, R. Smith, "*Why Are IPOs Underpriced? Evidence from Japan's Hybrid Auction-Method Offerings*" Claremont Graduate University Working Paper, 2003.

Capitolo Secondo

Disintermediazione: tecnologia *Fintech* al servizio del mercato primario

Il presente capitolo intende procedere con un'analisi relativa alla descrizione delle nuove tecniche di disintermediazione, concentrandosi dapprima sul funzionamento generale della *blockchain*, nonché sugli *smart contract* e *non fungible tokens*. A tal proposito nel prosieguo verranno delineati le metodologie di implementazione di tali strumenti nel conteso del mercato primario, con l'obbiettivo di massimizzare il valore dei titoli in sede di mercato. Nella seconda parte si procederà con un confronto tra i processi di quotazione, descrivendo i relativi vantaggi e svantaggi, infine l'analisi si focalizzerà sul quadro normativo attuale per l'implementazione delle tecnologie *fintech*, andando ad approfondire l'aspetto della trasparenza e dell'antiriciclaggio.

2.1 Introduzione alla tecnologia *Blockchain*: *Proof of Work* e *Proof of Stake*

Un tradizionale sistema finanziario può essere spiegato in modo astratto come un insieme di nodi, che rappresentano individui ed istituzioni al suo interno, questi ultimi sono connessi tra loro da reti, ovvero dalle transazioni che realizzano quotidianamente. In modo speculare un sistema di pagamento è caratterizzato da una serie di conti e di saldi, dove le transazioni specificano il movimento dei fondi nel corso del tempo, tra i diversi conti della rete.

Nel sistema finanziario tradizionale, l'intermediazione finanziaria è necessaria affinché questo struttura possa funzionare in modo corretto, gli intermediari infatti sono i responsabili del controllo e dell'accuratezza dei conti, nonché della contabilità e della sicurezza[41].

Fino a pochi anni fa, questo sistema caratterizzato dalla presenza di intermediari, era l'unica opzione possibile per garantire un senso di fiducia ed affidabilità ai propri clienti, grazie alle istituzioni finanziarie gli stessi potevano sentirsi maggiormente tutelati nelle transazioni quotidiane, nell'esercizio del risparmio e del credito.

Tuttavia oggi attraverso i recenti progressi tecnologici, è possibile implementare delle architetture finanziarie alternative che non necessitano dell'azione di alcun intermediario oppure di entità centralizzate che garantiscono la sicurezza della rete ed il controllo sulle transazioni. Questa architettura viene chiamata con il nome di *Distributed Ledger Technology*

[41] I. Makarov, A. Schoar, "*Cryptocurrencies and Decentralized Finance (DeFi)*", MIT Sloan School of Management, Marzo 2022.

(*DLT*), e si caratterizza per la presenza dei "validatori", ovvero di soggetti predisposti alla validazione appunto delle transazioni che avvengono nel sistema. In questa nuova architettura nessuno ha il controllo completo sulle transazioni, al contrario i validatori hanno a disposizione una serie di copie del registro dei pagamenti, decidendo quindi in modo congiunto quali transazioni risultano ammissibili o meno nel sistema.

La *blockchain* nello specifico è una forma di *DLT*, dove le transazioni sono registrate e crittografate in blocchi collegati tra di loro, uno tra i principali vantaggi di questa tecnologia è relativo alla sicurezza, poiché viene scongiurata l'ipotesi del singolo punto di fallimento. Attraverso la *blockchain* ogni validatore ha a diposizione una copia del registro delle transazioni, il che permette di garantire la sicurezza della rete, anche nell'eventualità del fallimento di un nodo. Questa tecnologia trova infatti forza nella numerosità della rete, di conseguenza più validatori sono coinvolti all'interno di essa e più il sistema sarà sicuro, il protocollo *blockchain* consente la presenza di più punti di fallimento o di corruzione, a condizione che la maggioranza dei validatori non sia compromessa. In particolare, permette ai validatori di essere soggetti che non si fidano l'uno dell'altro o che sono addirittura avversari, questa situazione quindi garantisce l'affidabilità della *blockchain*[42].

Allo stati attuale esistono due tipologie di *blockchain*, ovvero quelle *permissioned* e le *permissionless*, nel primo caso il gruppo di validatori deve essere necessariamente approvato da un'entità coordinatrice, che può essere un'impresa oppure un'istituzione privata, mentre nel secondo caso non vi è la presenza di alcun vincolo in termini di numero o identità dei validatori. Oltre a ciò, le *blockchain* possono essere classificate come pubbliche oppure private, in questo senso nel primo caso è chiaro che chiunque può accedervi mentre nel secondo caso solo le parti autorizzate possono osservare le transazioni, infatti le *blockchain permissioned* sono classificate come private, mentre quelle *permissionless* sono classificate come pubbliche. La differenza più grande che si può riscontrare tra le due tipologie di *blockchain* nel caso *permissioned*, gli utenti devono avere fiducia nei validatori, oppure nelle entità istituzionali che approvano questi ultimi, mentre nelle permissionless vi è un meccanismo di controllo che non si basa sulla fiducia quanto piuttosto un sistema definito come "*trustless trust*".

Nel primo caso le *blockchain* permissioned presentano un difetto di base che in fin dei conti non li rende molto dissimili dall'attuale sistema finanziario, le banche o gli altri intermediari comune presentano una licenza rilasciata da un'entità centrale, proprio come i validatori, pertanto secondo alcuni studi questa tecnologia è comunque soggetta agli stessi tipi di fragilità.

[42] I. Makarov, A. Schoar, op. cit.

Il secondo caso, ovvero le *blockchain* permissionless utilizzano un'architettura di "fiducia senza fiducia", in altri termini siccome chiunque potenzialmente può diventare validatore, sistema è potenzialmente vulnerabile a un attacco *Sybil*, in cui un soggetto malintenzionato sovverte il sistema creando un gran numero di validatori pseudonimi per ottenere un'influenza sproporzionata sul protocollo di consenso[43]. Al fine di risolvere questa problematica sono stati implementati due tipologie di approcci, ovvero il *proof of work* (*PoW*) ed il *proof of stake* (*PoS*). L'idea alla base di entrambi è quella di fornire ai validatori un incentivo economico, ovvero una ricompensa per la validazione delle transazioni con l'obiettivo di rendere costoso e poco invogliante per un malintenzionato l'idea di ottenere una quota di controllo maggioritaria e sovvertire il sistema. La ricompensa serve a incentivare finanziariamente i validatori ad operare in modo onesto, può assume due forme, quella di commissione di transazione e di ricompense di blocco predeterminate, in questo caso il protocollo distribuisce automaticamente una quantità esatta della valuta della *blockchain*, che funge da tassa di diluizione per gli altri utenti[44]. Come definito in precedenza, al fine di affermare la sicurezza e la stabilità nella transazioni che avvengono su *blockchain*, possono essere usati due tipi di approcci, ossia, il *proof of work* ed il *proof of stake*.

Per quanto concerne il *proof of work*, questo approccio viene usato nella *blockchain* di *Bitcoin* ed almeno inizialmente anche nella *blockchain* di *Ethereum*, che ad oggi risultano le due criptovalute più conosciute sul mercato. Nel *PoW*, i validatori sono chiamati con il nome di *miners*, gli stessi competono tra di loro al fine di poter validare tramite la potenza di calcolo computazionale più blocchi possibili nella *blockchain*. In altre parole i *miners* sono in competizione per il diritto di verificare le transazioni, queste infatti vengono aggregate in blocchi, l'obiettivo è quello di ricercare un valore chiamato *nonce*, che combinato con altre transazioni del blocco e altre informazioni come: *timestamp*, *harsh* del blocco precedente, produca un numero valido, chiamato appunto *harsh*. Questo *harsh* deve soddisfare delle caratteristiche più o meno complesse per validare il blocco, l'intero processo in questione prende il nome di *mining*, lo stesso può variare molto a seconda della *blockchain*, infatti più miners sono presenti su di essa più difficile diventa il problema matematico-computazionale da risolvere su *BTC*, attualmente viene "minato" in media un blocco ogni dieci minuti. In seguito all'ottenimento dell'*harsh*, il primo *miner* lo comunica alla rete, dove gli altri miners potranno validare la soluzione, e quindi aggiungere di conseguenza un ulteriore blocco alla

[43] M. Orcutt, "*What is Blockchain?*", Massachusetts Institute of Technology Review, 2018.
[44] Satoshi Nakamoto "*Bitcoin: A Peer-to-Peer Electronic Cash System*", protocollo originale Bitcoin, 2008.

catena ed il *miners* riceverà una ricompensa sotto forma di criptovaluta e commissioni di transazioni per la validazione nella rete.

Per condurre un attacco alla *blockchain* che utilizza questo approccio di *PoW*, il *miner* malintenzionato deve avere a disposizione almeno il 51% della potenza computazionale sull'intera rete, in tal senso si spiega perché si definisce "*51% attack*". Una volta quindi che il *miner* ha a disposizione questa potenza computazionale, allora potrà modificare le transazioni sul sistema, ad esempio approfittandosi di spendere per due volte la stessa criptovaluta, questo fenomeno è noto come "*double spending attack*". Come definito in precedenza i *miners* devono avere un incentivo economico per avere maggiore potenza computazionale, e lo stesso si ritrova proprio nella validazione delle transazioni, nell'approccio *PoW*, quindi le ricompense ottenute giustificano l'accumulo di *harsh power*. In tal senso non ci sono disincentivi per non accumulare più potenza computazionale possibile, dunque l'unica barriera al 51% risiede proprio nella fattibilità di accumulare tale percentuale di potenza di calcolo[45]. Come accade anche al sistema finanziario tradizionale gli utenti hanno un certo grado di fiducia sulla *blockchain*, di conseguenza ogni attacco riuscito riduce drasticamente la fiducia negli utenti e quindi anche il valore della criptovaluta, con il risultato di impedire il recupero degli investimenti iniziali da parte dei *miners*. In sostanza dunque più elevati risultano essere i costi iniziali e più saranno disincentivati i *miners* ad attaccare l'intera *blockchain*, poiché non le criptovalute in tal senso vedranno cade il proprio valore.

Tuttavia oggi non è necessario accumulare una potenza di calcolo tale su un unico *hardware* fisico, vi sono infatti dei potenziali rischi alla sicurezza della *blockchain* che sono direttamente collegati all' emergere di mercati come *NiceHash*, dove la potenza di *mining* può essere affittata per un periodo di tempo specifico, rendendo possibile un eventuale attacco. Oppure un'altra ipotesi più concreta è relativa all'attacco da parte dei *mining pools*, si stima infatti che circa il 10% dei *miners* controlla di fatto il 90% del *mining*, mentre lo 0,1%, ossia 50 miners controllano la *blockchain* con una percentuale di mining pari al 50%[46]. Questa eventualità viene minimizzata affermando che i *miners* possono semplicemente lasciare una *mining pool* per unirsi ad un'altra, quindi l potere di un operatore di *mining pool* rispetto ai singoli *miners* dipende dalla facilità con cui gli stessi possono spostare la loro capacità tra le *pool*, che a sua

[45] E. B. Budish, "*The Economic Limits of Bitcoin and the Blockchain*", University of Chicago Booth School of Business, Paper No. 18-07, 2018.

[46] L. W. Cong, Z. He, and J. Li, "*Decentralized Mining in Centralized Pools*". The Review of Financial Studies, 34(3):1191–1235, 2020.
D. Ferreira, J.Li, R. Nikolowa, "*Corporate Capture of Blockchain Governance*". Working Paper 593, European Corporate Governance Institute (ECGI), 2019.

volta dipende dalla distribuzione dimensionale dei *miners*. La struttura originale creata da Satoshi Nakamoto, l'inventore di *Bitcoin*, immaginava un mondo in cui il *mining* fosse completamente decentralizzato e non dipendesse da pochi attori di grandi dimensioni. In questo scenario infatti, sarebbe stato difficile per i *miners* colludere, e il fallimento di un singolo miner non avrebbe avuto alcun impatto sulla sicurezza della rete.
Di seguito si riportano delle statistiche descrittive sull'attuale concentrazione dei *pools*[47]:

Fig.1

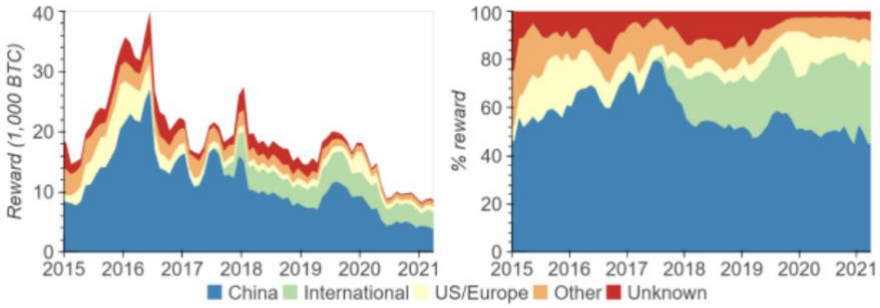
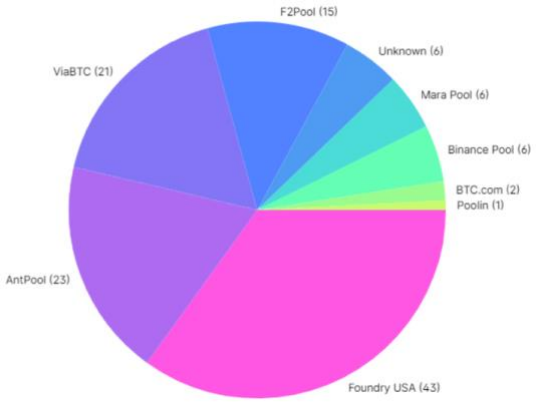


Fig.2



Oltre a ciò, l'approccio *PoW* risulta essere molto costoso in termini energetici ed inoltre l'efficienza relativa alla velocità di transazione risulta essere particolarmente bassa. Tutti questi svantaggi si accentuano ancora di più quando si parla della seconda tipologia di approccio,

[47] A. Simeone, "*Natura e rilevanza delle contabilità decentralizzate*", Report CONSOB, 2024;
La fig.1 rappresenta la quantità e la percentuale di ricavi derivanti dalle ricompense del *mining*, in base alla collocazione delle *farm*. Si nota che prima del 2018 la Cina era il paese che ospitava il più alto numero di *farm*, poiché offriva maggiori vantaggi in termini di regolamentazione ed il costo dell'energia era particolarmente basso. In seguito al 2021 tuttavia, il governo ha bandito le criptovalute, dichiarando illegale sia le transazioni che l'attività di *mining*, avvantaggiando quindi altri Paesi si sono aperti a questo mercato.
Nella fig. 2 si ritrovano i maggiori *pools* di validatori, dalla rappresentazione grafica si nota che la possibilità di un'eventuale "attacco al 51%", non sia poi così remota dal momento che solo l'unione di AntPool e Foundry potrebbe compromettere la *blockchain* di BTC.

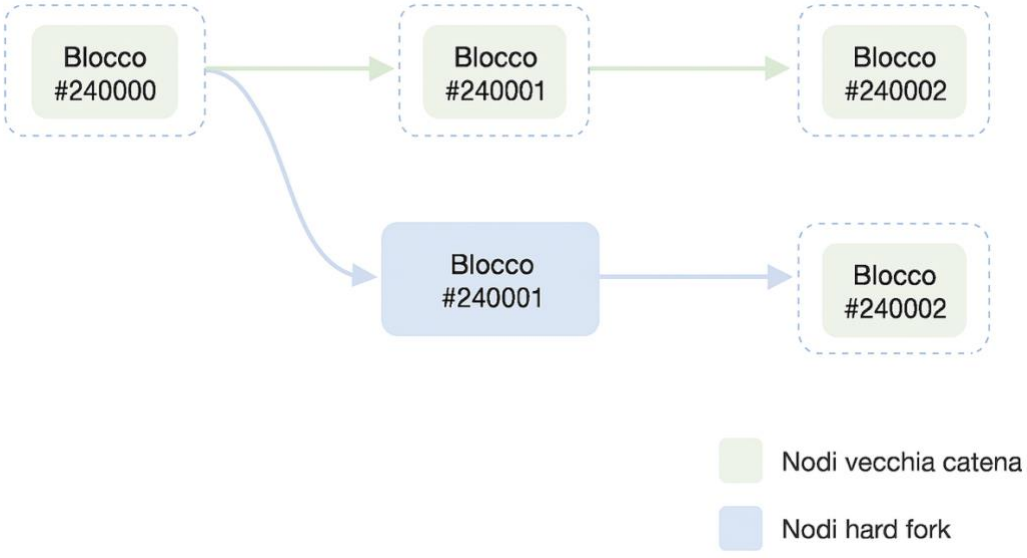
ovvero il proof of stake. In questo contesto non conta la potenza computazionale, bensì la quantità di criptovalute messe in garanzia, appunto in stake. Questo approccio infatti presenta dei bassi costi energetici, paragonabili al circuito Visa[48], ed inoltre risulta essere molto più efficiente in termini di velocità di transazione. Come già definito il proof of stake si basa sulla garanzia di criptovalute inserite al fine di validare una transazione, maggiore sarà l'importo messo in garanzia e più probabilità si avranno di validare un blocco di transazione e quindi ricevere la ricompensa e le commissioni in termini della medesima criptovaluta usata nella *blockchain*. Questo meccanismo disincentiva gli eventuali tentativi di frode, poiché nel caso in cui il validatore sia malintenzionato o abbia lo scopo di manipolare il sistema l'ammontare messo in garanzia verrà confiscato e quindi definitivamente perso, questo meccanismo prende il nome di *Slashing*. L'idea alla base del PoS è che un soggetto con una grande partecipazione alla rete non ha l'interesse a danneggiarla, anzi i guadagni generati dall'attacco non andrebbero a compensare la svalutazione della cripto moneta senza contare le eventuali penalità dovute allo *slashing*. Tuttavia anche questo approccio non è immune da pericoli, attraverso questa eventualità non vi sono dei rischi di *double spending*, come accade invece nel caso del *PoW*, bensì le *blockchain PoS* sono una base per *smart contract* e addirittura anche per altre *blockchain*. Nel caso in cui un validatore malintenzionato volesse speculare mediante uno *smart contract*, avrebbe la possibilità di attaccare la *blockchain* di base nel caso in cui i *token* di riferimento abbiano un valore più basso rispetto ai *token* dello stesso *smart contract*. Al fine di scongiurare questa eventualità, generalmente il *token* della *blockchain* presenta un valore maggiore rispetto a quelli definiti negli *smart contract*, un'alternativa è invece quella di adottare la medesima tipologia di *token* anche per il funzionamento del contratto, in modo da renderlo meno scalabile ad attacchi esterni.

Come discusso in precedenza uno dei problemi fondamentali per il *PoW* è la concentrazione della capacità di calcolo nei *pools*. Analogamente anche nell'approccio *PoS* vi sono le medesime problematiche. L'algoritmo infatti predilige i validatori che mettono in "*stake*" ovvero in garanzia, più *token* dunque i validatori hanno un maggiore incentivo ad unirsi e combinare i propri *stake*. Il risultato di questo fenomeno ad oggi è il seguente, prendendo in considerazione i validatori più rilevanti, i primi 10 presentano un controllo del 14% su tutte le *blockchain* di tipo *PoS*, se si passa ai primi 50 allora il controllo aumenta fino al 32%, mentre se il campione si allarga fino ai 100 più grandi il controllo arriva al 41%. Questo dimostra come

[48] M. Platt *et al*., "*The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work*," 21*st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2021, pp. 1135-1144

l'aggregazione di tali soggetti possa creare delle interdipendenze pericolose. Tuttavia questa eventualità secondo alcuni studi[49] si potrebbe facilmente aggirare tramite una biforcazione della *blockchain*. In altri termini nel caso in cui un gruppo di validatori dovesse sferrare un attacco alla *blockchain* o sfruttare in modo indebito i propri *token*, gli stessi verrebbero immediatamente bloccati dal resto della comunità che usa proprio la *blockchain*, rendendo illegale oppure annullando le transazioni che hanno compromesso l'intero registro. In questo caso il senso di legittimità è un cardine fondamentale, poiché i validatori reagirebbero copiando tutti i bilanci dei *token*, tranne quelli partecipanti all'attacco realizzando un nuovo registro, ovvero quello che nel gergo si definisce una biforcazione dalla *blockchain* originaria. La lezione in questo senso è che chiunque cerchi di abusare e di sfruttare in modo fraudolento questa tecnologia può essere facilmente aggirato e pertanto i profitti teorici realizzati in tal senso verrebbero annullati[50], marchiando di fatti gli stessi validatori fraudolenti come non meritevoli di fiducia, la legittimità è dunque strettamente connessa con il senso di comunità della struttura.

