Universitas Mercatorum

Università telematica delle Camere di Commercio Italiane

FACOLTÀ DI ECONOMIA

CORSO DI LAUREA IN INGEGNERIA GESTIONALE

Prova Finale in

SISTEMI ICT DISTRIBUITI

DLT e Blockchain: dalla finanza tradizionale alla finanza decentralizzata

RELATORE

Chiar.mo

Prof. Roberto Caldelli

CANDIDATO

SILVIO VENTRE

MATR. 0312000245

Anno Accademico 2021/22

Sommario

Introduzione *4*

Capitolo 1 Distributed Ledger Technologies *6*

1.1. Caratteristiche e tipologie di DLT **6**

1.2. Blockchain **7**

Capitolo 2 Digital Asset *16*

2.1. Bitcoin **17**

2.2. Ethereum **31**

Capitolo 3 Finanza Decentralizzata *44*

3.1. Decentralized Applications **47**

3.2. Token **50**

3.3. Nuove forme di finanziamento **55**

Capitolo 4 Regolamentazione *67*

4.1. Scenario legislativo Europeo **69**

4.2. Scenario legislativo Svizzero **75**

4.3. Scenario legislativo Italiano **78**

4.4. Scenario legislativo Mondiale **88**

Capitolo 5 Caso Studio Sperimentale *93*

5.1. Executive Summary **93**

5.2. Organizzazione **98**

5.3. Soluzione Tecnologica **98**

5.4. Modello Matematico **110**

5.5. Analisi di Mercato **113**

5.6. Strategia e Implementazione **118**

5.7. Piano finanziario e proiezioni **120**

5.8. Aspetti Legali **125**

Conclusioni *132*

Indice delle Figure *134*

Indice delle Tabelle *136*

Bibliografia *137*

Ringraziamenti *145*

Introduzione

Il termine “disruptive” viene utilizzato per la prima volta nel 1995 da Clayton M. Christensen[1]. Da quel momento nasce la definizione di innovazione dirompente attraverso la quale, lo studioso, descrive una tecnologia che irrompe nel mercato e rivoluziona le sue dinamiche.
Ripercorrendo la linea temporale dalla fine degli anni 90 ai nostri giorni si può notare come questa sia stata caratterizzata da numerose tecnologie dirompenti che hanno rivoluzionato i singoli settori in maniera radicale.
Il settore mediatico e quello delle telecomunicazioni, per esempio, con l’avvento di tecnologie sempre più performanti hanno avuto una crescita esponenziale interconnettendo milioni di persone e cambiando drasticamente il modo di comunicare.
Allo stesso modo i settori del Retail, della Musica, della Logistica sono diventati sempre più veloci, aperti e condivisi con la popolazione.
L’introduzione di queste tecnologie *disruptive* ha rivoluzionato anche il mondo delle Istituzioni Finanziarie rendendole più dinamiche, snelle e interconnesse.

Nel primo capitolo di questo elaborato verrà proposta una overview delle **Distributed Ledger Technologies** con un focus sulla tecnologia **Blockchain**, delineando il funzionamento, caratteristiche e ambiti di applicazione.

Nel secondo capitolo verranno trattate le due applicazioni più rilevanti in ambito Blockchain, quali **Bitcoin** e **Ethereum**, analizzando le rispettive

[1] Clayton Magleby Christensen era un accademico e consulente aziendale americano che ha sviluppato la teoria dell'innovazione dirompente, che è stata definita l'idea imprenditoriale più influente dell'inizio del 21° secolo.

caratteristiche e innovazioni che hanno apportato al contesto tecnologico e finanziario.

Nel terzo capitolo sarà introdotta quella che attualmente è nota come Finanza Decentralizzata, o DeFi (Decentralized Finance), andando a delineare i potenziali casi d'uso attraverso l'utilizzo delle tecnologie distribuite. In particolar modo sarà analizzato come queste tecnologie possono, e in alcuni casi lo stanno già facendo, rivoluzionare lo scenario finanziario internazionale.

Nel quarto capitolo verrà fornita una panoramica normativa riguardo l'utilizzo di queste tecnologie in ambiti Finanziari e non, attualmente incerta, analizzando diversi contesti Europei e Mondiali.
In particolare verrà preso in disamina lo scenario Italiano e quello Svizzero.