Rappresentazione grafica del processo di biforcazione (Hard Fork):



Fonte: elaborazione propria su schema di BitBox.

[49] V. Buterin, "*Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains*", Seven Stories Press, 2022.

[50] Questa eventualità si è presentata nella *blockchain* di Ethereum, in particolare era stato lanciato un fondo, chiamato "The DAO", che aveva raccolto circa 150 milioni di dollari in ETH, una cifra enorme nel 2016, tuttavia il codice dello *Smart contract* conteneva una vulnerabilità chiamata "*recursive call bug*" che hanno consentito un attacco alla *blockchain*, drenando circa 60 milioni di dollari. Al fine ripristinare lo *status quo ex ante* la frode, la *blockchain* di Ethereum ha subito un *hard fork* nel luglio del 2016, creando una nuova *blockchain* parallela, conosciuta oggi come Ethereum Classic (ETH).

Queste nuove tipologie di strutture basate sulla *blockchain*, sono caratterizzate da queste tipologie di meccanismi di sicurezza, che vanno sostanzialmente a rispondere al cosiddetto trilemma della *blockchain* o della scalabilità, ovvero il trade-off tre decentralizzazione, sicurezza e scalabilità, tutti aspetti comunque in contraddizione che devono necessariamente coesistere per mantenere un sistema efficiente e privo di intermediari tra i nodi della rete.

2.2 Smart Contract, Oracoli e *Non Fungible Tokens* (NFT)

Gli *smart contract* (*SC*) sono definiti come dei "protocolli digitali" che eseguono automaticamente i termini di un contratto, registrato sulla *blockchain*. Al pari di un normale accordo contrattuale infatti, anche gli *smart contract* hanno diversi obiettivi tra cui: soddisfare i termini definiti dalle parti come le condizioni di pagamento, minimizzare i rischi ed infine eliminare il ruolo di intermediari ed i tradizioni meccanismi di *enforcement*.

Questo concetto che oggi sembrerebbe assimilato indissolubilmente con la tecnologia *blockchain*, tuttavia non risulta così recente; il primo che ha definito questa tecnologia è stato Nick Szabo nel 1994[51], definendoli come: *"protocolli di transazione informatizzati, che eseguono i termini di un contratto"*. Più precisamente l'autore afferma che traducendo le clausole contrattuali in codice informatico, si possono evitare tutte quelle fattispecie spiacevoli che derivano dalla mancata loro esecuzione, riducendo al tempo stesso al minimo le interazioni con gli intermediari tra le parti del contratto.

Oggi il concetto di *smart contract* non risulta univoco, bensì questo termine presenta due tipi di identificazione, nello specifico infatti di può parlare di:

- *smart contract code:* che identifica una tecnologia specifica o un codice informatico che viene memorizzato, verificato ed eseguito su una *blockchain*.
- *smart legal contract:* per cui s'intende l'applicazione specifica di questa tecnologia come complemento o sostituto dei contratti giuridici tradizionali.

La caratteristica fondamentale degli SC è rappresentata dal fatto che le parti giungono alla formulazione di un accordo, adeguando le clausole contrattuali e le tempistiche di esecuzione delle stesse secondo la logica "*if-this-then-that*", ossia al verificarsi di un determinato

[51] N. Szabo, "*Smart Contracts: Building Blocks for Digital Markets*", Extropy Journal of Transhuman Thought, 16, 1996. Secondo Szabo: «A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises». «I call these new contracts "smart", because they are far more functional than their inanimate paper-based ancestors. No use of artificial intelligence is implied». «The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher»

presupposto stabilito dai contraenti (*this*), si verifica automaticamente un risultato stabilito nel codice del contratto digitale (*that*). Ciò che differenzia i contratti giuridici tradizionali rispetto agli *SC* su *blockchain permissionless* è appunto l'auto-esecuzione. Questo aspetto costituisce la caratteristica più rilevante di questo strumento; una volta registrati sulla *blockchain*, gli *smart contract* non possono più essere modificati, annullati o interrotti unilateralmente. Inoltre, l'anonimato garantito dal sistema rende impossibile identificare la controparte, rendendo di fatto inutile il ricorso a un'azione legale.

Numerosi studi si sono interrogati sulla legittimità della dottrina giuridica rispetto a questa nuova tecnologia[52], gli SC ribaltano infatti il ruolo tradizionale del diritto, che nello specifico corregge e completa l'intento delle parti anche in seguito all'esecuzione del contratto, indentificandosi soprattutto come uno strumento *ex post*. L'auto esecuzione degli SC non permette alcuna tipologia di protezione legale tradizionale, poiché la struttura della *blockchain*, che consente l'anonimato a tutti gli effetti non permette l'esistenza di uno strumento di rivalsa verso la controparte[53]. Ne consegue quindi che una limitazione rilevante per questa tecnologia risiede nella precisione e nella correttezza del codice, il quale una volta lanciato sulla *blockchain* non potrà più essere corretto o modificato. Gli eventuali errori o mancanze non potranno essere rettificate, a meno che non siano state predisposte *ex ante* determinate condizioni nel codice per l'interruzione anticipata del contratto. La mancanza di una rinegoziazione *ex post*, dovuta all'auto esecuzione del contratto, potrebbe suggerire una riduzione generale dei costi di transizione. Tuttavia, questi risparmi possono essere compensati da costi iniziali più elevati, soprattutto nel caso in cui l'oggetto del contratto riguarda strumenti finanziari complessi, la cui negoziazione deve essere definita nel dettaglio al fine di ridurre l'incertezza su ogni possibile eventualità. Nello specifico, i suddetti costi potrebbero aumentare ulteriormente qualora gli scenari futuri siano più incerti, dal momento che, in questo caso, si potrebbero dover immaginare numerosi e più complessi esiti futuri per la fattispecie. Questi costi aumentano nello specifico quando vi è grande incertezza sullo scenario futuro ed al tempo stesso nel caso in cui i possibili esiti in cui si può evolvere la fattispecie risultano particolarmente numerosi o difficili da immaginare. Viceversa le parti rinunciano alle protezioni contrattuali *ex post*, soltanto nel caso in cui hanno un'approfondita conoscenza della

[52] A. Wright, and P. De Filippi, "*Decentralized Blockchain Technology and the Rise of Lex Cryptographia*". Social Science Research Network, 34, 41-52; 2015.
K. Werbach, and N. Cornell, "*Contracts Ex Machina*", 67 Duke Law Journal, 2017.
[53] K. Werbach, "*Trust, but Verify: Why the Blockchain Needs the Law*." Berkeley Technology Law Journal, vol. 33, no. 2, 2018, pp. 487–550.

materia ad oggetto, e ripongono grande fiducia nella controparte, in questo modo possono prevedere tutti i possibili esiti della fattispecie contrattuale.

Gli studi di finanza comportamentale hanno evidenziato come molte persone che si approcciano ai mercati finanziari risultano particolarmente inesperte ed eccessivamente ottimisti in merito alla loro capacità di operare sui mercati[54]. Questo giudizio quindi li porta a sottoscrivere dei contratti complessi, per cui gli stessi non hanno piena conoscenza della materia e degli esiti indesiderati a cui il contratto può portare. Dunque viene meno la fattispecie già in precedenza menzionata, in aggiunta gli SC non consentono l'opportunità di annullare o eliminare gli effetti del contratto, esponendo ad un rischio ancora più elevato i soggetti finanziariamente meno esperti, ossia la clientela *retail*. Se gli stessi infatti fossero consapevoli dalla propria posizione, avendo una conoscenza finanziaria un po' più avanzata potrebbero decidere di non sottoscrivere tali accordi, oppure scegliendo di rivolgersi ad un intermediario a cui affidare la fattibilità del contratto. Tuttavia permane anche un altro problema, ossia come si può garantire che gli intermediari operino correttamente? La *blockchain* è infatti un'ambiente che per sua natura presenta i soggetti in modo anonimo, facendo si che la creazione di rapporti fiduciari risulti particolarmente complessa e difficoltosa.

In altri termini l'architettura degli SC, mette in crisi l'attuale quadro normativo sulla tutela dei soggetti risparmiatori nell'ambito finanziario, negli USA così come in tutti i Paesi occidentali, vi è un'ampia protezione degli individui rispetto alla mancanza di professionalità e di informazione. Ciononostante questa fattispecie legislativa non può essere applicata a questa tecnologia DeFi, la quale nel caso in cui dovesse diventare predominante rischia di escludere una parte degli investitori più piccoli dai mercati finanziari.

Il presente elaborato non ha come obiettivo quello di mettere in discussione la legittimità giuridica di questi nuovi strumenti tecnologici, ma si propone di offrire una panoramica descrittiva in merito alle eventuali problematiche relative al mondo empirico e nello specifico al contesto finanziario che interessa sia gli investitori istituzionali che *retail*.

Ora la discussione tratterà il tema degli oracoli ed il loro ruolo nel contesto della *blockchain* permissionless e degli SC.

Per poter eseguire automaticamente le transazioni dai differenti account tramite SC, si necessitano di informazioni, vale infatti il costrutto definito in precedenza, ovvero "*if this, then*

[54] D. Laibson, A. Repetto, J. Tobacman, "*Estimating Discount Functions with Consumption Choices over the Lifecycle*". Working Paper 13314, National Bureau of Economic Research, 2007.
J. Y. Campbell, "*Restoring rational choice: The challenge of consumer financial regulation*". American Economic Review, 106(5):1–30, 2016.

that", se vi è un determinato evento, piuttosto che una la determinazione di una condizione allora il contratto potrà essere eseguito.

L'integrazione dei dati *off-chain*, ovvero al di fuori del sistema della *blockchain*, avviene attraverso i cosiddetti oracoli, entità esterne alla *blockchain* che inseriscono i dati nello SC tramite una transazione *on-chain*, incorporando i dati esterni per il corretto funzionamento. Ciò significa quindi, che nonostante questa tecnologia cerchi di eliminare la dipendenza da terze parti, gli *smart contract* spesso devono accedere a dati esterni alla *blockchain* per interagire con il mondo reale, questa interazione avviene mediante il confronto con gli oracoli. Nello specifico gli oracoli hanno i compito di estrapolare, verificare ed autenticare le fonti esterne, trasmettendo poi le informazioni necessarie all'interno della *blockchain*. Si può facilmente intendere quindi che l'efficienza e la sicurezza di uno SC è subordinata soprattutto al corretto funzionamento dell'oracolo ad esso connesso, questo perché se i dati forniti dall'oracolo sono corrotti anche l'output dello SC lo sarà.

Per risolvere questa problematica, esistono due tipologie di oracoli[55], ossia quelli centralizzati e non centralizzati. Nel primo caso, gli oracoli centralizzati andranno ad interrogare, ovvero ad estrapolare i dati necessari per l'esecuzione dello SC direttamente da una singola fonte, come Coinbase, registrando in seguito il dato sulla *blockchain*. Questo meccanismo che risulta molto efficiente in termini di velocità non assicura tuttavia l'assenza di punti di vulnerabilità, in effetti il database potrebbe risultare corrotto, nello specifico potrebbe manipolare i dati per trarne vantaggio, oppure il dato potrebbe essere alternato durante la trasmissione verso la *blockchain*.

Un' alternativa a questa problematica sono gli oracoli decentralizzati, il cui funzionamento è il medesimo delle *blockchain* permissionless. Per minimizzare la fiducia nelle terze parti si fa affidamento alla validazione delle informazioni su più soggetti , i validatori mettono in garanzia i propri *token*, nel caso in cui i dati forniti risultano corretti si otterrà una commissione, viceversa ci sarà una perdita dello *stake* e l'esclusione futura dalla validazione. La vulnerabilità di questo processo, proprio come nel *PoS*, è relativa agli aspetti di collusione tra i differenti validatori, i nodi infatti possono mettersi d'accordo per generare un dato falso, se il guadagno è abbastanza alto da giustificare la perdita dello *stake*. Oltre a questa eventualità un attaccante può corrompere o creare nodi falsi per manipolare il risultato, e quindi definire l'esito desiderato per un determinato SC, per cui presenta particolari interessi economici[56]. Il concetto di validazione con gli oracoli assume una forma più complessa rispetto alla validazione delle

[55] A. Beniiche, "*A Study of Blockchain Oracles*" arXiv:2004.07140.

[56]G. Caldarelli, J. Ellul, "*The* Blockchain *Oracle Problem in Decentralized Finance* a *Multivocal Approach*" Applied Sciences, 11(16), 2021.

transazioni. In tal caso si tratta di informazioni, per cui non sempre esiste una "verità unica", ma solo valori approssimati. Al fine di ovviare a questo problema i validatori usano metodi come la media o la mediana tra le risposte per decidere il valore da considerare corretto o quantomeno univoco. Nonostante ciò, restano numerosi interrogativi: quale architettura tecnologica risulta più resistente ad attacchi distribuiti su più nodi? Quali meccanismi possono contrastare la collusione tra validatori? Inoltre, ci si chiede se un accesso libero alla validazione dei dati sia auspicabile, oppure se sia preferibile limitare il valore economico affidabile all'oracolo per ridurre i rischi.

Infine un *NFT* (*Non-Fungible Token*) è un dato univoco, registrato su una *blockchain* ed associabile ad un bene digitale o fisico, oppure a una licenza d'uso per uno scopo specifico ed andando oltre lo stesso può rappresentare azioni o altri titoli che definiscono il possesso di qualcosa. Essendo per sua natura un qualcosa di fungibile data la sua unicità e tracciabilità, un *NFT* si distingue dalle altre criptovalute, che invece sono fungibili e intercambiabili, ad esempio un *BTC* o un *ETH* non possono distinguersi in valore gli uni dagli altri essendo una cripto standardizzata. Pertanto gli *NFT* possono essere acquistati, venduti e scambiati ed inoltre sono spesso considerati una forma di arte digitale o collezionismo digitale. Per questa ragione possono essere molto rilevanti nel caso in cui si faccia riferimento a titoli di proprietà come accade con il caso delle azioni ed in particolare nell'ambito delle *ICO*, ovvero *Initial Coin Offer*.

Questo paragrafo ha voluto definite in modo macroscopico degli esempio di forza e debolezza in merito alle attuali tecnologie relative agli SC e oracoli, ovviamente trattandosi di nuove opportunità e frontiere tecniche si hanno oggi molti punti aperti in particolare sull'ambito della sicurezza, auto esecuzione, protezione finanziaria dei consumatori ed infine soluzione delle controversie e nullità delle clausole contrattuali. Questi aspetti infatti possono essere pregiudizievoli in particolare per l'uso comune e quindi per la diffusione di tali strumenti, tuttavia a causa della versatilità della tecnologia, l'autore ritiene che tali problematiche potranno sicuramente essere superate negli anni avvenire, mediante delle metodologie che subordineranno ancora di più la presenza dalla fiducia tra i nodi della rete.

2.3 Implementazione degli *smart contract* nei processi di quotazione

I paragrafi precedenti relativi alla tecnologia *blockchain* e agli *smart contract*, sono la base essenziale per comprendere l'idea innovativa che questo elaborato vuole proporre, ovvero risolvere i problemi di trasparenza ed efficienza allocativa nell'ambito delle offerte pubbliche iniziali.

L'idea di base di questo elaborato ricalca molto il concetto di *ICO*, ossia *Initial Coin Offering*, con delle differenze rilevanti in merito al processo di allocazione e al meccanismo di determinazione del prezzo, per i relativi *token* oggetto dell'offerta tramite l'uso di *smart contract*. L'introduzione degli *Smart contract* infatti, rappresenta una delle applicazioni più promettenti della tecnologia *blockchain* nell'ambito finanziario, rivelandosi estremamente utile ed efficiente nei processi di quotazione[57]. Il sistema finanziario attuale, così come il ruolo degli intermediari finanziari, potrebbe affrontare importanti cambiamenti, subendo sempre di più il processo di disintermediazione, avviato già lo scorso decennio mediante la tecnologia *Fintech*. I processi di *IPO,* attraverso il supporto della tecnologia *smart contract*, si evolveranno in modo più efficiente, con un risparmio di tempo e denaro per le imprese emittenti. Un esempio è dato dalla semplificazione della fase di allocazione dei titoli, ossia il *bookbuilding*, descritto nel primo capitolo. Grazie all'utilizzo degli *smart contract* infatti, si possono registrare le offerte degli investitori in tempo reale, ed evitare quindi di sostenere costi di *roadshow* e pertanto pagare elevate commissioni al sindacato di sottoscrizione[58]. Un'applicazione già esistente di questa tecnologia, usata per definire un'operazione di finanziamento, prende il nome di *ICO*, questa determinata operazione si configura sia per le imprese in *early stage*, che per le imprese mature, anche se in larga parte è stato usato da imprese relativamente giovani, molto legate al mondo *fintech*.

Un'*Initial Coin Offering* generalmente segue tre fasi, pianificazione strategica, prevendita (pre-*ICO*) e vendita vera e propria (*ICO*), cui segue infine una fase *post* emissione che prevede la quotazione e il *trading* secondario dei *token* su uno o più *exchange*[59].

Nella prima fase l'impresa deve definire in modo dettagliato il progetto di finanziamento, esplicitando la finalità della raccolta dei capitali, le tempistiche e la complessità dello *smart contract* da voler usare, piuttosto che scegliere la tipologia di *blockchain* o *token*[60]. Nello specifico, l'emittente deve determinare la struttura dell'operazione ed i diritti associati ai *token* che in seguito gli investitori andranno a scambiare in cambio di criptovalute, oppure di moneta fiat. In seguito, si definisce la metodologia per la determinazione dei prezzi, che nell'*ICO* risultano fissi, poiché decisi direttamente dall'emittente e successivamente si procede con la

[57] Catalini C. and Gans J. S., *Initial coin offerings and the value of crypto tokens*, National Bureau of Economic Research Working Paper 24418, March 2019.
[58] Nareg Essaghoolian, '*Initial Coin Offerings: Emerging Technology's Fundraising Innovation*', U.C.L.A. Law Review, 2019, pp. 294-343.
[59] Adhami S., Giudici G. and Martinazzi S., *'Why do businesses go crypto An empirical analysis of Initial Coin Offerings*', Journal of Economics and Business, 2018.
[60] Adhami S. and Giudici G., 'Initial Coin Offerings: Tokens as Innovative Financial Assets', in U. Hacioglu (ed.), *Blockchain* Economics and Financial Market Innovation, 2019, pp. 61-81.

pubblicazione del *white paper*, in genere sul sito web dell'impresa. Il *white paper* è un documento informativo dettagliato, che racchiude tutte le informazioni fondamentali sull'*ICO*, come: informazioni sull'emittente, sulla finalità dei fondi, sui protocolli informatici, e sulla *blockchain* pubblica adottata, nonché sul prezzo e sul meccanismo di distribuzione [61]. Solitamente al *white paper* viene allegato un *business plan*, per esplicitare meglio le prospettive finanziarie del progetto, in seguito viene identificato il pubblico *target* a cui rivolgere l'offerta e la strategia di comunicazione tramite campagne di *marketing* digitale. Inoltre, l'emittente può nominare dei comitati consultivi formati da esperti del settore, per esprimere pareri in merito alla fattibilità dell'offerta pubblica e sulla correttezza degli strumenti scelti per condurre l'operazione; di solito questi comitati sono remunerati direttamente tramite capitale o *token* della *blockchain* di riferimento[62].

Successivamente vi è la seconda fase, che prende il nome di prevendita o pre-*ICO*, dove l'emittente seleziona gli investitori istituzionali, ai quali proporre in anteprima l'offerta dei *token* ad un prezzo generalmente scontato. Questa fase è cruciale poiché permette all'impresa di raccogliere i capitali necessari per far fronte ai costi dell'*ICO*, e di testare la domanda di mercato, attirando maggiormente l'interesse di altri investitori[63]. Questa fase inoltre risulta essere più rapida rispetto alla precedente, poiché l'emittente offre la possibilità di sottoscrivere i token attraverso la valuta fiat, semplificando dunque il processo e riducendo maggiormente i costi di transazione per gli investitori.

In seguito vi è la vendita al pubblico dei *token*, chiamata anche *crowd sale*, questo è il momento in cui gli investitori inviano le criptovalute, di solito Ethereum, ad un portafoglio digitale pubblico (*digital wallet*), facente capo all'emittente. Una volta incassate le offerte degli investitori, a seconda della codifica, lo *smart contract* potrà distribuire i *token* immediatamente oppure a conclusione dell'*ICO*; la durata di questo processo dipende essenzialmente dalla domanda di *token*, e può protrarsi fino ad un mese. I *token* successivamente sono trasferiti nei portafogli degli investitori in base al tasso di cambio assegnato dall'emittente oppure rispetto alla quantità di Ethereum trasferiti, ossia in base al contributo. Conclusa la vendita iniziale, segue la fase conclusiva, che consiste nella quotazione del *token* associato all'emittente su uno o più *exchange* (borsa di criptovalute). Dopo la quotazione, i possessori dei *token* possono scambiarli sul mercato secondario, garantendo così la liquidità degli *asset* e consentendo una

[61] Huang W., Meoli M. and Vismara S., 'The geography of initial coin offerings', Small Business Economics, February 2019, pp. 77–102.
[62] Masiak C., Block J. H., Masiak T., Neuenkirch M. and Pielen K. N., 'Initial coin offerings (ICOs): market cycles and relationship with bitcoin and ether', Small Business Economics, 2020, pp. 1113-1130.
[63] Momtaz P. P., Initial Coin Offerings. PLOS ONE, October 2019.

valutazione trasparente e continua della società emittente. In questo modo i *token* si possono considerare come delle azioni e la loro quotazione definisce il valore della società emittente, proprio come in una normale borsa valori. Tuttavia, tale fase è caratterizzata da una significativa incertezza, poiché molti progetti *ICO* non riescono ad essere quotati oppure subiscono un rapido *delisting*, portando alla successiva perdita di valore e spesso alla conclusione del progetto. Uno studio evidenzia infatti che il 46% delle *ICO* lanciate nel 2017 fosse già fallita entro il 2018, sottolineando il rischio finanziario e operativo che accompagna questo modello di finanziamento[64]. Questo epilogo non stupisce affatto, il *white paper* infatti non presenta una coerenza strutturale tra le differenti *ICO*, ed inoltre anche la documentazione più completa non raggiunge il livello di dettaglio di un prospetto informativo, dovuto ad una mancanza di regolamentazione per la sua redazione. Un'ulteriore problematica è relativa all'euforia degli investitori ed al mancato controllo sul *management* dell'emittente; in altre parole l'implementazione di questa nuova tecnologia ha portato gli investitori a sottovalutare i rischi di mercato, determinando di conseguenza una cattiva allocazione del capitale, caratteristiche proprie di una bolla[65]. Questa problematica è stata poi accentuata da problemi di controllo degli investitori, perchè i *token*, al contrario delle azioni, molto spesso non includono il diritto di voto in merito alle scelte societarie e alla nomina degli amministratori[66].
Il modello di *ICO* tradizionale presenta infatti evidenti limiti sotto il profilo informativo e allocativo, derivanti principalmente dalla fissazione arbitraria del prezzo da parte degli emittenti, inoltre vi è una limitata trasparenza nei criteri di allocazione dei *token* e un'elevata esposizione a fenomeni speculativi ed asimmetrie informative per gli investitori *retail*.
Il presente elaborato quindi propone delle soluzioni innovative alle sopra menzionate problematiche, con l'obiettivo di rendere più efficiente e trasparente il processo di allocazione dei *token*. L'idea di base è quella di implementare un meccanismo di asta marginale decentralizzata all'interno dello *smart contract*, con l'obiettivo quindi di coniugare i vantaggi della tecnologia *blockchain* con l'efficienza di allocazione del mercato primario tradizionale. Contrariamente alle *ICO* descritte nel presente paragrafo, questo meccanismo permetterebbe di derivare il prezzo in base alla domanda degli investitori e non quindi sulla base di una scelta arbitraria imposta dall'emittente, tale procedura ricorda infatti l'allocazione dei titoli di Stato, nonché anche le disposizioni del mercato primario presenti in Giappone alla fine degli anni 90

[64] Momtaz P. P., op. cit.
[65] Zetzsche D. A., Buckley R. P., Arner D. W. and Föhr L. "*The ICO Gold Rush: It's a Scam It's a Bubble, It's a Super Challenge for Regulators*", European Banking Institute Working Paper series 18/2018.
[66] Kaal Wulf A., 'Initial Coin Offerings: the top 25 jurisdictions and their comparative regulatory responses', Stanford Journal of *Blockchain* Law and Policy, 2018.

(vd. cap. 1). Seguendo quindi la dottrina finanziaria su questi temi, l'efficienza in termini di allocazione e di raccolta di capitali potrebbe sortire un effetto molto positivo, consentendo quindi di ridurre il fenomeno dell'*underpricing* e quindi eliminando sensibilmente anche i casi di *winner's curse*. Gli investitori con questo sistema potranno decidere in modo totalmente autonomo il prezzo massimo a cui sono disposti a pagare i titoli, in questo caso i *token*, facendo emergere dalla domanda effettiva il prezzo marginale di equilibrio, ossia il prezzo più basso che consente di allocare integralmente l'offerta dei titoli. Questa procedura, testata anche in un ambiente sperimentale (vd. cap 3), può garantire migliori risultati in termini di trasparenza ed ottimizzazione dell'allocazione. Inoltre dal punto di vista economico, similmente alle aste marginali dei titoli di Stato, come accade per i *T-Notes* e *BTP*, consente di raccogliere maggiori finanziamenti rispetto ad un'asta con prezzo discriminatorio (asta competitiva)[67]. Rispetto ad una decisione arbitraria, in questo modo si otterrà maggiore trasparenza, infatti il codice dello *smart contract* è pubblico, e pertanto non ci possono essere dubbi sulle modalità di calcolo del prezzo marginale, che viene immediatamente mostrato in seguito alla ricezione ed invio delle offerte. L'impresa emittente che decide di avvalersi di questo meccanismo per la quotazione, ha un ulteriore vantaggio, infatti grazie alla capacità auto esecutiva degli SC, è possibile eliminare qualsivoglia intermediario finanziario, consentendo quindi un notevole risparmio sui costi di emissione, i quali ammontano in media intorno al 7% (vd. cap 1). I benefici quindi non si limitano soltanto alla maggiore *disclosure* verso il potenziale pubblico di investitori e all'efficienza allocativa, ma anche al risparmio dei costi di intermediazione. Oltre ai suddetti vantaggi, l'emittente che adotta questa tipologia di *ICO*, potrebbe riscontrare difficoltà dal punto di vista della programmazione informatica, è necessaria infatti particolare attenzione alla progettazione tecnica del meccanismo di allocazione e del *pricing*. La gestione del rischio informatico è quindi uno degli elementi cruciali per garantire l'integrità e l'affidabilità del processo di quotazione, ed in quanto tale potrebbe essere necessario avvalersi di un supporto esterno, ossia esternalizzare questa particolare attività verso altre imprese che operano esclusivamente nel settore informatico. Oltre a ciò, questa proposta potrebbe risolvere alcuni problemi relativi all'asimmetria informativa ed alla definizione del *white paper*. Le società emittenti infatti, potrebbero anche in questo caso appoggiarsi a *provider* esterni per standardizzare la documentazione delle *ICO* e mettere a disposizione una piattaforma libera. Questo strumento permetterebbe a tutti gli investitori di votare le decisioni delle assemblee e

[67] N. Fabra, G. Llobet, Auctions with Privately Known Capacities: Understanding Competition Among Renewables, *The Economic Journal*, Volume 133, Issue 651, April 2023, Pages 1106–1146.

quindi di impedire al *management* di assumere atteggiamenti scorretti, risolvendo così il problema tra *principal* ed *agent*. Queste tipologie di soluzioni sono già definite da molti *providers*, uno tra questi è Capitolis Inc., le cui piattaforme vengono già usate tra i differenti *primary brokers*, tra cui: BNP Paribas, HSBC, JPM, Citi, Standard Charter e Barclays, come parte essenziale dello scambio dei *deals* per le *clearing houses*, nello specifico per le attività di novazione.

Confronto e principali differenze tra ICO tradizionale e asta marginale decentralizzata:

Dimensione	ICO tradizionale	Asta marginale decentralizzata (proposta)
Determinazione del prezzo	Fissato *ex ante* dall'emittente	Calcolato dinamicamente in base alle offerte degli investitori
Formazione del prezzo	Unilaterale, non riflette la domanda	Basata su meccanismo concorrenziale → prezzo di equilibrio
Trasparenza del processo	Limitata: spesso opaca	Totale: *smart contract* pubblico e verificabile
Allocazione dei token	Proporzionale o *first-come-first-served*	Determinata automaticamente secondo priorità di offerta
Coinvolgimento degli investitori	Passivo: accettano un prezzo imposto	Attivo: inviano proposte con disponibilità a pagare
Efficienza allocativa	Bassa: rischio di *mispricing* e *over/under*-subscrizione	Alta: ottimizzazione della corrispondenza domanda-offerta
Intermediazione	Nessuna, ma con rischio di arbitrarietà	Nessuna, ma con regole codificate e auto eseguite
Rischi principali	Asimmetria informativa, manipolazione, *pump & dump*	Complessità tecnica, necessità di *auditing* del codice

Fonte: elaborazione propria

In conclusione, la proposta basata sull'asta marginale decentralizzata potrebbe rappresentare a livello teorico un passo evolutivo molto significativo rispetto alle *ICO* tradizionali, configurandosi come un potenziale *standard* per le future emissioni tokenizzate, in grado di integrare efficacemente automazione, trasparenza e logiche di mercato, rivelandosi inoltre uno strumento ancora più equo e comune tra gli investitori retail, che ad oggi hanno ancora molte barriere di entrata all'accesso al mercato primario.

2.4 Confronto tra i processi, vantaggi e svantaggi per il mercato

In seguito alla descrizione dell'idea centrale su cui si basa il presente elaborato, questo paragrafo ha l'obiettivo di approfondire in modo specifico le differenze tra il normale processo

di quotazione, mediante *IPO*, rispetto al meccanismo di *ICO* ad asta marginale illustrato in precedenza.

L'autore ritiene che la differenza più importante tra questi due processi di quotazione, risiede nella possibilità di estendere l'offerta ad un numero illimitato ed indiscriminato di investitori, ampliando di conseguenza la partecipazione degli investitori *retail*, i quali risultano esclusi nelle normali *IPO*. Difatti, le procedure tradizionali di *bookbuilding* e *roadshow*, coinvolgono prevalentemente investitori istituzionali selezionati dai sottoscrittori, lasciando ai margini del mercato gli investitori più piccoli e meno esperti che raramente partecipano direttamente ad operazioni di quotazione. Al contrario, l'adozione di piattaforme decentralizzate e basate su *smart contract* può avviare un processo di democratizzazione per i mercati primari, aumentando però al contempo le esigenze di trasparenza, chiarezza informativa e *compliance* regolamentare. In questo modo, tutti i potenziali investitori attratti tramite le campagne di *marketing* promosse dall'emittente, potranno collegarsi su una piattaforma come la già citata Capitolis, al fine di consultare il *white paper*/prospetto informativo e prendere così una decisione d'investimento ponderata. Nel caso in cui gli investitori istituzionali o *retail* dovessero partecipare, l'accesso sarebbe comunque garantito tramite l'automazione dello *smart contract*, avendo una maggiore sicurezza di non incorrere in fenomeni di *underpricing*, grazie all'individuazione di un prezzo marginale. In sostanza la decentralizzazione esclude ogni tipologia di barriera all'entrata per gli investitori, che in tale contesto si potranno differenziare solamente per quanto riguarda le quantità di *token* acquistate; si può intuire che gli investitori istituzionali avendo capitali più ingenti, potranno quindi acquistare maggiori *token*, ed avere di conseguenza un peso più rilevante nell'assetto societario. Quindi l'aspetto principale di questa soluzione è la possibilità di fornire un accesso diretto ai potenziali investitori *retail*, senza la necessità di ricorrere ad ulteriori intermediari che in precedenza hanno acquisito i titoli della società; di conseguenza si avrebbe un *level playing field* in termini di prezzo e quindi un notevole risparmio per gli investitori non professionali. Oltre ad un maggiore processo di democratizzazione, questa proposta innovativa presenta ulteriori vantaggi, come la maggiore trasparenza, in effetti lo SC risulta pubblico ed immutabile, consentendo ad ogni individuo di visionarlo autonomamente per capire la logica della transazione ed evitare le asimmetrie informative che sono presenti in un'offerta tradizionale. Al contrario, nel caso di un'IPO, non si conosce il sottostante oppure la logica di riferimento per la determinazione del prezzo, che viene inizialmente concordato tra emittente e sottoscrittori prima del *bookbuilding*. Un ulteriore vantaggio si ritrova nell'eliminazione della discrezionalità nell'allocazione dei titoli, nelle IPO infatti tutto ciò risulta altamente

pregiudizievole per tutte le categorie di investitori, i quali possono inizialmente prendere parte al *roadshow* e chiarire la quantità di titoli da acquistare. Tuttavia gli stessi non hanno la certezza di ricevere in seguito, il numero di titoli che avevano richiesto, compromettendo molto spesso delle strategie di allocazione di portafoglio, in favore della domanda più elevata di altri investitori sul mercato. Attraverso questa innovazione quindi, vi è un'allocazione dei *token* automatizzata e ottimale, secondo le preferenze espresse dagli investitori tramite il prezzo marginale, che si traduce nella prevenzione di fenomeni di sovra/sottoscrizione tipici delle *IPO* o *ICO* tradizionali[68], rendendo la procedura più equa per tutti gli investitori, sia retail che istituzionali. Inoltre i vantaggi non si limitano soltanto alla platea di investitori ma coinvolgono in special modo anche l'emittente, come affermato infatti nel capitolo 1, i costi di sottoscrizione possono essere molto elevati, senza considerare le perdite di opportunità in caso di *underpricing*, gli stessi possono raggiungere il 10% dell'intera emissione[69]. Dunque per una società emittente risulta più conveniente automatizzare il processo sia in termini temporali che soprattutto in termini di costi di commissione e di sottoscrizione; difatti prima dell'effettiva *IPO*, i sottoscrittori supportano l'impresa nella preparazione della documentazione al fine di ottemperare agli obblighi legislativi e di mercato. In questa nuova fattispecie, gli unici costi di intermediazione che sono necessari secondo l'autore per evitare danni economici e reputazionali, sono quelli relativi alla gestione delle piattaforme *on-chain* (es. Capitolis) e ancora di prevenzione e gestione dei rischi informatici. Le società emittenti difficilmente avrebbero le competenze per creare un codice relativo ad uno SC privo di errori, pertanto si ritiene che le stesse dovrebbero appunto esternalizzare questa attività, tuttavia una volta sostenuto questo costo, come accade nel caso dell'*IPO*, lo stesso codice potrebbe essere usato per definire offerte secondarie come aumenti di capitale o ancora *bought deals*.

Nonostante la presenza di molti vantaggi, questa proposta presenta comunque dei punti ancora aperti che potrebbero sottolineare delle debolezze caratterizzanti appunto le innovazioni finanziarie che utilizzano la tecnologia *fintech*. Come accennato in precedenza, le imprese emittenti dovrebbero quotarsi tramite *ICO*, solitamente non hanno una competenza specifica per creare uno *smart contract*, dovranno difatti esternalizzare questa attività, incrementando i costi rispetto al processo senza intermediari. Tra gli altri svantaggi vi sono i rischi derivanti dalla vulnerabilità del codice informatico alla base dello SC, infatti un errore al suo interno

[68] Cornelli, F., Goldreich, D., "*Bookbuilding: How Informative is the Order Book?*", Journal of Finance 58(4), 1415-1443, 2003.
Loughran, T., & Ritter, J., *Why has IPO underpricing changed over time?* Financial Management, 33(3), 5-37, 2004.
[69] R.S. Barden, J.E. Copeland, J.R. Hermanson, e R.H.L. Wat, op. cit.

comporterebbe ingenti perdite per gli investitori data la natura irreversibile della *blockchain*. Un ulteriore punto di debolezza si può anche riscontrare nell'implementazione degli oracoli, come descritto in precedenza, gli oracoli sono il tramite tra la blockchain ed il mondo empirico (*off-chain*), se l'informazione fornita da questi ultimi dovesse risultare errata oppure compromessa, l'effetto si ripercuoterebbe di conseguenza sullo SC, sottolineandone la vulnerabilità e di conseguenza vanificando l'intera emissione di *token*. Data la natura molto democratica di queste emissioni, potrebbe poi sorgere un'ulteriore problematica relativa alla stabilizzazione dei prezzi dei *token*, essendoci infatti un'ingente partecipazione di investitori retail, questi a differenza degli investitori istituzionali, potrebbero decidere di liquidare il proprio investimento in breve tempo, provocando di conseguenza una forte volatilità nei prezzi del *token*. Quest'ultima problematica potrebbe tuttavia risolversi mediante l'introduzione di clausole di *lock up*, al fine di evitare questi fenomeni di forte volatilità sul mercato, ciò non toglie che la presenza di un intermediario fisico potrebbe risolvere tale problema, creando dei report in seguito alla quotazione oppure agendo da *market maker* al fine di stabilizzare il prezzo. Infine un altro rischio in merito a questa nuova tipologia di emissione riguarda principalmente l'incertezza normativa, in Italia non esiste ancora un regolamento che definisce in modo chiaro le offerte pubbliche di token attraverso la *blockchain*, ciò quindi potrebbe comportare incertezza da parte degli investitori, il che implicherebbe almeno nel breve periodo una bassa partecipazione di investitori istituzionali i quali sono obbligati a rispettare determinati limiti di rischio per gli investimenti, ovviamente al fine di tutelare il risparmio pubblico[70]. La mancanza di un'adeguata regolamentazione potrebbe poi affermare ulteriori costi di *compliance* per l'impresa emittente che si troverebbe in questo senso in una posizione di svantaggio rispetto alle normali procedure di IPO.

[70]Si veda ad esempio la regolamentazione inerente al Dodd-Frank Act, così come tutte le norme costituzionali e la Mifid in Italia ed UE.

2.5 Quadro normativo attuale: focus sulla trasparenza ed antiriciclaggio

Questo paragrafo ha l'obiettivo di definire almeno in grandi linee lo stato normativo e giuridico attuale, che definisce e regola queste nuove tecnologie, descritte nei precedenti paragrafi. Gli SC sono stati definiti come dei "protocolli digitali" che eseguono automaticamente i termini di un contratto su *blockchain*. Il legislatore italiano ha definito di queste innovazioni mediante il Decreto Legge No. 135/2018, noto anche come Decreto Semplificazioni, nello specifico definisce gli *smart contracts* come "*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*". In questa definizione per registri distribuiti si intende appunto la *blockchain* e la tecnologia sottostante ad essa, definendoli meglio nell'Art. 8 del medesimo DL come: "*le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*". Tutto ciò può sembrare estremamente complicato se non anche confuso, tuttavia è bene precisare che trattandosi di un ambito estremamente innovativo, il legislatore italiano al pari di altri Paesi, non ha attualmente approvato alcun regolamento per queste nuove tecnologie, proprio per evitare un risultato controproducente e quindi frenare lo sviluppo e l'implementazione delle stesse in altri campi in cui sarebbero cruciali. Tuttavia questa assenza di regolamenti non implica necessariamente una mancanza delle istituzioni, bensì in questo momento le autorità si limitano a vigilare ed in generale a supervisionare gli sviluppi e le applicazioni delle tecnologie *DeFi*, principalmente per comprendere come intervenire ed in seguito regolare questa fattispecie. Questo intento si ravvisa anche tra gli obiettivi della *European Securities and Market Authority* (*ESMA*), affermando che l'introduzione di un regolamento europeo su in questi ambiti avrebbe come unico risultato quello di rallentare le applicazioni e lo sviluppo. Non si può negare infatti come questo campo rappresenti una vera e propria sfida per il contesto normativo e per la dottrina giuridica, principalmente poiché ad oggi si fa ancora fatica ad inquadrare questa fattispecie alle norme preesistenti. Fino al decennio scorso infatti, queste innovazioni avevano un'applicazione marginale in pochi ambiti, e solo in questi ultimi anni, le stesse sono diventate cruciali per l'economia ed in generale nel settore dell'*asset management*.