Come ultimo capitolo si propone un caso sperimentale della creazione di una Piattaforma DeFi per investire in fonti di energia sostenibili e rinnovabili attraverso la tokenizzazione su blockchain di finanziamenti per progetti sulla transizione energetica (Corporate bond, prestiti, ecc.) in modo da garantire un anticipo sui flussi di cassa a istituti di credito che erogano tali finanziamenti.

Capitolo 1
Distributed Ledger Technologies

Distributed Ledger Technology o DLT sono sistemi basati su un **registro distribuito**, ovvero sistemi in cui tutti i nodi di una rete hanno la stessa copia di un database che può essere letto e modificato in modo indipendente dai singoli nodi. (Vella, 2019)

Data la precedente definizione di DLT si potrebbe pensare ad una qualche correlazione ad una forma di Database, quindi è opportuno fare una distinzione tra Distributed Database e Distributed Ledger Technologies:

Distributed Database: in questa tipologia di Base Dati tutti i nodi possono consultare i registri, ma devono essere autorizzati da una o più entità centrali per ottenere permessi di scrittura e quindi modificarlo;
Distributed Ledger Technologies: alla base della regolamentazione di questi registri distribuiti ci sono algoritmi di consenso che regolano le azioni dei singoli nodi e fanno uso della crittografia.

1.1. Caratteristiche e tipologie di DLT

Constatato che le cosiddette DLT sono caratterizzate dalla condivisione di un registro tra i vari nodi del network, le **caratteristiche fondamentali** che distinguono questi sistemi sono tre:

- tipologia di rete
- meccanismo di consenso
- struttura del registro

In base alla tipologia di rete si possono distinguere 2 tipi di sistemi: **Permissionless e Permissioned**

- **Permissionless**: comunemente chiamate *Blockchain* si ispirano al network Bitcoin. Chiunque può partecipare al network e non c' è bisogno di pre-approvazione;
- **Permissioned:** sono dei network simili a dei consorzi in cui occorre registrarsi o essere pre-approvati da una o più entità centrali.

1.2. Blockchain

Come definito nel paragrafo precedente la Blockchain fa parte della famiglia delle DLT di tipo permissionless.
È una tecnologia usata per creare, condividere, modificare e archiviare dati in maniera sicura e trasparente tramite un registro strutturato come una **catena di blocchi contenenti più transazioni,** dove i blocchi sono tra di loro concatenati tramite crittografia. Vi sono poi soluzioni in cui il registro è formato da transazioni che vengono processate in parallelo o altri casi in cui il registro è formato da una catena di transazioni.

I sistemi Blockchain, in genere consentono di **effettuare dei trasferimenti o più genericamente delle transazioni**. Tali trasferimenti possono essere semplici o più evoluti a seconda del livello di programmabilità consentito dalla piattaforma. (Vella, 2019)

La Blockchain, quindi, è un **libro mastro distribuito e immutabile**, cioè chiunque partecipa alla rete ha la copia esatta della blockchain sul proprio nodo.

Essa è come una struttura dati ordinata all'indietro, dove ogni blocco ha al suo interno l'hash[2] del blocco precedente. Il Blocco 'x' avrà un campo che contiene l'hash del blocco precedente *x-1*.
Quindi l'ordine dei blocchi è sequenziale e univoco, non può esserci un blocco uguale ad un altro.

Ovviamente la blockchain pesa in termini di GigaByte, quindi il software scarica i nodi **SPV (Simplified Payment Verification detti anche lightweight clients)**, nodi leggeri, che permettono di scaricare i dati essenziali.
In sostanza, è un raccoglitore di transazioni ordinate temporalmente dove ogni nodo ha un timestamp che marca il momento in cui il blocco entra nella catena.

1.2.1. Caratteristiche Principali

Le caratteristiche della Blockchain sono le seguenti:

- **Decentralizzazione**: le informazioni vengono registrate distribuendole tra più nodi per garantire sicurezza informatica e resilienza dei sistemi;
- **Tracciabilità dei Trasferimenti:** ciascun elemento sul registro è tracciabile in ogni sua parte e se ne può risalire all'esatta provenienza;
- **Disintermediazione**: le piattaforme consentono di gestire le transazioni senza intermediari, ossia senza la presenza di enti centrali;

[2] L'hash è una stringa crittografica digitale che identifica in maniera univoca un determinato set di dati.

- **Trasparenza e Verificabilità**: il contenuto del registro è trasparente e visibile a tutti ed è facilmente consultabile e verificabile;
- **Immutabilità del Registro**: una volta scritti sul registro, i dati non possono essere modificati senza il consenso della rete;
- **Programmabilità dei Trasferimenti**: possibilità di programmare determinate azioni che vengono effettuate al verificarsi di certe condizioni. (Osservatorio Politecnico di Milano, s.d.)

1.2.2. Infrastrutture Centralizzate, Peer-to-Peer e Distribuite

Una infrastruttura centralizzata client/server ha un unico nodo, un unico database e un unico proprietario.
Va senza dire che una infrastruttura di questo tipo è meno resiliente e i nodi partecipano alla rete tramite i server.
Un esempio di infrastruttura centralizzata lo si può notare in figura 1.

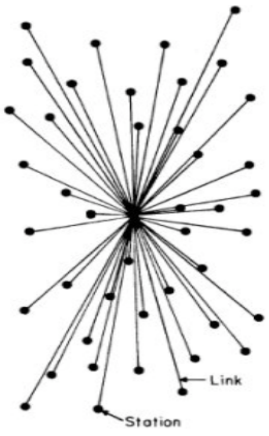

Figura 1: Topografia di una infrastruttura centralizzata

Una infrastruttura decentralizzata, invece, non ha un unico nodo e le varie operazioni sono presenti su più nodi, quindi si può dire che i dati sono immagazzinati su più server.
In figura 2 si può avere un'idea di come è strutturata una infrastruttura decentralizzata.

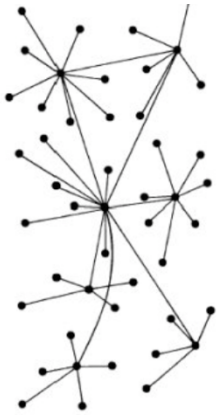

Figura 2: Topografia di una infrastruttura decentralizzata

Una rete P2P è decentralizzata e distribuita, quindi ad alta resilienza e non esiste un unico proprietario essendoci dati replicati su più server. Ci sono più nodi (partecipanti alla rete) tutti di pari privilegi. Una delle caratteristiche principali è quella di essere trustless.
Si può notare in figura 3 come si presenta una rete distribuita.

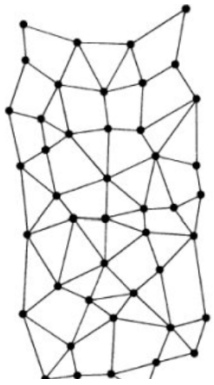

Figura 3: Topografia di una infrastruttura di rete distribuita

La blockchain è decentralizzata e distribuita, ma in qualche modo può essere vista anche con una certa centralizzazione, perchè nel momento in cui raggiunge il consenso emergente si comporta come un unico computer e quindi tutto il network asserisce il fatto che una transazione sia sintatticamente corretta o meno.

Non c'è un ente superiore e non c'è nessun punto di fallimento NPOF (No point of failure).
È a tutti gli effetti un unico computer dove il protocollo, il codice sorgente alla base, è il software della blockchain.
È un insieme di regole che il partecipante alla rete deve rispettare, quindi se si ha un nodo e si vuole fare manualmente una transazione bisogna attenersi a delle regole. Il codice sorgente è open source e si trova su Github[3].

1.2.3. Sicurezza di una Rete P2P

Generalmente la sicurezza di una Blockchain è garantita proprio dall'utilizzo di una rete Peer-to-Peer (P2P) e un Ledger distribuito (*libro mastro*).

Infatti, una rete P2P è una rete basata su un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi, ma anche sotto forma di *nodi equivalenti* o 'paritari' (*peer*), potendo fungere al contempo da client e server verso gli altri nodi terminali (host) della rete. (Wikipedia, s.d.)

[3] https://github.com/bitcoin

Quindi, in una Blockchain ogni peer che partecipa alla rete possiede una copia sincronizzata e completa della blockchain stessa (*Distributed Ledger).* Il Ledger è appunto distribuito e visibile a tutti, non è detenuto da nessuno in particolare né tantomeno da un'unità centrale (Trusted-Third-Party). Ciò garantisce al contempo sia la sicurezza sia l'immutabilità della blockchain. I vari nodi possono entrare e uscire dalla rete P2P, ogni volta che rientrano ricevono una copia del Ledger aggiornata.