Ai fini dell'elaborato, l'autore ritiene che per lo sviluppo e l'implementazione di queste innovazioni nei contesti più importanti, e per far si che le stesse possono contribuire alla

risoluzione delle problematiche attuali nel contesto delle offerte pubbliche, bisognerebbe concentrarsi su due ambiti ovvero la tutela della trasparenza delle operazioni finanziarie e scongiurare le pratiche di antiriciclaggio. Si è visto infatti che la *blockchain* consente di avere un completo anonimato attraverso la crittografia dei blocchi e gli *harsh* che indentificano la transazione. Questo potrebbe essere un problema per quanto concerne l'identificazione e la legittimità dei fondi che vengono investiti nelle operazioni finanziarie, tuttavia se è vero che le informazioni non appaiano in chiaro è vero che esistono delle tecniche avanzate per risalire al dato reale anche nelle *blockchain permissionless*. Oggigiorno sono presenti delle forme più evolute ed efficienti di *blockchain analytics*[71], ossia una serie di tecniche informatiche ed elaborazione di dati che vengono utilizzate per ricercare ed indagare su attività illecite che si celano dietro indirizzi apparentemente anonimi, tra queste attività la più comune è il riciclaggio di denaro sporco[72]. A livello europeo sono stati fatti molti passi avanti in questo senso soprattutto per scongiurare queste eventualità e quindi giustificare delle attività illecite dietro una semplice operazione finanziaria. In primo luogo l'UE ha approvato alla fine del 2023 il regolamento *MiCA*, ossia *Markets in Crypto-Assets*, che definisce delle linee guida per la creazione del *white paper*, inoltre le norme riguardano il funzionamento, l'organizzazione e la governance degli emittenti e dei prestatori di servizi per le cripto attività[73], così come anche l'autorizzazione e la vigilanza dei prestatori di servizi e degli emittenti di *token*. In altre parole, impone agli emittenti di produrre e divulgare un *white paper* dettagliato che includa, tra l'altro, informazioni chiare sull'emittente, descrizioni precise del progetto imprenditoriale, caratteristiche tecniche della *blockchain* adottata, dettagli sulla fornitura e distribuzione dei *token*, criteri di determinazione del prezzo e analisi completa dei rischi associati. L'obiettivo è mitigare le asimmetrie informative e garantire agli investitori una base informativa uniforme, chiara e verificabile prima di procedere alla sottoscrizione[74].

Parallelamente oltre ai regolamenti che definiscono una maggiore trasparenza, la commissione europea ha approntato dei miglioramenti legislativi anche in materia di antiriciclaggio, mediante la direttiva 843/2018, anche chiamata *Anti-money Laundry Directive Fifith* (*AMLD5*), in seguito ampliata e rafforzata nel 2021 con l'approvazione della *AMLD6.* Nello specifico queste normative non si rivolgono principalmente agli emittenti di servizi finanziari digitali, come accade nella *MiCA*, ma questi vengono espressamente distinti rispetto agli emittenti

[71] Alcune aziende, come Coinalytics, Coinometrics o Elliptic ne hanno fatto una fonte di business. V. P. *DeFilippi*, The interplay between decentralization and privacy: the case of *blockchain technologies*.
[72] S. Capaccioli, Criptovalute e bitcoin: un'analisi giuridica: volume 4, Giuffrè Editore, 2015.
[73] https://eur-lex.europa.eu/IT/legal-content/summary/european-crypto-assets-regulation-mica.html.
[74] https://www.bancaditalia.it/media/approfondimenti/2024/micar/index.html.

tradizionali, per cui la direttiva dedica uno spazio a parte. Le principali novità consistono in requisiti rigorosi per i fornitori di servizi finanziari digitali, comprese le piattaforme *blockchain* che facilitano ICO o offerte analoghe, imponendo agli operatori obblighi stringenti relativi alle procedure *Know Your Customer* (*KYC*). Le procedure di *KYC* in particolare prevedono: l'identificazione puntuale e accurata dei clienti, la verifica dell'origine dei fondi investiti e la valutazione continua del rischio di riciclaggio associato alle transazioni, subordinando quindi la riuscita delle operazioni finanziarie ad un costante monitoraggio e ove necessario, segnalare tempestivamente eventuali attività sospette alle autorità competenti.

L'autore considera tuttavia che l'applicazione di queste norme alle piattaforme decentralizzate introduce notevoli complessità operative soprattutto nel caso in cui si vada a prendere in considerazione un'emissione primaria, a causa di differenti ragioni. In primo luogo, la natura decentralizzata dei processi basati su *blockchain* può rendere più difficoltosa l'implementazione efficace delle procedure *KYC*. Inoltre, l'adozione di *smart contract* implica un elevato livello di automazione, che potrebbe entrare in conflitto con la necessità di verifiche manuali approfondite e costanti. Di conseguenza, le imprese che intendano adottare modelli di emissione decentralizzati dovranno sviluppare soluzioni tecniche innovative e metodologie di compliance adeguati a soddisfare pienamente i requisiti normativi vigenti. In questa sede si ritiene infatti che l'unica soluzione possibile sia adeguare le pratiche di trasparenza e di *KYC* alla piattaforma in precedenza citata come Capitolis, infatti le imprese emittenti potrebbero permettere ai potenziali investitori di registrarsi, e quindi consentire agli stessi di caricare tutte le informazioni rilevanti al fine di scongiurare eventuali illegalità, ed elaborare tutte la documentazione relativa al *KYC*. Solo in seguito all'accertamento di queste informazioni si potrebbe accedere all'asta e quindi all'offerta vera e propria, trasformando quindi la *blockchain* da *permissionless* in *permissioned*, in alternativa si potrebbe sempre esternalizzare l'operazione di verifica e controllo degli investitori ad un intermediario finanziario con maggiore esperienza.

In conclusione questo panorama normativo e le soluzioni che perdono in considerazione la tecnologia *blockchain*, allo stato attuale non permettono una completa disintermediazione, ma al massimo la creazione di modelli ibridi all'interno dei quali le banche così come altri intermediari finanziari potrebbero comunque avere un peso rilevante per lo svolgimento delle operazioni di quotazione, dunque l'autore ritiene che tali tecnologie non decretano una fine del modello di *business* di queste realtà, ma piuttosto un cambiamento dello stesso e una integrazione con le nuove necessità ed innovazioni.

Capitolo Terzo

Simulazione di offerta pubblica iniziale tramite Algorand

Il presente capitolo vuole definire l'idea centrale dell'elaborato dal punto di vista strettamente computazionale e tecnico, al suo interno verranno infatti illustrati i procedimenti relativi alla creazione pratica di uno *smart contract* che segue la logica di allocazione mediante asta marginale. In particolare si è ritenuto necessario allegare e spiegare in modo generale le parti fondamentali del codice informatico che costituisce il contratto con il quale si rende possibile il pricing e l'allocazione dei *token*. Mentre nella prima parte verranno chiariti alcuni aspetti come la scelta della *blockchain* Algorand e l'implementazione pratica di questo contratto in ambiente di *test*.

3.1 Criteri e motivazioni per l'implementazione di Algorand

Per poter sostenere le ipotesi iniziali riguardo l'utilizzo dei sistemi decentralizzati all'interno delle operazioni di IPO, sono state vagliate differenti alternative in termini di *blockchain*. La scelta iniziale si focalizzava sull'implementazione della *blockchain* di *Ethereum*, progettata per gli *smart contract* e molto più semplice da usare a causa della vasta letteratura *open source* che la caratterizza[75]. Tuttavia questa scelta poteva comportare differenti problemi, sia sul piano dei costi di transazione che sui tempi di latenza, nello specifico questi diventano maggiormente evidenti quando la *blockchain* presenta molti utenti attivi nel medesimo momento, una situazione che in una normale ICO si riscontra con grande frequenza. A causa di queste problematiche si è ritenuto opportuno realizzare il protocollo d'asta marginale decentralizzato sulla blockchain di Algorand, ovviamente meno conosciuta di Ethereum, ma perfettamente strutturata per le esigenze di questo elaborato e ideale per testare lo *script* in modo sicuro. Algorand è stata inizialmente sviluppata per affrontare alcune delle sfide chiave associate alle *blockchain* tradizionali, come la scalabilità, la sicurezza, e il consenso decentralizzato, riuscendo in una certo senso a coniugare questi tre aspetti e quindi superare il trilemma della *blockchain*[76], questa si presenta infatti come una soluzione particolarmente adatta per le operazioni finanziarie più complesse come le IPO[77]. Inoltre Algorand è una *blockchain* indipendente, rientra infatti nella categoria di *layer*-1[78], in altre parole non necessita di

[75] A. Collomb, P. De Filippi, "*From IPOs to ICOs: The Impact of Blockchain Technology on Financial Regulation*", Blockchain Perspectives Joint Research Initiative, BNP Paribas, 2019.
[76] S. Micali, "*Algorand: A Secure And Efficient Distributed Ledger*", Theoretical Computer Science. Volume in Memory of Maurice Nivat, pp. 155-183. July 2019.
[77] T. Halevi *et al*., "*Initial Public Offering (IPO) on Permissioned Blockchain Using Secure Multiparty Computation*," IBM Research, Brooklyn College, 2019.
[78] https://algorandtechnologies.com/news/fungible-tokens-and-atomic-multi-party-transfers.

appoggio su altre *blockchain* per il suo funzionamento piuttosto che per la sicurezza, infatti le sue transazioni, criptovalute e applicazioni decentralizzate vengono supportate in modo autonomo. Quest'ultima similmente ad *Ethereum* si basa sul meccanismo di consenso *Pure Proof of Stake*, il che quindi consente di avere un'elevata decentralizzazione che aumenta la sicurezza del registro salvaguardandola da attacchi esterni[79]. Inoltre il meccanismo *Pure Proof of Stake* permette di avere un alto *throughput*[80], ossia rende possibile elaborare e trasmettere una grande quantità di dati in un tempo molto breve, il che è fondamentale nel caso in cui bisogna gestire un'asta marginale con numerosi partecipanti, soprattutto nel momento in cui gli stessi inoltrano molte offerte con prezzi differenti. Un' ulteriore caratteristica di Algorand è la finalizzazione immediata delle transazioni, ciò implica che una volta registrate, le transazioni non possono più essere modificate o cancellate, garantendo *disclosure* e sicurezza, da momento che le transazioni risultano pubbliche. Oltre a queste misure in termini di sicurezza, Algorand permette di aumentare la trasparenza mediante gli ASA, ovvero *Algorand Standard Assets*, dei *token* ai quali possono essere associati restrizioni o regole di *compliance* come il *whitelisting* degli investitori per conformarsi alle normative KYC e AML[81].

Un altro aspetto da non sottovalutare è la sostenibilità ambientale, con Ethereum i costi di emissione risultano essere particolarmente gravosi, soprattutto nel caso in cui come detto in precedenza vi sono molti utenti associati alla *blockchain*, i tempi di esecuzione si dilatano notevolmente e ciò causa inevitabilmente un maggiore rischio per gli investitori. Al contrario le emissioni di CO_2 di Algorand risultano bassissime fino a registrare delle gas *fee* inferiori al centesimo di dollaro, rendendola difatti l'unica *blockchain* ad oggi *carbon negative*, ossia assorbe più carbonio rispetto a quanto ne emette[82], questo protocollo assegna automaticamente una parte di ogni commissione di transazione per compensare le emissioni di carbonio.

Oltre ad Ethereum altre *blockchain* equivalenti sono Hyperledger Fabric e Solana, tuttavia seppur Hyperledger offre più controllo e riservatezza, Algorand offre il vantaggio di essere una *blockchain* pubblica**,** *permissionless* e allo stesso tempo sicura e scalabile, con possibilità di integrazione di funzionalità *permissioned* tramite *ASA*. Solana invece offre alte prestazioni, simili ad Algorand in termini di *throughput* e velocità, tuttavia, il suo *design* risulta essere meno

[79] Y. Gilad, R. Hemo, S. Micali et al. "*Algorand: Scaling Byzantine Agreements for Cryptocurrencies*", Massachusetts Institute of Technology CSAIL, Cambridge 2017.

[80] "F. Raimondi, "*Blockchain: un'analisi comparativa dei diversi protocolli*", Politecnico di Torino, 2022.

[81] Queste misure sono state già citate nel capitolo secondo, in particolare si suggeriva di implementare un ulteriore controllo delle misure di Anti money Laundry e Know Your Customer direttamente attraverso la piattaforma Capitolis, che potenzialmente potrebbe essere sfruttata dagli investitori come accesso all'asta dei *token*.

[82] https://climatetrade.com/algorand-partners-with-climatetrade-to-be-the-greenest-blockchain-with-a-carbon-negative-network/

robusto e questo sicuramente è uno svantaggio soprattutto in un ambito come quello finanziario [83] dove potenzialmente possono essere scambiati decine di milioni di *USD* al secondo, compromettendo la fiducia degli investitori.

In conclusione Algorand tenta di avvicinarsi alla risoluzione del trilemma della *blockchain*, che si propone di coniugare: decentralizzazione, sicurezza, e scalabilità, infatti questi tre aspetti vengono garantiti da differenti peculiarità. Primo fra tutti il *Pure Proof of Work*, che assicura la decentralizzazione randomizzando la validazione delle transazioni tra i differenti utenti mediante una funzione casuale verificabile (VRM)[84], influenzando anche la sicurezza che viene inoltre garantita dal rispetto delle normative KYC e AML. Infine l'architettura del registro si presenta molto solida tale da permettere la partecipazione di un grande numero di utenti senza compromettere la scalabilità del registro. Tuttavia ci sono alcuni aspetti che possono creare delle problematiche, questi derivano dalla decisione di eliminare gli *stake* in garanzia per la validazione delle transazioni e quindi la penalizzazione per i nodi malevoli. Questo ha permesso di ampliare la partecipazione al protocollo di consenso a molti più nodi, aumentando la sua decentralizzazione e anche scalabilità. Inoltre un altro aspetto che può costituire punti di forza o di debolezza è il particolare linguaggio che caratterizza il protocollo, ossia TEAL, ancora poco diffuso ai più, infatti se da un lato questo aspetto non consente di ritrovare facilmente i *bug* come nel caso di altre *blockchain*, lo scarso numero di *coder* non consente di poter effettuare immediate migliorie che potrebbero contribuire ad efficientare il protocollo.

Di seguito si riporta una figura che definisce Algorand rispetto al trilemma della *blockchain*[85]:

[83] J. Overdahl, Craig M. Lewis, "*Solana and the SOL Market*", Vanderbilt Univeristy, feb. 2025.

[84] "Verifiable Random Function": una funzione che raggruppa in ingresso dei dati e definisce un output pseudocasuale, con in aggiunta una prova che chiunque può utilizzare per verificare il risultato prodotto.

[85] In questo caso il triangolo nero in grassetto rappresenta le caratteristiche di Algorand allo stato attuale, mentre l'ultimo triangolo grigio esterno è la situazione di perfetto bilanciamento dei tre aspetti, che consente di superare il trilemma della *blockchain*, si può notare che il protocollo in questo momento si avvicina molto alla soglia esterna, prediligendo tuttavia ancora la scalabilità e la sicurezza a discapito della decentralizzazione.
Fonte immagine: F. Raimondi, Op. cit.

3.2 Test di verifica e costruzione dell'ambiente di controllo

Al fine di procedere con la costruzione dello *smart contract* vero e proprio, inizialmente si è ritenuto opportuno optare per l'ambiente di riferimento migliore in base alle caratteristiche dell'*output* desiderato, in questo caso vi erano differenti alternative, ovvero una rete locale chiamata Algorand Sandbox e una pubblica chiamata TestNet Algorand. La scelta alla fine è ricaduta sulla prima, ovvero sulla rete locale, realizzata appositamente per la fase di prova, evitando conseguenze che potrebbero modificare la *blockchain*. Una volta scelto l'ambiente di riferimento dove testare lo *smart contract* e osservare il corretto funzionamento, si è proceduto ad installare Sandbox clonando il *repository* GitHub ufficiale, ovvero lo spazio *online* dove gli sviluppatori di Algorand pubblicano il codice sorgente ufficiale, la documentazione ed i materiali di sviluppo del protocollo. Per poter usare Algorand Sandbox, si è rivelato necessario utilizzare un terminale, nello specifico la rete locale deve essere installata su un *container* Docker, pertanto una volta scaricata l'applicazione si è proceduto ad installare il tutto.
Da questo momento in poi si ritiene opportuno riportare i codici informatici usati nel terminale, come specificato in precedenza il linguaggio di programmazione usato su Algorand è TEAL :

```
git clone https://github.com/algorand/sandbox.git
cd sandbox
```

una volta clonato il *repository*, si procede ad avviare Algorand *sandbox* con il comando: questo comando crea un'istanza di Algorand che permette quindi di accede alla *blockchain* in formato appunto locale, in questo modo si potrà procedere alla simulazione ed ai test in modo sicuro ma comunque mantenendo le funzionalità essenziali del protocollo.

```
./sandbox up
```

Dopo aver avviato il protocollo era necessario creare degli *account* fittizi che potessero prendere parte all'asta vera e propria, nella quale gli investitori fittizi potevano contendersi i *token* messi a disposizione e quindi inoltrare le proprie offerte, che in seguito sarebbero state considerate per calcolare il prezzo marginale. Essendo una dimostrazione puramente accademica, si è ritenuto opportuno creare non più di 50 *account*, è normale che in una vera *IPO* il numero sarebbe stato molto più considerevole, potenzialmente migliaia nel caso di investitori istituzionali e *retail*, questa scelta non è avvenuta in modo casuale, creare più di 50 *account* avrebbe comportato uno sforzo ancora più elevato in termini di codice e risorse informatiche. Tuttavia si è ritenuto che con questo numero si potesse osservare innanzitutto la definizione di un prezzo marginale ed in secondo luogo anche la competizione degli investitori, così come le dinamiche di *oversubscription* (domanda superiore rispetto all'offerta). Anche dal

punto di vista statistico-inferenziale il numero risulta sufficiente per rispettare i fondamenti del teorema del limite centrale, il quale afferma che con grandi campioni di popolazione, la distribuzione della media dei campioni tende ad approssimarsi verso una normale, e questo fenomeno si può riscontrare a partire da 30 osservazioni[86].

In codice TEAL si può procedere in due modi, il primo più veloce, ma richiede il codice identificativo dell'applicazione lanciata su *Sandbox*, il secondo crea degli *account* in modo casuale senza la necessità di creare un'applicazione specifica per le transazioni.

Primo metodo:

```
# Parametri base
CREATOR="5SPCXRA3VGXXGWBSNZNZYGBK7FROU4HJESQBSTKYVCPFAS3RHLHVXYTF7E"
APP_ID=1099
NUM_PARTICIPANTS=50
```

Secondo metodo:

```
goal account new
```

Come si può intuire per creare molteplici account si necessita una ripetizione continua del codice sopra riportato, pertanto si è convenuto usare il primo metodo per velocizzare la procedura.

Dopo aver creato gli account necessari per i test di riferimento, si potranno osservare i loro codici identificativi e i fondi a disposizione che verranno definiti di *default* dal sistema, il comando sarà quindi il seguente:

```
goal account list
```

Per quanto riguarda l'*output*, si riporta un esempio di tre *account*:

```
[offline]DIAJLQEGCBY33ZZBNROWQAKWV3IJ3C7QSEU5LGKQFXHMBXUJRHZEW7JPVI
1000000000000000 microAlgos
[offline] DVOO36LOHBBB2GK2B7RSFK7RH6XZJ6IHIQTKOGFJTY4XB3MKFGOEZ7GOOA      0
microAlgos
[offline] DV5LXQBXKMYF4JDLMQAVYWG6OFUBJEUTLM22GSP3Q2ENTEQ52YMM3PKBMY      0
microAlgos
```

[86] A. Monti, "*Introduzione alla statistica*", Edizioni Scientifiche Italiane Seconda Edizione, 2008.