Il protocollo però potrebbe essere attaccato. Infatti in termini di sicurezza, un potenziale attaccante dovrebbe quindi guadagnare il consenso di almeno il 51% dei nodi della rete P2P al fine di far accettare come valida la blockchain da lui riprodotta in maniera fraudolenta. I nodi che si trovano in possesso della blockchain falsa saranno quindi in numero ridotto e la blockchain anomala viene scartata. Il sistema, basandosi sulla rete P2P e sul concetto di Ledger pubblico e distribuito, riesce da solo a garantire la propria sicurezza. (Curzi, 2021)

1.2.4. Struttura della Blockchain

La struttura della Blockchain è caratterizzata, come suggerisce il termine stesso, da una catena di blocchi, ciascuno dei quali contiene informazioni differenti e dipendenti dal tipo di blockchain. L'aspetto determinante è che tali informazioni sono vincolate tra loro ed ogni blocco è collegato con il precedente (anche con il successivo). Nell'immagine sottostante (Figura 4) viene illustrato questo concetto; il blocco iniziale della catena viene denominato "blocco di genesi". (Curzi, 2021)

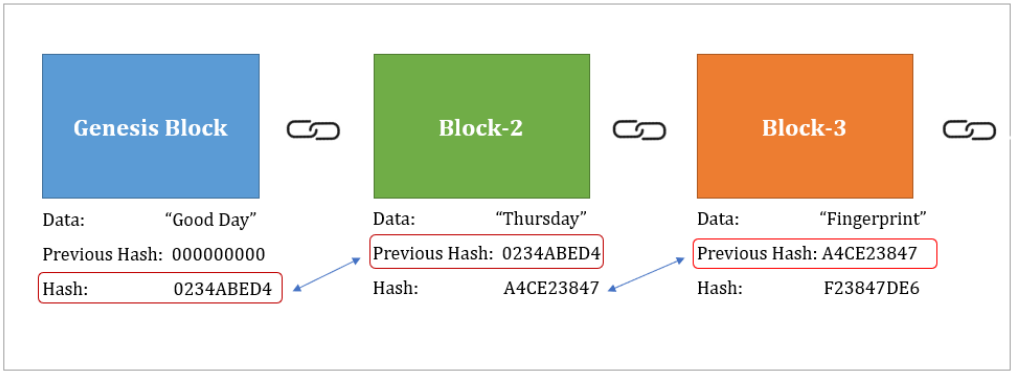

Figura 4: Rappresentazione di una catena di blocchi, sulla sinistra il Blocco di Genesi.

Un blocco di genesi, oltre ad *inizializzare* la blockchain, serve anche a garantire la comunicazione tra due nodi. Questo perché due nodi possono essere accoppiati solo se hanno lo stesso blocco di genesi. Altrimenti entrambi i nodi sarebbero incompatibili. D'altra parte, è importante tenere presente che ogni nodo ha il proprio blocco iniziale, creando una rete enorme in cui un blocco di genesi di maggiore difficoltà non può mai essere sostituito da uno di minore difficoltà. (Bit2Me, s.d.)

È bene definire, quindi, precisamente cosa è un blocco: quando si parla di **blocco** si intende una "pagina" di un libro mastro o di un registro. Ogni volta che un blocco viene "completato", lascia il posto al blocco successivo nella blockchain. Un blocco è quindi un archivio permanente di record che, una volta scritti, non possono essere modificati o rimossi.

1.2.5. Principali ambiti di utilizzo

La Blockchain è una tecnologia molto versatile, infatti può essere applicata in tutti i settori di business. Al giorno d'oggi sono presenti moltissimi casi d'uso aziendali e alcuni di essi verranno approfonditi nel corso dell'elaborato.

Nell'ultimo periodo la blockchain è oggetto di discussione e di studio per comprendere a fondo quali sono i settori che meglio possono sfruttare i benefici e le proprietà di questa tecnologia descritta in precedenza.

Al giorno d'oggi sono diverse le aziende di tutto il mondo che hanno iniziato a sperimentare **soluzioni Blockchain e Distributed Ledger**. Ma continua ad esserci una incertezza di fondo sulle potenziali applicazioni e benefici in ambito industriale.

Il settore più avanzato è sicuramente quello della **Finanza** e delle **Assicurazioni**, che si è attivato per primo per rispondere alla minaccia degli Asset Digitali tanto in voga in questi anni.

Prevalentemente l'applicazione di questa tecnologia è relativa a scambio di valore, verificabilità dei dati, coordinamento dei dati e realizzazione di processi affidabili.