Come si può notare alcuni account presentano 0 ALGO, ovvero la criptovaluta di riferimento per la *blockchain* di Algorand quindi per ovviare a questa problematica si può trasferire una parte di ALGO dall'*account* principale verso gli altri *account* creati per la simulazione. Ovviamente in un contesto reale questo non accadrebbe poiché si ipotizza che ogni investitore abbia già convertito i propri fondi in valuta fiat nella criptovaluta di riferimento del protocollo, tuttavia il comando usato in questo caso sarà:

```
goal clerk send --amount 1000000 --from [indirizzo_central_fund] --to
[indirizzo_account_investitore]
```

Questo è un comando generico, con una somma anch'essa generica, proprio per chiarire nel modo più semplice possibile come avviene l'operazione.
Il prossimo passo è la creazione dei *token* ASA che fondamentalmente rappresentano le azioni di nuova emissione, il comando in questione indica l'impresa emittente, ossia il *creator*, il nome ed il numero totale dei *token* emessi nell'ICO , un ulteriore parametro è l'*asseturl*, ovvero un sito *online* che definisce in modo esaustivo e dettagliato maggiori informazioni sulle caratteristiche del *token*. In questo caso la piattaforma Capitolis (vd. cap.2), potrebbe essere di fondamentale importanza, poiché gli investitori possono esaminare tutte le caratteristiche dell'emissione mediante il *whitepaper* ed inoltre andare a depositare direttamente i fondi necessari per l'acquisto dei *token* in questo modo si può quindi affermare l'intero processo di allocazione, direttamente attraverso la piattaforma *online*.
il comando sarà appunto il seguente:

```
goal asset create --creator [indirizzo_azienda_emittente] \
  --total 1000000 \
  --unitname IPOTOKEN \
  --decimals 0 \
  --defaultfrozen false \
  --note "Token azionari IPO" \
  --asseturl https://esempio.com
```

In seguito alla creazione dell'ambiente di *test* e quindi dei differenti account su *sandbox*, si è ritenuto opportuno prendere in considerazione l'idea di creare uno *smart contract* totalmente nuovo, che potesse implementare l'idea centrale dell'elaborato, ovvero un meccanismo ad asta marginale per il *pricing* dell'ICO e che potesse garantire inoltre la distribuzione dei *token* verso gli investitori che hanno partecipato effettivamente all'asta sulla piattaforma di Capitolis. Come accennato anche in precedenza Algorand sfrutta un linguaggio di programmazione

chiamato TEAL, ossia *Transaction Execution Approval Language*, che in effetti presenta non poche difficoltà per coloro che si apprestano ad usarlo per la prima volta. Tuttavia attraverso differenti *test* e modificando il contratto per adattarlo alle specifiche desiderate, alla fine lo *smart contract* realizzato rappresenta un'implementazione completa e robusta di un sistema d'asta su *blockchain* Algorand. Questo infatti incorpora tutte le fasi essenziali di un'ICO, dalla raccolta delle offerte alla distribuzione dei *token*, con meccanismi di sicurezza e controllo appropriati. Ovviamente trattandosi di un esperimento accademico il contratto in questione non si può adattare a tutte le esigenze di un'impresa emittente che voglia cimentarsi in questo processo, tuttavia questo potrebbe rappresentare una base di partenza significativa per costituire lo sviluppo di un'ICO, il design modulare facilita infatti la comprensione del codice e consente eventuali estensioni future, come l'implementazione di algoritmi più sofisticati per il calcolo del prezzo marginale o l'aggiunta di funzionalità come l'estensione automatica del termine dell'asta. Per quanto concerne poi la sicurezza all'interno dello *smart contract* si fa riferimento in particolare ai processi di determinazione dell'offerta e in seguito alla riscossione dei *token*, si è volutamente tralasciata la parte che riguarda l'AML e KYC. In effetti trattandosi di argomenti molto complessi e relativi ad una disciplina in forte cambiamento si è ritenuto opportuno tralasciare l'implementazione di questi controlli, esternalizzandoli appunto in Capitolis, ossia la piattaforma che ospiterà l'interfaccia dell'ICO, dove è presente l'intera documentazione relativa agli investitori. D'altra parte è vero che Algorand implementa tutte queste funzionalità sulla propria *blockchain* e sui *token* ASA, tuttavia per definire al meglio questi aspetti di *compliance* si necessita di casi reali e di investitori con uno storico veritiero. Se infatti si dovessero effettuare delle simulazioni accademiche, con investitori casuali, l'unico risultato sarebbe essenzialmente distorto e poco applicabile ad un contesto reale, dove nella maggior parte dei casi vi sono investitori istituzionali e *retail*, con obiettivi e profili differenti.

3.3 Costruzione dello Smart Contract su Algorand

L'argomentazione in questo paragrafo si sposterà sulla descrizione approfondita dello *smart contract* e sulle sezioni in cui lo stesso è diviso, queste corrispondono alle diverse funzioni e controlli appositamente creati per strutturare l'intero processo.

Sistema di Routing e Architettura di Controllo:

```
txn ApplicationID
int 0
= =
bnz handle_creation
```

La parte iniziale rappresenta il punto di ingresso del contratto, infatti quando una transazione viene inviata all'applicazione, quest'ultimo verifica innanzitutto se si tratta della fase di creazione iniziale, nello specifico:

- txn ApplicationID: Accede all'ID dell'applicazione nella transazione corrente
- int 0: Carica il valore 0 nello stack
- = =: Confronta i due valori in cima allo stack (ApplicationID e 0)
- bnz handle_creation: Se il risultato è vero (ApplicationID = 0), salta alla sezione handle_creation

Questo meccanismo è fondamentale perché la prima chiamata a un'applicazione Algorand ha un ApplicationID di 0, indicando che è la transazione di creazione.

```
txn OnCompletion
int NoOp
= =
bnz route_noop_operations
txn OnCompletion
int DeleteApplication
= =
bnz handle_delete
```

Dopo aver verificato che non si tratta della fase di creazione, il contratto esamina il campo OnCompletion della transazione:

- txn OnCompletion: Recupera il valore OnCompletion dalla transazione
- int NoOp: Carica il valore che rappresenta "nessuna operazione"
- = =: Confronta i due valori

- bnz route_noop_operations: Se corrispondono, salta alla sezione che gestisce le operazioni NoOp

Il campo *OnCompletion* indica quale operazione il contratto è chiamato ad eseguire dopo il completamento della chiamata all'applicazione, infatti può capitare che il contratto subisca degli aggiornamenti oppure si potrebbe verificare la presenza di *bugs* durante la fase di *test* o anche semplicemente vi sono delle sezioni e controlli che appesantiscono il contratto rendendo costoso il processo in termini di potenza computazionale, pertanto si potrebbe modificare o eliminare determinate sezioni, escludendole dall'esecuzione.

- **NoOp**: Operazione standard senza modifiche al contratto
- **DeleteApplication**: Richiesta di eliminazione dell'applicazione
- **UpdateApplication**: Richiesta di aggiornamento del codice dell'applicazione
- **OptIn**: Un utente sta aderendo all'applicazione (per utilizzare lo stato locale: potenziale investitore)

Questa struttura gerarchica di percorso (routing) consente al contratto di gestire diverse operazioni in modo ordinato e modulare, snellendo l'architettura del processo e specificando la singola richiesta che il contratto è chiamato ad eseguire.

```
route_noop_operations:
txna ApplicationArgs 0
byte "place_bid"
==
bnz handle_place_bid
```

Una volta stabilito che la transazione è di tipo NoOp, il contratto esamina il primo argomento dell'applicazione per determinare quale operazione specifica eseguire:

- txna ApplicationArgs 0: Accede al primo argomento dell'applicazione
- byte "place_bid": Crea una sequenza di byte per il confronto
- = =: Confronta i due valori
- bnz handle_place_bid: Se corrispondono, salta alla sezione che gestisce il piazzamento di un'offerta

Gli argomenti dell'applicazione sono dati arbitrari forniti con la chiamata e vengono utilizzati per specificare l'azione desiderata, per fare un esempio questo contratto supporta differenti tipologie di operazioni comuni all'interno di un'asta come:

- **place_bid**: Piazzare un'offerta
- **finalize_auction**: Finalizzare l'asta

- **claim_tokens**: Richiedere i *token* guadagnati
- **withdraw_funds**: Ritirare i fondi raccolti
- **update_pause**: Modificare lo stato di pausa dell'asta

Per quanto riguarda l'ultimo comando, ovvero *update_pause*, è stato aggiunto per garantire un maggiore controllo e più sicurezza nel processo di ICO ed in generale nella gestione del contratto. Potrebbe in effetti accadere che vi sia la presenza di un bug, piuttosto che l'impresa emittente desideri un aggiornamento nella logica del contratto, come ad esempio nuove funzioni oppure modifiche nel processo di allocazione dei *token*. In questo modo infatti il processo si potrebbe interrompere senza compromettere l'intera emissione, bisogna però precisare che, essendo fondamentalmente un punto di debolezza, questo comando a differenza degli altri ed insieme a *finalize_auction* e *withdraw_funds* può essere attivato soltanto dall'indirizzo del *creator*, ovvero l'impresa emittente che gestisce l'intero processo[87].

Inizializzazione dell'Applicazione

```
handle_creation:

byte "paused"

int 0

app_global_put

byte "auction_finalized"

int 0

app_global_put
```

Questa sezione del codice viene eseguita soltanto durante la creazione iniziale ovvero nel momento in cui il contratto viene pubblicato sulla *blockchain* e vengono assegnati gli stati globali iniziali.

- byte "paused": Crea una chiave per lo stato globale, questo è un valore booleano, in tal caso viene impostato a 0 il che indica quindi un stato attivo e non di pausa.
- int 0: Carica il valore 0 (falso, non in pausa)

[87] All'interno del contratto sono presenti gli *script* dei comandi riportati, in questo paragrafo al fine di snellire la descrizione si riportano soltanto le parti principali che costituiscono la struttura di questo strumento, per approfondire si veda l'appendice.

- app_global_put: Scrive la coppia chiave-valore nello stato globale dell'applicazione

La fase di inizializzazione è in effetti una della più delicate dell'intero processo, infatti la criticità deriva dal fatto che lo stato iniziale dell'asta e tutte le variabili che in seguito verranno utilizzate nel processo di offerta, allocazione dei fondi e ritiro degli stessi, vengono definite in questa sezione.

Le variabili chiave inizializzate in questo contratto sono le seguenti, si nota inoltre come le prime tre siano essenzialmente degli operatori booleani che possono assumere due valori, ovvero 0 e 1 che indica lo stato attivo oppure disattivo.

Variabile	**Tipo**	**Valore iniziale**	**Descrizione**
paused	intero	0	Flag che indica se l'asta è in pausa (0=attiva, 1=in pausa)
auction_finalized	intero	0	Flag che indica se l'asta è stata finalizzata
funds_withdrawn	intero	0	Flag che indica se i fondi sono stati ritirati
total_tokens	intero	10,000,000	Numero totale di *token* disponibili per l'asta
distributed_*token*s	intero	0	Contatore dei *token* già distribuiti
min_bid_amount	intero	1000	Importo minimo accettabile per un'offerta (in microAlgos)
highest_bid	intero	0	Valore dell'offerta più alta ricevuta
highest_bidder	stringa	""	Indirizzo dell'offerente con l'offerta più alta
total_bids	intero	0	Contatore del numero totale di offerte ricevute
total_bid_amount	intero	0	Somma totale di tutte le offerte ricevute
clearing_price	intero	0	Prezzo finale di liquidazione dell'asta
*token*s_to_distribute	intero	0	Quantità totale di *token* da distribuire

Meccanismo di gestione delle offerte

Il processo di piazzamento delle offerte è il punto centrale del sistema d'asta, in questa sezione si vuole spiegare la logica e le funzioni utilizzate nel contratto al fine di registrare ed accettare le offerte piazzate dai differenti *account* degli investitori.

```
handle_place_bid:
byte "paused"
app_global_get
int 0
==
bz pause_err
byte "auction_finalized"
app_global_get
int 0
==
bz finalized_err
```

Come si può facilmente notare, questi comandi assicurano in primo luogo che lo stato iniziale dell'asta sia attivo, e questo può essere verificato quando lo stato di pausa non è attivo e quindi impostato a zero. Dopo questa verifica il contratto procede con il controllo della struttura del gruppo di transazioni che in tal caso devono essere necessariamente due, infatti il sistema si aspetta un pagamento ed una chiamata all'applicazione che permette di inizializzare lo *smart contract*.

```
global GroupSize
int 2
==
bz group_size_err
// Verifica i tipi di transazione
gtxn 0 TypeEnum
int pay
==
bz type_err
gtxn 1 TypeEnum
int appl
==
bz type_err
```

In seguito alla definizione delle due transazioni, si procede con la verifica del destinatario del pagamento, in questo caso lo *smart contract* e l'applicazione sul quale questo è stato

inizializzato, presentano un indirizzo specifico e univoco che non può essere replicato da altri protocolli. per poter visualizzare quindi l'indirizzo specifico si usa CurrentApplicationAddress, ovvero una funzione globale che restituisce l'indirizzo Algorand associato al contratto corrente.

```
gtxn 0 Receiver
global CurrentApplicationAddress
==
bz receiver_err
```

Dopo aver verificato l'indirizzo del destinatario, si procede a definire in modo corretto l'importo dell'offerta, questa per ovvie ragioni deve essere maggiore di zero e almeno pari all'importo minimo stabilito, ad esempio nella simulazione in ambiente controllato questa è stata posta uguale a 100000 microAlgos.

```
gtxn 0 Amount
int 0
>
bz invalid_bid_err
gtxn 0 Amount
byte "min_bid_amount"
app_global_get
>=
bz low_bid_err
```

Una volta superate tutte le verifiche, il contratto procede quindi a memorizzare l'offerta e ad aggiornare i contatori globali:

```
txn Sender
byte "user_bid"
gtxn 0 Amount
app_local_put
```

L'importo dell'offerta viene memorizzato nello stato locale dell'utente sotto la variabile "user_bid", permettendo quindi di tenere traccia delle offerte individuali di ciascun investitore. Il contatore globale delle offerte viene incrementato di 1 e l'operazione duplica l'elemento in cima al blocco "total_bids" per riutilizzarlo.

```
byte "total_bids"
dup
app_global_get
```

```
int 1
app_global_put
byte "total_bid_amount"
dup
app_global_get
gtxn 0 Amount
+
app_global_put
```

La somma totale delle offerte viene incrementata dell'importo dell'offerta corrente, se poi l'offerta corrente è superiore all'offerta più alta finora ricevuta, il contratto aggiorna le variabili corrispondenti:

```
gtxn 0 Amount
byte "highest_bid"
app_global_get
>
bz skip_highest_update
byte "highest_bid"
gtxn 0 Amount
app_global_put
byte "highest_bidder"
txn Sender
app_global_put
byte "Nuovo miglior offerente"
log
```

Questo meccanismo consente di mantenere costantemente aggiornato il registro delle offerte, identificando automaticamente le proposte più elevate e generando un evento di log ogni volta che viene registrata una nuova offerta massima. L'evento di log consiste nell'emissione di una stringa testuale contenente un messaggio informativo, che viene allegato alla transazione in modo trasparente. In questo modo, il sistema assicura tracciabilità e trasparenza durante l'intero svolgimento dell'asta, permettendo a tutti i partecipanti di monitorarne l'evoluzione in tempo reale.

Processo di Finalizzazione dell'Asta

Dopo aver accettato e registrato le offerte degli investitori, l'asta deve giungere ad una conclusione, prima della chiusura effettiva avviene un processo chiamato finalizzazione, questo consiste essenzialmente nella determinazione di un prezzo finale per i singoli *token*, in questo caso un prezzo marginale derivante dalle offerte inoltrate, e nella distribuzione dei *token* ai nuovi soci.

Come affermato anche in precedenza soltanto la società emittente, ovvero l'*admin* può eseguire il comando di finalizzazione, pertanto i seguenti controlli garantiscono innanzitutto che l'indirizzo sia quello dell' autore del contratto, in seguito il protocollo deve accertarsi che l'asta non sia stata già finalizzata ed infine deve essere presente almeno un'offerta da parte di un singolo *account* prima di concludere definitivamente il processo.

```
txn Sender
global CreatorAddress
==
bz auth_err
byte "auction_finalized"
app_global_get
int 0
==
bz already_finalized_err

byte "total_bids"
app_global_get
int 0
>
bz no_bids_err
```

All'interno di questo contratto per semplicità si è ritenuto opportuno stabilire il prezzo marginale come il prezzo minimo al quale veniva allocata l'intera offerta di *token*, tuttavia questo non impedisce l'implementazione di calcolo più sofisticato, ad esempio si potrebbe prendere in considerazione un prezzo basato su una media ponderata di tutte le offerte, piuttosto che implementare algoritmi di compensazione più complessi.

```
byte "clearing_price"
byte "min_bid_amount"
app_global_get
app_global_put
```

In seguito al calcolo del prezzo secondo la logica stabilita dall'impresa emittente, si procede quindi a concludere formalmente l'asta, per farlo bisogna impedire agli utenti-investitori di immettere ulteriori offerte per acquisire i *token*. L'obiettivo di questi comandi è quello di calcolare e memorizzare l'importo totale dei *token* da distribuire alla platea di nuovi soci, ovviamente in seguito al riscatto dei fondi. In questa implementazione semplificata, viene utilizzato direttamente l'importo totale delle offerte, ma si potrebbe anche applicare una formula di conversione, che riporti ad esempio una proporzione tra Algos investiti e *token* da distribuire, in altre parole un rapporto che definisca una conversione tra criptovaluta e *asset* acquisiti.

```
byte "auction_finalized"
int 1
app_global_put
byte "total_bid_amount"
app_global_get
store 0
byte "tokens_to_distribute"
load 0
app_global_put
```

Procedura di Riscatto dei Token

All'interno di questa sezione, i controlli implementati garantiscono inizialmente che l'asta sia stata finalizzata prima che gli utenti possano riscattare i *token*, si ricorda infatti che qualunque account può eseguire questo comando, successivamente il contratto controlla che l'investitore associato all'*account* abbia effettivamente partecipato all'offerta e che non abbia già riscattato i propri *token*.

```
byte "auction_finalized"
app_global_get
int 1
==
bz not_finalized_err
txn Sender
byte "user_bid"
app_local_get
int 0
>
bz no_participation_err
txn Sender
```

```
byte "tokens_claimed"
app_local_get
int 0
==
bz already_claimed_err
```

Attraverso questi comandi si avvia un processo che recupera e memorizza l'offerta dell'utente nel registro 1, in seguito viene calcolato il rapporto tra l'offerta e l'importo complessivo di tutte le proposte ricevute, questo risultato viene salvato nel registro 2. Il rapporto così ottenuto viene quindi moltiplicato per il numero totale di *token* disponibili, determinando la quantità specifica spettante al singolo utente, questa informazione viene dunque archiviata nel registro 3. È importante sottolineare che TEAL effettua le divisioni con arrotondamento verso il basso, il che può comportare leggere perdite di precisione nel calcolo finale.
In sintesi i comandi memorizzano e applicano la seguente formula per ottenere i *token* specifici:
*token_utente = (offerta_utente / importo_totale_offerte) * token_totali*

```
txn Sender
byte "user_bid"
app_local_get
store 1  // Offerta dell'utente
load 1
byte "total_bid_amount"
app_global_get
/
store 2  // Rapporto (offerta_utente / totale_offerte)
load 2
byte "total_tokens"
app_global_get
*
store 3  // Token da assegnare
```

Infine, il contratto tiene traccia dei *token* riscattati, aggiornando lo stato locale dell'utente, in questo modo il contatore globale dei *token* distribuiti si aggiorna considerando il numero di *token* assegnati per il singolo investitore. Questo meccanismo assicura da un lato che l'utente non possa riscattare i *token* più di una volta, e dall'altro che si mantenga uno storico accurato del numero complessivo di *token* effettivamente distribuiti.

```
txn Sender
byte "tokens_claimed"
```

```
int 1
app_local_put
byte "distributed_tokens"
dup
app_global_get
load 3
+
app_global_put
```

Meccanismo di Ritiro dei Fondi

Si procede poi con la descrizione del meccanismo che consente il ritiro dei fondi ottenuti mediante l'asta marginale. Questi controlli nello specifico assicurano che il ritiro possa essere effettuato esclusivamente dal creatore del contratto, ossia dall'impresa emittente, soltanto in seguito alla finalizzazione dell'asta. In questo esempio si è ritenuto necessario creare ulteriori controlli di verifica, il sistema infatti si accerta che i fondi non siano già stati precedentemente ritirati, impedendo così eventuali tentativi di prelievo multiplo non autorizzato.

```
txn Sender
global CreatorAddress
==
bz auth_err
byte "auction_finalized"
app_global_get
int 1
==
bz not_finalized_err
byte "funds_withdrawn"
app_global_get
int 0
==
bz already_withdrawn_err
```

Il contratto imposta un *flag* per indicare che i fondi sono stati ritirati, ma in un'implementazione completa questo passaggio dovrebbe essere accompagnato da una transazione di pagamento che trasferisca effettivamente i fondi dal contratto al creatore. Va precisato che, nelle versioni più recenti di Algorand, tale trasferimento richiede l'impiego di una *inner transaction*, una funzionalità che consente al contratto stesso di inviare fondi a un indirizzo specificato. In questo esempio, la logica della *inner transaction* non è stata implementata per motivi di semplicità.

```
byte "funds_withdrawn"
int 1
app_global_put
```

Questa è in generale la macro struttura del contratto su Algorand, tuttavia come accennato anche nella descrizione delle sezioni, si necessita di un'applicazione al fine di inizializzare il processo di asta marginale. Inizialmente dopo aver strutturato il contratto e salvato sul server si eseguono i seguenti comandi per caricarlo nella directory corretta e quindi sulla *blockchain* di Algorand, dopo aver eseguito i comandi, si genera un codice univoco, questo non è altro che un *bytecode* necessario per il corretto caricamento dello *smart contract* sul protocollo. Ovviamente in questa sede si riportano i comandi reali usati all'interno del Docker personale con i riferimenti specifici alla macchina usata per il *test* di caricamento. In particolare in questo test, il nome del *file* usato per il salvataggio del contratto è "IPO_Smart_Contract_2.teal", anche il codice *sandbox* riferito ad Algorand, ovvero "98995153edee" risulta essere quello reale usato per l'implementazione.

```
docker cp /Users/alessandroamelio/Desktop/IPO_Smart_Contract_2.teal
98995153edee:/root/IPO_Smart_Contract_2.teal
docker exec -it 98995153edee /bin/sh
cd /root
goal clerk compile IPO_Smart_Contract_2.teal
```

In seguito al caricamento del contratto nella *directory*, il passo successivo è creare l'applicazione, necessaria per inizializzare il tutto. In questa implementazione si usa il seguente comando, dove viene specificato il *file* TEAL del contratto da eseguire, ovvero la logica fondamentale dell'applicazione, successivamente viene indicato il programma, sempre realizzato con il medesimo linguaggio, da eseguire quando un utente imposta un'operazione di *clear state*, cioè la rimozione volontaria della propria partecipazione all'applicazione.

```
goal app create \
  --creator 5SPCXRA3VGXXGWBSNZNZYGBK7FROU4HJESQBSTKYVCPFAS3RHLHVXYTF7E \
  --approval-prog IPO_Smart_Contract_2.teal \
  --clear-prog clear.teal \
  --global-byteslices 1 \
  --global-ints 8 \
  --local-byteslices 1 \
  --local-ints 1
```

Le quattro stringhe finali, sono dei parametri che incidono sullo stato globale e locale:

- `--global-byteslices 1`: alloca 1 *slot* di tipo *byte slice* nello *stato globale* del contratto (es. per salvare una stringa o un indirizzo).
- `--global-ints 8`: alloca 8 interi nello *stato globale* (usati ad esempio per registrare il prezzo corrente, il numero di partecipanti, il totale dei *token*,).
- `--local-byteslices 1`: alloca 1 *slot* di tipo *byte slice* nello *stato locale* di ogni utente (utile per informazioni personalizzate, come un flag).
- `--local-ints 1`: alloca 1 intero nello *stato locale* per ogni utente (ad esempio per memorizzare l'offerta individuale o i *token* riscattati).

Il comando una volta lanciato, genera un numero identificativo per l'applicazione che dovrà in seguito essere riportato nei comandi successivi per la definizione dell'offerta, nello specifico un esempio di comando con il quale un *account* può generare un'offerta per i *token* è il seguente:

```
goal clerk send \
  --from 5SPCXRA3VGXXGWBSNZNZYGBK7FROU4HJESQBSTKYVCPFAS3RHLHVXYTF7E \
  --to <Application Account > \
  --amount 700000 \
  --out payment.tx
// chiamata applicativa
goal app call \
  --app-id <app-id-creato> \
  --from 5SPCXRA3VGXXGWBSNZNZYGBK7FROU4HJESQBSTKYVCPFAS3RHLHVXYTF7E \
  --app-arg "str:place_bid" \
  --out app_call.tx
```

Si può notare come l'ammontare dell'offerta sia pari a 700000 microAlgos, questa proviene dall'*account* principale usato per la creazione dell'applicazione. Nella chiamata applicativa poi, si procede ad aggiornare lo stato globale dell'applicazione, quindi poter concludere la propria offerta, bisogna inserire l'*app-id*, cioè specificare quale tipologia di logica aggiornare, in questo caso appunto lo *smart contract* caricato nel comando precedente.

Per quanto riguarda poi il *file* clear.teal, usato come accennato per le operazioni di rimozione degli account, si compone essenzialmente di un intero, il suo utilizzo si ha nello specifico nel

momento in cui un *account* voglia interrompere la propria partecipazione al processo di asta marginale e quindi lasciare definitivamente il processo di ICO.

```
#pragma version 6

int 1

return
```

3.4 Considerazioni e analisi delle limitazioni

Il contratto appena descritto è stato creato con l'obiettivo di implementare un'architettura abbastanza complessa, tale da potersi affermare come una potenziale innovazione per la gestione delle procedure di ICO. Questa innovazione, nello specifico, si concretizza attraverso una differente procedura di *pricing*, che va ad aggiungere le caratteristiche di un'asta marginale per evitare l'incertezza e quindi il fenomeno dell'*underpricing* tra gli investitori. L'intera struttura del contratto è infatti pensata per garantire scalabilità, efficienza e robustezza, anche se, trattandosi di una versione puramente dimostrativa ed accademica, presenta delle evidenti limitazioni operative.

Nel momento in cui si va a delineare la costruzione di uno *smart contract*, soprattutto nell'ambito finanziario, uno dei punti fondamentali che viene testato maggiormente è la sicurezza. In particolare se il contratto viene destinato alla gestione di un'ICO, trattandosi di un ambito molto innovativo, la fiducia degli investitori può essere messa a repentaglio da potenziali errori imputabili al codice di programmazione. Pertanto, in seguito allo studio di casi pratici[88], che hanno implementato questi strumenti innovativi con successo, si è capito come il punto fondamentale dovesse essere garantire una sicurezza più elevata possibile con le conoscenze e gli strumenti a disposizione. In questo caso il contratto ha un *design* molto robusto, che permette di coniugare in modo efficiente scalabilità e sicurezza; in particolare questi aspetti si evidenziano poiché il contratto riuscirebbe potenzialmente a gestire un numero elevato di *account* (es. i potenziali investitori) e al tempo stesso mantenere i ruoli assegnati.

Come si è visto in precedenza soltanto gli amministratori possono eseguire determinati comandi come la finalizzazione, la pausa e il ritiro dei fondi, d'altro canto gli altri utenti possono soltanto piazzare le proprie offerte. Tuttavia, visto che la separazione dei ruoli non basta per garantire la completa sicurezza, nei comandi vi sono vari controlli di stato, che

[88] https://www.cdp.it/sitointernet/page/it/cdp_emette_con_successo_il_suo_primo_digital_bond_su_blockchain_intesa_sanpaolo_sottoscrive_interamente_loperazione?contentId=CSA48474
https://www.enel.it/it-it/blog/storie/ebitts-blockchain-accesso-rinnovabili

assicurano la correttezza e l'esecuzione di tutte le operazioni. Di fatti, il riscatto dei fondi può avvenire soltanto dopo la finalizzazione, così come il ritiro dei *token* può essere eseguito soltanto una volta, al fine di evitare la duplicazione. Un'ulteriore garanzia per la maggiore sicurezza è la verifica degli *input*, il codice gestisce tutte le operazioni di verifica controllando che le transazioni siano inviate all'indirizzo corretto e che le offerte soddisfino i requisiti minimi. Inoltre, per evitare ulteriori errori del codice, all'interno del contratto vi sono molteplici *log* che hanno la funzione essenziale di mostrare dove il codice fallisce e quindi, segnalare quale parte non viene correttamente eseguita.

Per quanto concerne poi la scalabilità, il contratto è stato progettato con particolare attenzione anche su questo punto, con l'obiettivo di poter supportare un elevato numero di partecipanti senza compromettere l'efficienza operativa.

La gestione delle offerte individuali è semplice, queste ultime sono memorizzate nello stato locale dei singoli *account* per tenerne traccia ed in questo modo si riduce la pressione sullo stato globale del contratto, che conserva solamente le statistiche aggregate ed i parametri essenziali.

In aggiunta, le operazioni sono tutte singole, cioè concepite per completarsi interamente all'interno di un'unica transazione o di un gruppo di transazioni eseguite simultaneamente, evitando così le dipendenze tra chiamate differenti e facilitando quindi l'automazione del processo.

Infine, l'uso efficiente dei registri temporanei (*scratch space*) consente di ottimizzare i calcoli intermedi e di limitare l'accesso allo stato globale, contribuendo quindi alla riduzione dei costi computazionali ed energetici.

Nonostante la solidità generale della struttura del contratto, questo presenta alcune limitazioni tecniche, dovute principalmente alle modalità di calcolo del prezzo marginale e al meccanismo di ritiro dei fondi che segue la finalizzazione dell'asta. Questi aspetti quindi lasciano spazio a diversi miglioramenti, che potranno essere implementati attraverso strumenti e funzioni più avanzate. Nello specifico, per il calcolo del prezzo marginale la logica attuale del contratto prende in considerazione un approccio semplificato, ovvero va a definire il prezzo più basso al quale viene allocata l'intera offerta dei *token*; in un contesto reale infatti sarebbe più opportuno stabilire un algoritmo di calcolo che si adatti alla complessità delle esigenze della singola ICO.

Per quanto riguarda il meccanismo di ritiro dei fondi, attualmente il contratto si limita a segnalarli come ritirati, senza includere un sistema di trasferimento dei fondi verso l'account della società emittente. Questo potrebbe essere implementato tramite la piattaforma Capitolis

che, senza appesantire la struttura del contratto, trasferirebbe i fondi dalla piattaforma verso l'account exchange dell'emittente.

In alternativa si potrebbe utilizzare la funzionalità di *inner transactions*[89], sfortunatamente però la stessa non è ancora disponibile nelle ultime versione di Algorand senza macchina virtuale, e, dal momento che possono essere effettuate solo 16 transazioni, la dimostrazione pratica sarebbe alquanto limitata. Un'ulteriore tipologia di limitazione, come accennato nei precedenti capitoli, è il tema della sicurezza normativa, nello specifico appunto KYC e AML. Algorand, infatti, supporta strumenti volti a testare e controllare i fondi in entrata, ma risultano ancora molto approssimativi. Uno degli aspetti più problematici di questa disciplina è data dal fatto che gli *smart contract* sono puramente logici e anonimi, questi non hanno modo di verificare l'identità delle controparti, poiché non possono leggere documenti o interpretare dati *off chain*. Una soluzione, come definito in precedenza, è l'implementazione della piattaforma Capitolis che potrebbe fungere da oracolo, ovvero un'entità esterna ad Algorand, con il quale si aggiorna la logica del contratto, permettendo quindi lo svolgimento del processo nel modo corretto, in altre parole un "via libera" dopo aver verificato l'identità degli *account*. L'oracolo potrebbe anche fungere da entità per l'aggiornamento dei prezzi, nel caso in cui l'impresa emittente voglia affermare tutto il processo su una piattaforma, sorpassando in questo modo il tema della sicurezza e della complessità del codice.

Infine, l'ultima limitazione che potrebbe essere superata tramite l'utilizzo di Capitolis o di un'altra piattaforma di gestione di *token,* è l'incasso dei dividendi e la partecipazione alle assemblee societarie per i nuovi investitori. Uno *smart contract* ad oggi non presenta queste funzionalità, che potrebbero tuttavia essere implementate, ma per avere una visione maggiormente pratica della gestione degli *asset*, si ritiene che la piattaforma per queste scelte sia la migliore alternativa al momento possibile.

In conclusione questo *smart contract* rappresenta un'implementazione completa e sofisticata di un sistema d'asta decentralizzato su *blockchain* grazie ad Algorand, che garantisce trasparenza, sicurezza ed efficienza in ogni fase del processo. Si ritiene che il contratto incorpori tutti gli elementi fondamentali che caratterizzano una piattaforma d'asta affidabile: la raccolta sicura delle offerte, la finalizzazione dell'asta con calcolo del prezzo di assegnazione, la distribuzione dei *token* ai partecipanti in base ai risultati, il ritiro controllato dei fondi raccolti

[89] Le inner transactions, o transazioni interne, sono una funzionalità avanzata introdotta nella Algorand Virtual Machine (AVM). Questa consente a uno *smart contract* di creare ed eseguire transazioni direttamente dall'interno della propria logica. In pratica, un contratto può inviare pagamenti, trasferire token ASA, optare per *asset* o applicazioni, o persino chiamare altri *smart contract*, tutto all'interno della stessa esecuzione.

da parte dell'amministratore, e strumenti di gestione come la possibilità di mettere in pausa o riattivare il sistema in modo selettivo. Inoltre, la struttura modulare si presta a una facile manutenzione e modifica sulle esigenze di un'emittente, e, il sistema per la gestione degli errori previene abusi o comportamenti inconsueti, assicurando la robustezza del sistema. Infine la memorizzazione delle offerte degli utenti nello stato locale e dei dati aggregati nello stato globale, contribuiscono in modo decisivo alla scalabilità dell'infrastruttura, ottimizzando contemporaneamente il consumo di risorse e i costi di esecuzione.

Capitolo Quarto

Analisi econometriche dei risultati ottenuti tramite simulazione

In questo capitolo conclusivo si vuole affermare un'ulteriore analisi, questa volta di tipo econometrico con l'obiettivo di rendendere ancora più robusta la giustificazione in merito all'implementazione del meccanismo di asta marginale per le procedure di *pricing* all'interno del mercato primario. L'analisi svolta si concentrerà dapprima sulla creazione di una simulazione di ICO tramite lo *smart contract*, ovvero in ambiente controllato sulla *blockchain* di Algorand. Successivamente il processo di simulazione verrà reiterato per ottenere un campione di osservazioni più numeroso, infine verrà sviluppato un modello inferenziale per testare le determinanti dell'*underpricing* e dunque trarre le conclusioni in merito all'efficienza di questo sistema di *pricing*.

4.1 Implementazione del modello multivariato

In seguito alla realizzazione del contratto attraverso la *blockchain* di Algorand, l'obiettivo successivo dell'analisi si focalizza sulla realizzazione di un *test*, per stabilire la validità del codice e dunque avviare un'asta sul mercato primario tramite lo *smart contract*. Il *test* in questione è cruciale, questo perché dimostra innanzitutto la presenza di eventuali errori nel codice, e come le offerte dei singoli investitori influenzano l'*underpricing* dell'intera emissione dei *token*. Per definire quindi un'ambiente di *test* valido, in primo luogo sono stati creati 50 *account ex novo*, che rappresentano il totale degli investitori partecipanti all'asta. Come chiarito anche nel capitolo precedente, questo numero non risulta realistico, visto che in una reale emissione vi sono migliaia di investitori, tuttavia è sufficiente per rispettare i principi del teorema del limite centrale.

Di seguito si riportano i comandi usati su Docker per la creazione della simulazione:

```
#!/bin/bash
CREATOR="5SPCXRA3VGXXGWBSNZNZYGBK7FROU4HJESQBSTKYVCPFAS3RHLHVXYTF7E"
APP_ID=1099
NUM_PARTICIPANTS=50
FUND_AMOUNT=2000000
MIN_BID=100000
MAX_BID=1000000
rm -f test_accounts.txt payment.tx app_call.tx combined.tx grouped.tx split-0.tx
split-1.tx signed-0.tx signed-1.tx signed-final.tx
ACCOUNTS_FILE="test_accounts.txt"
> "$ACCOUNTS_FILE"
```

```
echo "1. Creo $NUM_PARTICIPANTS account"
for i in $(seq 1 $NUM_PARTICIPANTS); do
    ACCOUNT=$(goal account new | grep "Created new account" | awk '{print $4}')
    echo "$ACCOUNT" >> "$ACCOUNTS_FILE"
done
echo "2. Finanziamento account"
for ACCOUNT in $(cat "$ACCOUNTS_FILE"); do
    goal clerk send --from "$CREATOR" --to "$ACCOUNT" --amount "$FUND_AMOUNT"
done
echo "3. Opt-in all'app ID $APP_ID..."
for ACCOUNT in $(cat "$ACCOUNTS_FILE"); do
    goal app optin --app-id "1053" --from "$ACCOUNT"
done
echo "4. Invio offerte random"
APP_ADDRESS=$(goal app info --app-id "$APP_ID" | grep 'Application account' | awk
'{print $3}')
for ACCOUNT in $(cat "$ACCOUNTS_FILE"); do
    BID_AMOUNT=$((MIN_BID + RANDOM % (MAX_BID - MIN_BID)))

    goal clerk send --from "$ACCOUNT" --to "$APP_ADDRESS" --amount "$BID_AMOUNT" --
out payment.tx
    goal app call --app-id "$APP_ID" --from "$ACCOUNT" --app-arg "str:place_bid" --
out app_call.tx
    cat payment.tx app_call.tx > combined.tx
    goal clerk group -i combined.tx -o grouped.tx
    goal clerk split -i grouped.tx -o split.tx
    goal clerk sign -i split-0.tx -o signed-0.tx
    goal clerk sign -i split-1.tx -o signed-1.tx
    cat signed-0.tx signed-1.tx > signed-final.tx
    goal clerk rawsend -f signed-final.tx
done
echo "5. Finalizzazione dell'asta"
goal app call \
  --app-id "1053" \
  --from "$CREATOR" \
  --app-arg "str:finalize_auction"
echo "goal app read --app-id 1053 --global --guess-format"
```

Attraverso l'esecuzione del codice vengono generate delle transazioni in modo casuale; ogni *account* esegue infatti una transazione singola, composta da un pagamento e una chiamata all'applicazione con l'argomento "place_bid", corrispondente all'invio di un'offerta casuale compresa tra due soglie ovvero MIN_BID e MAX_BID. Questo processo vuole riprodurre, nel modo più realistico, il comportamento eterogeneo dei partecipanti in un'asta pubblica.

Ovviamente, essendo ogni investitore dotato di una razionalità differente, non è possibile con una semplice simulazione prevedere tutti gli scenari che si otterrebbero con 50 *account* reali. Inoltre molto spesso le decisioni di investimento sono anche dettate dalle scelte euristiche[90] e ciò rende ancor più complesso il quadro generale.
Infine, il prezzo marginale viene determinato in base alla distribuzione delle offerte ricevute, selezionando la soglia, in questo caso il 70° percentile[91], che separa i vincitori dai non vincitori dell'asta. La finalizzazione dell'asta sancisce il termine della simulazione, che può essere stabilito soltanto dell'amministratore. In questo modo si attiva la logica di chiusura e il sistema si prepara alla successiva distribuzione dei *token* ed il ritiro dei fondi da parte dell'emittente.
In seguito per testare il processo di esecuzione dell'asta su un numero maggiore di transazioni e ottenere così dei risultati più robusti, sono state eseguite 100 aste indipendenti, sempre con 50 partecipanti ed un prezzo marginale fissato al medesimo percentile di cui sopra. In questo caso il valore effettivo dei *token* è stato posto a 90 Algos, mentre la variabile *underpricing* è stata calcolata come il differenziale tra questo valore ed il prezzo marginale.
Con questo ulteriore test si intende comprendere se il modello ad asta marginale implementato nel contratto possa effettivamente ridurre l'*underpricing* in un contesto di offerta pubblica. Ciò è possibile analizzando i risultati ottenuti attraverso un modello di regressione multivariato, con l'obiettivo di definire quali siano le variabili determinati dell'*underpricing* nelle IPO.

Il modello può essere così sintetizzato[92]:

$$Underpricing_i = \alpha_0 + \beta_1 . Distanza\_Marginale_i + \beta_2 . Ranking\_Offerte_i + \beta_3 . Volatilità_i + \varepsilon_i$$

Questo modello multivariato presenta tre variabili, ovvero Distanza_Marginale$_i$, Ranking_Offerte$_i$ e Volatilità$_i$. La prima si riferisce al differenziale tra il prezzo di offerta individuale ed il prezzo marginale, la seconda variabile, consente di valutare quanto un'offerta sia competitiva su base relativa. Il ranking, infatti, fa riferimento alla competitività dell'offerta individuale sul totale delle offerte ricevute dall'emittente. Ogni offerta viene classificata in un

[90] Kahneman, Daniel. *Thinking, Fast and Slow*. London: Penguin Books, 2011.
[91] Questa soglia non è stata di certo scelta caso, infatti per avere un risultato maggiormente realistico nella simulazione soltanto il 30% delle offerte immesse viene accettato, ovvero solo una parte degli account risulta a tutti gli effetti vincitrice. La soglia è infatti definita per diverse ragioni, in primo luogo garantire una selezione significativa di vincitori, in seguito riprodurre una condizione in cui la domanda supera l'offerta, è limitato e solo ed infine evitare gli effetti distorsivi degli outliers.
[92] Per l'elaborazione del modello econometrico è stato utilizzato python, il codice completo del modello multivariato così come tutti i test sull'eteroschedasticità degli errori e sulla non stazionarietà della serie si ritrovano in appendice.

range normalizzato tra 0 ed 1, quelle con *ranking* vicino a 0 sono classificate come più elevate e quindi più aggressive, mentre le offerte vicine al valore 1 indicano quelle deboli o marginali. Infine, la volatilità è stata introdotta nel modello come misura *proxy* dell'incertezza sul valore reale del *token*. La volatilità è stata generata esogenamente come parametro aleatorio continuo in un intervallo compreso tra 2 e 10 ed in seguito assegnata in modo omogeneo a tutti gli investitori partecipanti all'asta. La scelta di implementare anche la volatilità, riflette un contesto in cui ciascuna emissione avviene sotto condizioni di mercato diverse, più o meno stabili, che influenzano le strategie di offerta degli investitori. L'evidenza empirica dimostra infatti che in presenza di maggiore incertezza, gli investitori tendono a comportarsi in modo più prudente, riducendo l'aggressività delle offerte, ciò porta ad un prezzo marginale inferiore e ad un minore differenziale tra valore dell'*asset* e prezzo pagato, con conseguente riduzione dell'*underpricing* individuale.