Lo scambio di valore è, forse, il primo vero obiettivo per cui è nata la blockchain, e l'applicazione consiste nell'usare i crypto-asset per **scambiare denaro o altri asset di valore in modo sicuro e disintermediato**. Un esempio in ambito bancario è in particolar modo quello di ***JPM Coin di JP Morgan*** *che ha l'obiettivo di emettere una versione custom del dollaro (stablecoin) per ridurre le lentezze nei pagamenti all'ingrosso transfrontalieri.*

Come si evince dalle caratteristiche intrinseche di una blockchain, ossia l'immutabilità e la trasparenza, una delle varie applicazioni consiste nel registrare su di essa dati o documenti, in modo che queste siano *visibili e verificabili* da altri attori dell'ecosistema o ad attori terzi. Questa pratica

prende il nome di **notarizzazione** e, appunto, ha l'obiettivo di offrire maggiori garanzie all'utente finale sulla tracciabilità e veridicità dei dati.

Per coordinare e condividere i dati si sfruttano i cosiddetti **smart contract**, che verranno analizzati meglio in seguito, per portare on-chain lo scambio di dati. L'obiettivo principale è quello di disintermediare la condivisione di informazioni tra attori diversi evitando eventuali divergenze e conflitti.

La sfida più difficile è rappresentata dall'utilizzo della blockchain per riprogettare i processi di business per garantire l'integrità di ogni singolo processo. Anche in questo caso ci si avvale di smart contract. Uno degli esempi più rilevanti nel panorama finanziario è quello di Banca Santander con l'*emissione di un'obbligazione su Ethereum, coordinando ogni processo sulla blockchain, compresa la gestione dei pagamenti degli interessi maturati utilizzando una stablecoin*[4].

[4] Le Stablecoin sono criptovalute in cui il prezzo è progettato per essere ancorato a una criptovaluta, alla moneta fiat, o a materie prime scambiate in borsa (come i metalli preziosi o industriali).

Capitolo 2
Digital Asset

Una società concettualmente è una rete di individui che interagiscono tra loro. Questa interazione, in un contesto di risorse limitate e di affermazione del concetto di proprietà, è sempre stata caratterizzata dallo scambio di beni e servizi.
Inizialmente questo scambio avveniva tramite il cosiddetto baratto e l'oro era il bene ideale per questo scopo. Infatti l'oro era facile da suddividere, era considerato strumento al portatore e difficilmente censurabile, e per questo è stato usato come 'moneta' sin da subito.
Ovviamente sorgono presto problematiche legate alla facile riconoscibilità, alla difficoltà nel trasportarlo e a stoccaggi presso una terza parte.

Quindi, fu necessario introdurre quella che viene chiamata *moneta fiat* (fiat money), ossia moneta cartacea inconvertibile, generalmente accettata come mezzo di pagamento in quanto dichiarata a corso legale, detto anche forzoso, dallo Stato che la emette, indipendentemente dal suo valore intrinseco. (Treccani, s.d.)
La moneta quindi assume sin da subito un valore di intermediario negli scambi e mezzo di pagamento. Va senza dire che questa condizione fa sì che tutte le problematiche di pagamento relative al baratto vengano superate.
Inoltre, un'altra importante funzione che assume la moneta è quella di strumento numerario. Infatti, attraverso la moneta si iniziano a quantificare costi e ricavi, debiti e crediti e cosi via.

Tuttavia, un sistema di scambio basato su monete metalliche e banconote comporta che acquirente e venditore si debbano trovare nello stesso posto al momento dello scambio.
Questo problema storico della moneta può essere superato con l'avvento di Internet e con la conseguente creazione della cosiddetta *moneta digitale*.
Ma la moneta elettronica presenta un problema noto come *double-spending problem* (Wallace, 2011). Con questa definizione si intende il processo mediante il quale si rende possibile duplicare lo stesso *token* (gettone) e spenderlo due volte (Dwyer, 2014) per acquistare beni.
Questo problema ha due soluzioni possibili: la prima è quella dell'introduzione di una terza parte, un cosiddetto intermediario, che certifica il possesso della moneta e la validità dello scambio bene-servizio; e il secondo modo è quello di creare una infrastruttura decentralizzata governata dalle leggi della crittografia al fine di gestire senza un'autorità centrale la proprietà e i diritti associati ad una moneta digitale.
Di seguito nel prossimo paragrafo verrà analizzato il primo caso di Blockchain, il caso Bitcoin.