Di seguito si riportano i risultati ottenuti attraverso questo modello di regressione:

- Intercetta $\alpha_0 = 80.95$
- $\beta_1 = +\ 0.96$***; unità di *underpricing* in più per ogni unità offerta sopra il prezzo marginale.
- $\beta_2 = -\ 86.68$***; Se l'offerta è tra le meno competitive (*ranking* vicino a 1), l'*underpricing* si riduce fortemente.
- $\beta_3 = -\ 0.25$***; Maggiore incertezza (volatilità percepita), minore sarà l'*underpricing.*

OLS Regression Results

Dep. Variable:	underpricing	R-squared:	0.292
Model:	OLS	Adj. R-squared:	0.291
Method:	Least Squares	F-statistic:	206.2
Date:	Sat, 10 May 2025	Prob (F-statistic):	6.66e-112
Time:	16:41:02	Log-Likelihood:	-4928.5
No. Observations:	1500	AIC:	9865.
Df Residuals:	1496	BIC:	9886.
Df Model:	3		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
const	80.9536	3.030	26.719	0.000	75.011	86.897
marginal_distance	0.9614	0.039	24.572	0.000	0.885	1.038
ranking_offer	-86.6758	4.023	-21.543	0.000	-94.568	-78.784
volatility	-0.2505	0.078	-3.230	0.001	-0.403	-0.098

Omnibus:	4.274	Durbin-Watson:	0.446
Prob(Omnibus):	0.118	Jarque-Bera (JB):	4.356
Skew:	0.089	Prob(JB):	0.113
Kurtosis:	3.196	Cond. No.	516.

Come si può facilmente notare dall'*output* di Python, tutti i coefficienti testati nel modello risultano statisticamente significativi al 1%, questo evidenzia quindi la robustezza dell'analisi

e delle relazioni osservate che spiegano la variabile dipendente, in questo caso il fenomeno dell'*underpricing*.

In linea con le attese, l'*underpricing* aumenta all'aumentare della distanza tra offerta e prezzo marginale. Questo accade perché i partecipanti che offrono importi superiori alla soglia di assegnazione dei *token*, beneficiano di un maggiore guadagno implicito, poiché il prezzo pagato sarà più basso di quello offerto, e dunque si ottiene un risparmio. Il coefficiente negativo associato al *ranking* suggerisce che chi presenta un'offerta più vicina alla soglia minima e quindi con un *ranking* alto, sperimenta un *underpricing* inferiore, poiché il risparmio in questo caso sarà più basso, visto che il prezzo pagato sarà vicino a quello marginale. Infine, anche la volatilità ha un effetto negativo sull'*underpricing*, evidenziando che all'aumentare dell'incertezza i partecipanti presentano un atteggiamento più cauto, riducendo il divario tra valore e prezzo effettivo, come illustrato graficamente nella figura in basso.

Il modello conferma dunque che l'*underpricing* non dipende soltanto da quanto un'offerta si discosta dal prezzo marginale, ma anche dalla competitività relativa dell'offerta e dalla percezione del rischio nel contesto dell'asta. Il modello presenta inoltre un R^2 *Adjusted* pari al 29,2%, il che implica quindi che i fattori al suo interno spiegano poco più del 29% delle osservazioni relative all'*underpricing* presso gli investitori che partecipano a queste 100 aste randomizzate. Per testare la validità del modello OLS è stato effettuato un white test per l'eteroschedasticità degli errori, ed un Dickey-Fuller test aumentato (ADF) per la stazionarietà della variabile dipendente, ossia l' *underpricing.* I risultati del white test presentano un p-value pari a 7.44×10^{-15}, confermando la presenza di una varianza non costante degli errori, mentre per l'ADF test il p-value è pari a 4.93×10^{-6} indicando che si può rifiutare con alto livello di confidenza l'ipotesi nulla di radice unitaria, dimostrando quindi che la serie è stazionaria.

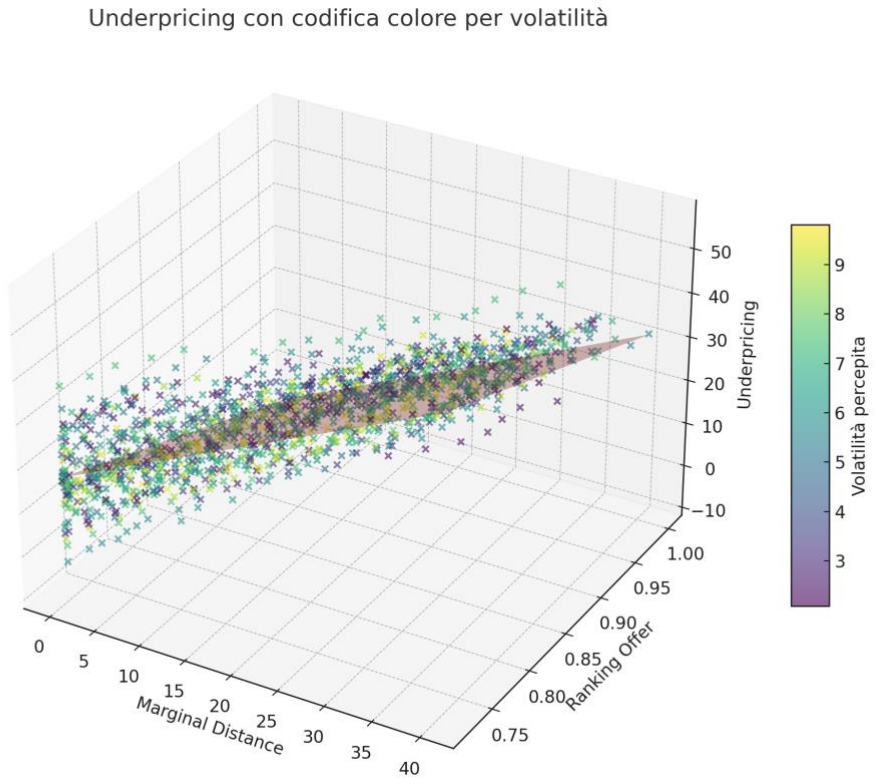
Sebbene quindi il modello delle aste marginali non vada necessariamente a ridurre il fenomeno dell'*underpricing* in termini relativi, questo si presenta come un'ottima soluzione in termini aggregati. Il modello inferenziale afferma che in base alle tre variabili, l'*underpricing* essenzialmente dipende dalle offerte che ciascun investitore presenta all'interno dello *smart contract*, tuttavia bisogna considerare che l'asta marginale riduce se non annulla definitivamente la maledizione del vincitore. Questo fenomeno è una delle cause principali dell'*underpricing* per la società emittente e delle perdite che la stessa riceve nei giorni successivi alle quotazioni sul mercato primario. La teoria delle aste[93], afferma che in un'asta discriminatoria, i fondi raccolti dovrebbero essere superiori rispetto ad un'asta di tipo

[93] Wilson, Robert. "Auctions of Shares." *The Quarterly Journal of Economics* 93, no. 4 (1979): 675–89.

marginale, tuttavia questo non accade. Tuttavia, questa teoria si discosta dalla realtà empirica, in quanto, durante un'asta discriminatoria i partecipanti hanno un incentivo a offrire meno del valore reale dell'*asset* di riferimento, proprio per evitare la *winner's curse*. Al contrario, nelle aste marginali gli investitori possono permettersi di presentare offerte maggiori, poiché sono consapevoli che quasi certamente non pagheranno la cifra offerta. Secondo la teoria delle aste, quindi, l'elemento fondamentale per ottenere più fondi rispetto ad un'asta marginale, consisterebbe nella sincerità dei partecipanti, i quali, non dovrebbero aver nessuna intenzione di effettuare una speculazione.

All'interno dell'asta marginale, i partecipanti possono beneficiare di un prezzo inferiore rispetto alla propria offerta, la natura del meccanismo quindi incentiva offerte più aggressive grazie all'eliminazione del rischio di *winner's curse*, il che quindi conduce a un prezzo marginale spesso più vicino al valore reale del bene. Di conseguenza, l'*underpricing* medio sull'intera emissione si riduce, rendendo l'asta marginale uno strumento più efficiente dal punto di vista della raccolta fondi.

Rappresentazione della regressione tramite modello multivariato a tre variabili[94]:



Fonte: elaborazione propria

[94] In questa figura si nota che osservazioni riprese nelle 100 aste vengono descritte attraverso una superficie regressiva che spiega il 30% di esse attraverso le 3 variabili, distanza marginale, volatilità e ranking dell'offerta.

Studi empirici su larga scala confermano questo effetto, Goldreich[95] analizza i dati delle aste di titoli di Stato nel Regno Unito affermando che, nonostante il meccanismo marginale consenta agli investitori un guadagno potenziale sul prezzo, la media dei proventi per il Tesoro è superiore rispetto alle aste discriminatorie, proprio grazie alla maggiore competitività delle offerte. Simili evidenze emergono anche per i titoli statunitensi; in uno studio commissionato dal *U.S. Treasury Office*[96], si evidenzia che le aste marginali "*producono risultati più prevedibili e raccolte medie superiori, pur in presenza di minore dispersione tra le offerte vincenti*". Anche in Italia, il Ministero dell'Economia e delle Finanze (MEF) utilizza sistematicamente l'asta marginale per l'emissione dei BTP, proprio per favorire la trasparenza e massimizzare la partecipazione, accettando un modesto surplus per gli investitori in cambio di offerte più aggressive e maggiore raccolta complessiva.

[95] Goldreich, D. (2007). *Underpricing in Discriminatory and Uniform-Price Treasury Auctions*. Journal of Financial and Quantitative Analysis, 42(3), 443–466.
[96] Malvey, P. F., & Archibald, T. D. (1998). *Uniform-Price Auctions: Evaluation of the Treasury Experience*. U.S. Treasury Office of Market Finance, Working Paper.

Conclusioni

Il lavoro fin qui svolto si è basato su una domanda fondamentale, ovvero l'attuale sistema di quotazione sul mercato primario risulta efficiente in termini economici? Sia gli aspetti teorici che l'evidenza empirica della disciplina economica suggeriscono che, in fin dei conti, nonostante siano stati creati e predisposte delle metodologie oggettive basate sui fondamentali, il *pricing* non rispecchia l'effettivo valore di una società emittente. A partire dal 2013 un'alternativa seppur poco conosciuta è stata appunto l'ICO, tuttavia anche questo processo presenta non pochi problemi, relativi per lo più all'incertezza e all'asimmetria informativa che lo caratterizza. A dimostrazione di ciò gli ultimi studi in questo ambito, sottolineano come gli investimenti in tal senso non siano efficienti a parità di rischio. Infatti, analizzando un campione di 1707 ICO, in un arco temporale tra il 2019 ed il 2024, si può notare che soltanto una parte di esse ha avuto successo, ovvero soltanto 813 sul totale presentano un volume medio giornaliero di scambi superiore a 100.000 dollari nell'ultimo mese. Il resto, ovvero 894 ICO, sono ufficialmente classificate come "morte" oppure irrilevanti ai fini economici, tuttavia la vera domanda è: valeva la pena investire in queste 813 ICO? La risposta più sintetica è no. Se infatti si prende come *benchmark* Bitcoin (BTC), soltanto 282 ICO hanno ottenuto una *performance* superiore, mentre i *token* rimanenti hanno ottenuto una *performance* soddisfacente ma non tale da essere definita come un successo o comunque non alla stregua di un investimento più semplice e meno rischioso come quello in BTC[97]. Uno studio ha confrontato questi 282 *token* individualmente, dalla data di lancio fino al 6 dicembre 2024, Bitcoin in tal caso viene preso in considerazione come punto di riferimento per comparare le criptovalute, proprio come l'indice S&P 500 nel mercato azionario[98]. Se un progetto quindi non riesce a superare i rendimenti di Bitcoin, il suo valore come investimento diminuisce e pertanto viene considerato meno efficiente. Lo studio quindi, analizzando le 1707 ICO, evidenzia come solo il 16,52% di queste si è rivelato un investimento di successo, mentre il 52% delle ICO sono di fatti classificate come inattive in seguito a 120 giorni dal lancio. Queste osservazioni risultano coerenti anche con un altro studio che prende tuttavia come riferimento un campione di ICO che va dal 2013 fino al 2018, dove anche in questo caso le ICO inattive rappresentavano il 52,37%.

[97] In questo caso la rischiosità si deve confrontare con il protocollo Bitcoin e non in generale con altri strumenti presenti sul mercato. L'autore in questo senso confronta differenti token, ovvero quelli di recente emissione, molto rischiosi, rispetto a BTC, già presente da molti anni sul mercato e quindi molto più sicura se paragonato alle ICO più recenti.
[98] https://www.ccn.com/analysis/crypto/are-icos-still-worth-it/.

Nonostante queste perdite deludenti, l'alternativa più diffusa ovvero l'IPO, presenta delle *performance* altrettanto scarse. Il medesimo studio infatti ha confrontato 2030 imprese che si sono quotate tramite IPO tra il 2019 e il 2024, di queste solo il 9,85% ha effettivamente sovra performato l'S&P 500. Queste analisi sono in linea con le conclusioni di altri autorevoli studi, primo fra tutti quelli di Siegel[99]. Questi ha esaminato la *performance* delle IPO a bassa capitalizzazione, concludendo che, nonostante le IPO generino spesso entusiasmo iniziale e guadagni rapidi, di solito non riescono a dare risultati duraturi nel lungo termine. Nello specifico il campione si compone di quasi 9.000 IPO in un arco temporale che va dal 1968 al 2001, il risultato è che il 79% ha sottoperformato gli indici più ampi delle *small cap*, con quasi la metà in calo di oltre il 10% annuo. Anche nel corso del tempo e con un'attività di IPO di alto profilo, la maggior parte dei portafogli contenenti i titoli neo quotati è rimasta costantemente indietro rispetto al *benchmark* di mercato.

Le evidenze di mercato quindi suggeriscono che sia le ICO che le IPO deludono le aspettative degli investitori, tuttavia nel primo caso bisognerebbe considerare differenti variabili, ovvero la novità di questo strumento così come anche la predominanza del settore *tech* per la quotazione tramite ICO. Ad oggi visti gli enormi vuoti normativi, economici e la predominanza di pochi settori altamente innovativi, elementi che caratterizzano questa procedura, la *performance* economica del 16,52% non risulta affatto negativa, soprattutto con un *benchmark* come BTC, un *asset* che ha costituito una rivelazione per molti investitori ed economisti. Le ICO oggi stanno prendendo sempre più piede, sia nelle offerte pubbliche istituzionali, in Italia esempio per le aste dei BOT[100], così come per le imprese private, che ad oggi sfruttano la tecnologia *blockchain* per suddividere in *token asset* poco liquidi e pertanto poco attrattivi sul mercato (vd. Enel)[101].

Al contrario le IPO, nonostante siano uno strumento che ha raggiunto la sua maturità, presentano ancora delle lacune di efficienza, per la determinazione dei prezzi e per i costi ad essa associati. In questo caso vi è un detto tra gli investitori, ovvero *"IPOs don't stand for initial public offering but, instead, for it's probably overpriced"*. Questo sottolinea la sfiducia che hanno nei confronti delle offerte pubbliche primarie; in effetti nel corso degli ultimi anni, il mercato nel breve periodo non ha saputo prezzare al meglio le azioni delle imprese neo quotate, generando, nella maggior parte dei casi, delle fiammate di volatilità, che alla fine

[99] Siegel, Jeremy J, *Stocks for the Long Run: A Guide to Selecting Markets for Long-term Growth.* Irwin, 1994.
[100] https://www.cdp.it/sitointernet/page/it/cdp_emette_con_successo_il_suo_primo_digital_bond_su_blockchain_intesa_sanpaolo_sottoscrive_interamente_loperazione?contentId=CSA48474.
[101] https://www.enel.it/it-it/blog/storie/ebitts-blockchain-accesso-rinnovabili.

portano ad un'euforia ingiustificata e quindi ad un incremento dei prezzi. La metodologia di *pricing* descritta nell'elaborato presenta certamente delle limitazioni, tuttavia questa potrebbe rappresentare una buona base per migliorare il sistema di *pricing* attuale. Lo scopo come definito anche nell'introduzione è quello di realizzare un *level playing field*, dove tra investitori e società emittente, non vi sia una parte più debole oppure una che debba necessariamente rimetterci per definire un ottimo investimento, di modo che tutti gli interessi degli attori economici siano essenzialmente tutelati al medesimo livello.

Appendice

Si riporta lo *Smart Contract* creato per il processo di simulazione viene riportato ora in forma completa con i commenti utili per definire le azioni e le sezioni del processo di ICO, vista la difficoltà del linguaggio TEAL, durante la costruzione del codice, l'autore si è avvalso di differenti fonti che vanno al di là della conoscenza personale, come appunto le fonti *Open Source*, *script* già presenti sulla pagina di Algorand, sezioni di *smart contract* già testati e implementati, non ultimo anche l'intelligenza artificiale tramite Claude Sonnet 3.5 :

```
#pragma version 6

// --- ROUTING PRINCIPALE ---
txn ApplicationID
int 0
==
bnz handle_creation

// Gestisce le operazioni basate su OnCompletion
txn OnCompletion
int NoOp
==
bnz route_noop_operations
txn OnCompletion
int DeleteApplication
==
bnz handle_delete
txn OnCompletion
int UpdateApplication
==
bnz handle_update
txn OnCompletion
int OptIn
==
bnz handle_optin
err

// --- ROUTING DELLE OPERAZIONI NoOp ---
route_noop_operations:
txna ApplicationArgs 0
byte "place_bid"
```

```
==
bnz handle_place_bid
txna ApplicationArgs 0
byte "finalize_auction"
==
bnz handle_finalize_auction
txna ApplicationArgs 0
byte "claim_tokens"
==
bnz handle_claim_tokens
txna ApplicationArgs 0
byte "withdraw_funds"
==
bnz handle_withdraw_funds
txna ApplicationArgs 0
byte "update_pause"
==
bnz handle_pause_update
err

// --- GESTIONE DELLE PAUSE ---
handle_pause_update:
// Solo l'amministratore può mettere in pausa/riattivare
txn Sender
global CreatorAddress
==
bz auth_err

// Necessita di un argomento: 0=attivo, 1=in pausa
txn NumAppArgs
int 2
==
bz args_err

// Aggiorna lo stato di pausa
byte "paused"
txna ApplicationArgs 1
btoi
app_global_put

byte "Stato di pausa aggiornato"
```

```
log
int 1
return

// --- PIAZZAMENTO OFFERTA ---
handle_place_bid:
// Verifica se l'asta è in pausa
byte "paused"
app_global_get
int 0
==
bz pause_err

// Verifica se l'asta è già finalizzata
byte "auction_finalized"
app_global_get
int 0
==
bz finalized_err

// Controlla la struttura del gruppo di transazioni
global GroupSize
int 2
==
bz group_size_err

// Verifica i tipi di transazione
gtxn 0 TypeEnum
int pay
==
bz type_err

gtxn 1 TypeEnum
int appl
==
bz type_err

// Verifica che il pagamento vada all'indirizzo del contratto
gtxn 0 Receiver
global CurrentApplicationAddress
==
```

```
bz receiver_err

// Verifica che l'offerta sia valida (maggiore di zero)
gtxn 0 Amount
int 0
>
bz invalid_bid_err

// Verifica che l'offerta sia almeno pari al prezzo minimo
gtxn 0 Amount
byte "min_bid_amount"
app_global_get
>=
bz low_bid_err

// Salva l'offerta nello stato locale dell'utente
txn Sender
byte "user_bid"
gtxn 0 Amount
app_local_put

// Aggiorna il contatore delle offerte
byte "total_bids"
dup
app_global_get
int 1
+
app_global_put

// Aggiorna la somma totale delle offerte
byte "total_bid_amount"
dup
app_global_get
gtxn 0 Amount
+
app_global_put

// Se l'offerta è più alta dell'offerta massima finora, aggiorna il record
gtxn 0 Amount
byte "highest_bid"
app_global_get
```

```
>
bz skip_highest_update

byte "highest_bid"
gtxn 0 Amount
app_global_put

byte "highest_bidder"
txn Sender
app_global_put

byte "Nuovo miglior offerente"
log

skip_highest_update:
byte "Offerta registrata"
log
int 1
return

// --- FINALIZZAZIONE ASTA ---
handle_finalize_auction:
// Solo l'amministratore può finalizzare l'asta
txn Sender
global CreatorAddress
==
bz auth_err

// Verifica che l'asta non sia già finalizzata
byte "auction_finalized"
app_global_get
int 0
==
bz already_finalized_err

// Verificare che ci sia almeno un'offerta
byte "total_bids"
app_global_get
int 0
>
bz no_bids_err
```

```
// Calcola e salva il prezzo marginale (in una implementazione completa)
// Nel nostro esempio, impostiamo il prezzo marginale come prezzo di liquidazione
byte "clearing_price"
byte "min_bid_amount"
app_global_get
app_global_put

// Marca l'asta come finalizzata
byte "auction_finalized"
int 1
app_global_put

// Calcola quanti token distribuire in totale
byte "total_bid_amount"
app_global_get
store 0  // Importo totale delle offerte

byte "tokens_to_distribute"
load 0
app_global_put

byte "Asta finalizzata con successo"
log
int 1
return

// --- RISCATTO TOKEN ---
handle_claim_tokens:
// Verifica che l'asta sia finalizzata
byte "auction_finalized"
app_global_get
int 1
==
bz not_finalized_err

// Verifica che l'utente abbia partecipato
txn Sender
byte "user_bid"
app_local_get
```

```
int 0
>
bz no_participation_err

// Verifica che l'utente non abbia già riscattato
txn Sender
byte "tokens_claimed"
app_local_get
int 0
==
bz already_claimed_err

// Calcola quanti token spettano all'utente
txn Sender
byte "user_bid"
app_local_get
store 1  // Offerta dell'utente

// Formula per il calcolo dei token: (offerta_utente / importo_totale_offerte)
* token_totali
load 1
byte "total_bid_amount"
app_global_get
/
store 2  // Rapporto

load 2
byte "total_tokens"
app_global_get
*
store 3  // Token da assegnare

// Segna come riscattato
txn Sender
byte "tokens_claimed"
int 1
app_local_put

// Aggiorna i token totali distribuiti
byte "distributed_tokens"
dup
```

```
app_global_get
load 3
+
app_global_put

byte "Token riscattati con successo"
log
int 1
return

// --- RITIRO FONDI ---
handle_withdraw_funds:
// Solo l'amministratore può ritirare i fondi
txn Sender
global CreatorAddress
==
bz auth_err

// Verifica che l'asta sia finalizzata
byte "auction_finalized"
app_global_get
int 1
==
bz not_finalized_err

// Verifica che i fondi non siano già stati ritirati
byte "funds_withdrawn"
app_global_get
int 0
==
bz already_withdrawn_err

// Imposta il flag di ritiro fondi
byte "funds_withdrawn"
int 1
app_global_put

byte "Fondi pronti per il ritiro"
log
int 1
return
```

```
// --- GESTIONE OPT-IN ---
handle_optin:
// Inizializza lo stato locale dell'utente
txn Sender
byte "user_bid"
int 0
app_local_put

txn Sender
byte "tokens_claimed"
int 0
app_local_put

byte "Opt-in completato"
log
int 1
return

// --- GESTIONE AGGIORNAMENTO ---
handle_update:
// Solo l'amministratore può aggiornare l'applicazione
txn Sender
global CreatorAddress
==
bz auth_err
int 1
return

// --- GESTIONE ELIMINAZIONE ---
handle_delete:
// Solo l'amministratore può eliminare l'applicazione
txn Sender
global CreatorAddress
==
bz auth_err
int 1
return

// --- INIZIALIZZAZIONE CONTRATTO ---
handle_creation:
```

```
// Inizializza le variabili globali dell'asta
byte "paused"
int 0
app_global_put

byte "auction_finalized"
int 0
app_global_put

byte "funds_withdrawn"
int 0
app_global_put

byte "total_tokens"
int 10000000
app_global_put

byte "distributed_tokens"
int 0
app_global_put

byte "min_bid_amount"
int 1000
app_global_put

byte "highest_bid"
int 0
app_global_put

byte "highest_bidder"
byte ""
app_global_put

byte "total_bids"
int 0
app_global_put

byte "total_bid_amount"
int 0
app_global_put
```

```
byte "clearing_price"
int 0
app_global_put

byte "tokens_to_distribute"
int 0
app_global_put

byte "Contratto creato con successo"
log
int 1
return

// --- GESTIONE ERRORI ---
pause_err:
byte "Errore: Asta in pausa"
log
err

finalized_err:
byte "Errore: Asta già finalizzata"
log
err

group_size_err:
byte "Errore: Struttura del gruppo di transazioni non valida"
log
err

type_err:
byte "Errore: Tipo di transazione non valido"
log
err

receiver_err:
byte "Errore: Il destinatario deve essere l'indirizzo del contratto"
log
err

invalid_bid_err:
byte "Errore: Offerta non valida"
```

```
log
err

low_bid_err:
byte "Errore: Offerta inferiore al minimo richiesto"
log
err

auth_err:
byte "Errore: Non autorizzato"
log
err

already_finalized_err:
byte "Errore: Asta già finalizzata"
log
err

no_bids_err:
byte "Errore: Nessuna offerta ricevuta"
log
err

not_finalized_err:
byte "Errore: Asta non ancora finalizzata"
log
err

no_participation_err:
byte "Errore: Nessuna partecipazione rilevata"
log
err

already_claimed_err:
byte "Errore: Token già riscattati"
log
err

already_withdrawn_err:
byte "Errore: Fondi già ritirati"
log
```

```
err

args_err:
byte "Errore: Argomenti non validi"
log
err
```

Di seguito si riporta il codice Python usato per lo sviluppo del modello di regressione multivariato e per l'analisi delle componenti di *underpricing*, anche in questo caso, l'autore si è avvalso di molte fonti *Open Source*:

```
# Librerie necessarie
import numpy as np
import pandas as pd
import statsmodels.api as sm
import matplotlib.pyplot as plt
from statsmodels.stats.diagnostic import het_breuschpagan, het_white
from statsmodels.tsa.stattools import adfuller
from sklearn.linear_model import LinearRegression
from mpl_toolkits.mplot3d import Axes3D

# Parametri simulazione
np.random.seed(42)
n_auctions = 100
n_accounts = 50

records = []
for auction_id in range(n_auctions):
    offers = np.random.uniform(10, 100, n_accounts)
    marginal_price = np.percentile(offers, 70)
    true_value = np.random.normal(loc=90, scale=5)  # Valore reale variabile
    volatility = np.random.uniform(2, 10)  # Volatilità uniforme tra 2 e 10
    ranking = (offers.argsort().argsort() + 1) / n_accounts  # Ranking
normalizzato

    for account_id, (offer, rank) in enumerate(zip(offers, ranking)):
        underpricing = true_value - marginal_price if offer >= marginal_price
else np.nan
        records.append({
            "auction_id": auction_id,
```

```
            "account_id": account_id,
            "offer": offer,
            "marginal_price": marginal_price,
            "true_value": true_value,
            "volatility": volatility,
            "ranking_offer": rank,
            "underpricing": underpricing,
            "marginal_distance": offer - marginal_price
        })

# Creazione DataFrame
df_extended = pd.DataFrame(records)
df_winners_ext = df_extended.dropna(subset=["underpricing"])

# Regressione OLS multivariata
X_multi     =     df_winners_ext[["marginal_distance",     "ranking_offer",
"volatility"]]
X_multi = sm.add_constant(X_multi)
y_multi = df_winners_ext["underpricing"]
model_extended = sm.OLS(y_multi, X_multi).fit()



# White Test
white_test = het_white(residuals, X_multi)

# Test Dickey Fuller
adf_result = adfuller(df_winners_ext["underpricing"].dropna())

# Plot 3D con colore della volatilità
x = df_winners_ext["marginal_distance"]
y = df_winners_ext["ranking_offer"]
z = df_winners_ext["underpricing"]

model_3d = LinearRegression()
model_3d.fit(df_winners_ext[["marginal_distance", "ranking_offer"]], z)

xx, yy = np.meshgrid(
    np.linspace(x.min(), x.max(), 30),
    np.linspace(y.min(), y.max(), 30)
)
zz = model_3d.predict(np.c_[xx.ravel(), yy.ravel()]).reshape(xx.shape)
```

```
fig = plt.figure(figsize=(12, 8))
ax = fig.add_subplot(111, projection='3d')
p = ax.scatter(x, y, z, c=df_winners_ext["volatility"], cmap='viridis',
alpha=0.6)
ax.plot_surface(xx, yy, zz, color='red', alpha=0.4)
ax.set_xlabel("Marginal Distance")
ax.set_ylabel("Ranking Offer")
ax.set_zlabel("Underpricing")
ax.set_title("Modello multivariato: osservazioni colorate per Volatilità")
cbar = plt.colorbar(p, ax=ax, pad=0.1)
cbar.set_label("Volatilità del valore reale")
plt.tight_layout()
plt.show()
"""
final_code_path = "/mnt/data/Codice_ Modello_OLS_Completo.py"
with open(final_code_path, "w") as f:

final_code_path
```

Bibliografia

Adhami, S., Giudici, G. & Martinazzi, S., 2018. Why do businesses go crypto? An empirical analysis of Initial Coin Offerings. *Journal of Economics and Business*.

Adhami, S. & Giudici, G., 2019. Initial Coin Offerings: Tokens as Innovative Financial Assets. In: U. Hacioglu, ed. *Blockchain Economics and Financial Market Innovation*. pp. 61–81.

Barden, R.S., Copeland, J.E., Hermanson, J.R. & Wat, R.H.L., 1984. Going public—what it involves: A framework for providing advice to management. *Journal of Accountancy*.

Beniiche, A., 2020. A Study of Blockchain Oracles. *arXiv:2004.07140*.

Benveniste, L.M. & Wilhelm Jr., W.J., 1997. Initial Public Offerings: Going by the Book. *Journal of Applied Corporate Finance*, 10, pp.98–108.

Berk, J. & DeMarzo, P., 2016. *Corporate Finance*, 4th ed. Boston: Pearson.

Brealey, R.A., Myers, S. & Allen, F., 2008. *Principles of Corporate Finance*, 9th ed. New York: McGraw-Hill.

Brau, J.C., 2010. Why do firms go public?. Marriott School, Brigham Young University.

Brau, J.C. & Fawcett, S.E., 2006. Evidence on What CFOs Think about the IPO Process: Practice, Theory and Managerial Implications. *Journal of Applied Corporate Finance*, 18, pp.107–117.

Budish, E.B., 2018. The Economic Limits of Bitcoin and the Blockchain. University of Chicago Booth School of Business, Working Paper No. 18-07.

Buterin, V., 2022. *Proof of Stake: The Making of Ethereum and the Philosophy of Blockchains*. New York: Seven Stories Press.

Caldarelli, G. & Ellul, J., 2021. The Blockchain Oracle Problem in Decentralized Finance: A Multivocal Approach. *Applied Sciences*, 11(16).

Campbell, J.Y., 2016. Restoring rational choice: The challenge of consumer financial regulation. *American Economic Review*, 106(5), pp.1–30.

Capaccioli, S., 2015. *Criptovalute e bitcoin: un'analisi giuridica*, vol. 4. Milano: Giuffrè Editore.

Catalini, C. & Gans, J.S., 2019. Initial Coin Offerings and the Value of Crypto Tokens. *National Bureau of Economic Research Working Paper* No. 24418.

Chen, H.C. & Ritter, J.R., 2000. The Seven Percent Solution. *Journal of Finance*, 55, pp.1105–1132.

Collomb, A. & De Filippi, P., 2019. From IPOs to ICOs: The Impact of Blockchain Technology on Financial Regulation. *Blockchain Perspectives Joint Research Initiative*, BNP Paribas.

Consob, 2024. *Decreto Legislativo 24 febbraio 1998, n. 58 - Testo unico delle disposizioni in materia di intermediazione finanziaria*, aggiornato con il D.Lgs. n. 125 del 6 settembre 2024.

Cong, L.W., He, Z. & Li, J., 2020. Decentralized Mining in Centralized Pools. *The Review of Financial Studies*, 34(3), pp.1191–1235.

Cornelli, F. & Goldreich, D., 2003. Bookbuilding: How Informative is the Order Book?. *Journal of Finance*, 58(4), pp.1415–1443.

D'Ascenzo, M., 2022. Private capital, 2022 miglior anno di sempre con 23,6 miliardi investiti. *Il Sole 24 Ore*.

De Filippi, P., 2019. The interplay between decentralization and privacy: the case of blockchain technologies. *Coinalytics Whitepaper*.

Di Cagno, D., Guth, W., Pace, N. & Pannaccione, L., 2015. Experience and Gender Effects in an Acquiring-a-Company Experiment Allowing for Value Messages. *LUISS Guido Carli University*.

Ellis, K., Michaely, R. & O'Hara, M., 2000. When the Underwriter is the Market Maker: An Examination of Trading in the IPO Aftermarket. *Journal of Finance*, 55, pp.1039–1074.

Essaghoolian, N., 2019. Initial Coin Offerings: Emerging Technology's Fundraising Innovation. *UCLA Law Review*, pp.294–343.

Equita & LUISS, 2024. *Recent trend of IPOs on Italian markets*. Ottobre.

Fabra, N. & Llobet, G., 2023. Auctions with Privately Known Capacities: Understanding Competition Among Renewables. *The Economic Journal*, 133(651), pp.1106–1146.

Ferreira, D., Li, J. & Nikolowa, R., 2019. Corporate Capture of Blockchain Governance. *European Corporate Governance Institute Working Paper*, No. 593.

Gao, X., Ritter, J.R. & Zhu, Z., 2013. Where Have All the IPOs Gone?. *Journal of Financial and Quantitative Analysis*, 48, pp.1663–1692.

Gilad, Y., Hemo, R. & Micali, S. et al., 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *Massachusetts Institute of Technology CSAIL*.

Gonzalez, M., Guzman, A., Pombo, C. & Trujillo, M., 2012. Family firms and financial performance: the cost of growing. *Emerging Markets Review*, 13(4), pp.626–649.

Goldreich, D., 2007. Underpricing in Discriminatory and Uniform-Price Treasury Auctions. *Journal of Financial and Quantitative Analysis*, 42(3), pp.443–466.

Halevi, T., et al., 2019. Initial Public Offering (IPO) on Permissioned Blockchain Using Secure Multiparty Computation. *IBM Research, Brooklyn College*.

Hansen, R., 2001. Do Investment Banks Compete in IPOs? The Advent of the Seven Percent Plus Contract. *Journal of Financial Economics*, 59, pp.313–346.

Huang, W., Meoli, M. & Vismara, S., 2019. The geography of initial coin offerings. *Small Business Economics*, pp.77–102.

Iosio, C., 2011. IPO per le PMI italiane. *IPSOA Gruppo Wolters Kluwer*, Vol. 32, cap. 1.

Jain, B.A. & Kini, O., 1994. The Post Issue Operating Performance of IPO Firms. *Journal of Finance*, 49, pp.1699–1726.

Kaal, W.A., 2018. Initial Coin Offerings: The Top 25 Jurisdictions and Their Comparative Regulatory Responses. *Stanford Journal of Blockchain Law and Policy*.

Kahneman, D., 2011. *Thinking, Fast and Slow*. London: Penguin Books.

Kerins, F., Kutsuna, K. & Smith, R., 2003. Why Are IPOs Underpriced? Evidence from Japan's Hybrid Auction-Method Offerings. *Claremont Graduate University Working Paper*.

Krigman, L., Shaw, W.H. & Womack, K.L., 2001. Why Do Firms Switch Underwriters?. *Journal of Financial Economics*, 60, pp.245–284.

Laibson, D., Repetto, A. & Tobacman, J., 2007. Estimating Discount Functions with Consumption Choices over the Lifecycle. *National Bureau of Economic Research Working Paper*, No. 13314.

Loughran, T. & Ritter, J.R., 2004. Why has IPO underpricing changed over time?. *Financial Management*, 33(3), pp.5–37.

Loughran, T., Ritter, J.R. & Rydqvist, K., 1994. Initial Public Offerings: International Insights. *Pacific-Basin Finance Journal*, 2, pp.165–199. Aggiornato al febbraio 2021: bear.cba.ufl.edu/ritter

Lowry, M. & Schwert, G.W., 2002. IPO Market Cycles: Bubbles or Sequential Learning?. *The Journal of Finance*, 57(3), pp.1171–1200.

Lowry, M.B., Michaely, R. & Volkova, E., 2017. Initial Public Offerings: A Synthesis of the Literature and Directions for Future Research. *Forthcoming in Foundations and Trends in Finance*.

Makarov, I. & Schoar, A., 2022. Cryptocurrencies and Decentralized Finance (DeFi). *MIT Sloan School of Management*, March.

Malvey, P.F. & Archibald, T.D., 1998. Uniform-Price Auctions: Evaluation of the Treasury Experience. *U.S. Treasury Office of Market Finance Working Paper*.

Masiak, C., Block, J.H., Masiak, T., Neuenkirch, M. & Pielen, K.N., 2020. Initial Coin Offerings (ICOs): Market Cycles and Relationship with Bitcoin and Ether. *Small Business Economics*, pp.1113–1130.

Micali, S., 2019. Algorand: A Secure And Efficient Distributed Ledger. *Theoretical Computer Science*, Volume in Memory of Maurice Nivat, pp.155–183.

Mikkelson, W.H., Partch, M. & Shah, K., 1997. Ownership and Operating Performance of Companies that Go Public. *Journal of Financial Economics*, 44, pp.281–307.

Momtaz, P.P., 2019. Initial Coin Offerings. *PLOS ONE*, October.

Monti, A., 2008. *Introduzione alla statistica*, 2a ed. Napoli: Edizioni Scientifiche Italiane.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Whitepaper originale Bitcoin*.

Orcutt, M., 2018. What is Blockchain?. *Massachusetts Institute of Technology Review*.

Overdahl, J. & Lewis, C.M., 2025. Solana and the SOL Market. *Vanderbilt University*, February.

Platt, M. et al., 2021. The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work. *21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp.1135–1144.

Raimondi, F., 2022. Blockchain: un'analisi comparativa dei diversi protocolli. *Politecnico di Torino*.

Rathnayake, N., Nawadali, I., Louembé, P. et al., 2019. Are IPOs underpriced or overpriced? Evidence from an emerging market. *Research in International Business and Finance*, 50, pp.171–190.

Ritter, J.R., 2020. Monthly number of IPOs and the average first-day return, December. *University of Florida*.

Ritter, J.R., 2025. Initial Public Offerings: Underwriting Statistics Through 2024. *Warrington College of Business, University of Florida*, 27 January.

Salerno, D., Sampagnaro, G. & Verdoliva, V., 2022. Fintech and IPO underpricing: An explorative study. *University of Naples Parthenope*.

Siegel, J.J., 1994. *Stocks for the Long Run: A Guide to Selecting Markets for Long-term Growth*. Irwin.

Simeone, A., 2024. Natura e rilevanza delle contabilità decentralizzate. *Report CONSOB*.

Szabo, N., 1996. Smart Contracts: Building Blocks for Digital Markets. *Extropy Journal of Transhuman Thought*, 16.

Werbach, K. & Cornell, N., 2017. Contracts Ex Machina. *Duke Law Journal*, 67.

Werbach, K., 2018. Trust, but Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, 33(2), pp.487–550.

Wilson, R., 1979. Auctions of Shares. *The Quarterly Journal of Economics*, 93(4), pp.675–689.

Wright, A. & De Filippi, P., 2015. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network*, 34, pp.41–52.

Zetzsche, D.A., Buckley, R.P., Arner, D.W. & Föhr, L., 2018. The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *European Banking Institute Working Paper Series*, 18/2018.

Sitografia

https://www.bancaditalia.it/media/approfondimenti/2024/micar/index.html

https://www.borsaitaliana.it/borsa/glossario/requisiti-di-ammissione.html

https://www.borsaitaliana.it/borsa/glossario/offerta-pubblica-di-sottoscrizione.html

https://www.borsaitaliana.it/borsa/glossario/offerta-pubblica-di-vendita.html

https://www.borsaitaliana.it/azioni/mercati/mercati-landingpage/mercati.htm

https://www.borsaitaliana.it/azioni/mercati/euronext-growth-milan/requisiti/come-accedere.htm

https://www.cdp.it/sitointernet/page/it/cdp_emette_con_successo_il_suo_primo_digital_bond_su_blockchain_intesa_sanpaolo_sottoscrive_interamente_loperazione?contentId=CSA48474

https://www.ccn.com/analysis/crypto/are-icos-still-worth-it/

https://climatetrade.com/algorand-partners-with-climatetrade-to-be-the-greenest-blockchain-with-a-carbon-negative-network/

https://www.enel.it/it-it/blog/storie/ebitts-blockchain-accesso-rinnovabili

https://eur-lex.europa.eu/IT/legal-content/summary/european-crypto-assets-regulation-mica.html

https://www.sec.gov/resources-small-businesses/going-public