2.1. Bitcoin

Verso la fine del 2008, Satoshi Nakamoto[5] pubblica il Whitepaper di Bitcoin. Nasce ufficialmente un nuovo modo per poter trasferire valore basato su una tecnologia completamente nuova, decentralizzata, non censurabile e accessibile a tutti, la Blockchain.
Occorre precisare anche che il periodo storico era caratterizzato da una profonda incertezza a livello economico dovuta alla crisi di liquidità e di solvibilità sia a livello di banche e Stati, sia da una scarsità di credito verso

[5] Satoshi Nakamoto è lo pseudonimo della persona, o del gruppo di persone, che ha inventato la criptovaluta Bitcoin.

le imprese. Quindi l'esordio di Bitcoin rappresenta a tutti gli effetti una sorta di guerra alle istituzioni finanziarie.

Sarebbe opportuno fare qualche passo indietro per comprendere bene cosa ha portato Nakamoto a pubblicare il paper che ha rivoluzionato la concezione del mondo finanziario.

Nel 1989 il crittografo David Lee Chaum[6] pubblica il primo vero protocollo di moneta digitale basato su un sistema di pagamento digitale crittografico, che ha cercato poi di rendere concreto con **DigiCash**. Chaum, però, non riesce a risolvere un problema fondamentale per la riuscita del progetto, quello del double spending che, tra le varie problematiche legate ai finanziamenti necessari, porta al fallimento una decina di anni dopo.

Nel 1997 Adam Back[7] inventa **Hashcash** che è un sistema crittografico di *proof-of-work* utilizzato per limitare lo spam nelle email e gli attacchi denial-of-service.

Subito l'anno dopo grazie a Wei Dai[8] per la prima volta prende vita un sistema di scambio di valore elettronico anonimo e distribuito chiamato **B-Money.**

[6] David Lee Chaum è un informatico e crittografo americano. È conosciuto come un pioniere della crittografia e delle tecnologie per la tutela della privacy e ampiamente riconosciuto come l'inventore del denaro digitale.

[7] Adam Back, noto crittografo britannico, è conosciuto per aver inventato Hashcash, algoritmo che viene utilizzato nel processo di mining di Bitcoin.

[8] Wei Dai è un ingegnere informatico noto per i contributi alla crittografia e alle criptovalute. Tra le varie invenzioni è il creatore del sistema di criptovaluta **b-money**. La più piccola subunità di Ether, il wei, prende il nome da lui.

Nel 1998 Nick Szabo[9] crea una valuta virtuale chiamata "**Bit Gold**". Questo progetto non riscuote molto successo ma introduce concretamente il concetto di proof of work e il concetto di chain che lega la verifica di ogni transazione alla successiva. Inoltre, definisce gli smart contract come protocolli di transazione computerizzati che eseguono i termini di un contratto rendendo le transazioni tracciabili, trasparenti e irreversibili.

Infine, nel 2004 Hal Finney[10], un noto professore di crittografia, inventò sulla base del lavoro di Adam Back la **Reusable Proofs of Work**, un sistema centralizzato di pagamento la cui moneta basava le sue caratteristiche su un protocollo in grado di verificare, grazie ad una prova crittografica, che un computer avesse speso una certa quantità di risorse computazionali. La prova non era nient'altro che la soluzione di un puzzle crittografico costoso e difficile da risolvere ma facilmente verificabile. (Mione, 2017)

Quindi la bravura di Satoshi Nakamoto risiede nell'aver saputo mettere insieme nozioni, algoritmi e sperimentazioni dei crittografi sopra citati.
Ed ecco che Nakamoto con Bitcoin risolve il problema della spesa-doppia grazie all'utilizzo di un network peer-to-peer distribuito, che attribuisce un timestamp sulle transazioni registrate in blocchi generando una prova computazionale dell'ordine cronologico degli stessi, la proof-of-work (Nakamoto, 2008).

[9] Nicholas "Nick" Szabo è uno scienziato informatico, giurista e crittografo noto per le sue ricerche sui contratti digitali e le valute digitali.

[10] Harold Thomas Finney II era uno sviluppatore americano. È stato la prima persona a eseguire il software Bitcoin dopo Satoshi Nakamoto.

Il concetto di proof-of-work, come anticipato, consiste in un meccanismo in grado di coniare moneta risolvendo un problema crittografico e affrontando così dei costi reali dovuti al consumo di energia della CPU.

I primi giorni del Gennaio 2009, viene minato il primo blocco di Bitcoin da Hal Finney.

Figura 5: Screenshot rappresentante il tweet di Hal Finney riguardante l'esecuzione del software Bitcoin per la prima volta.

2.1.1. Il concetto di Halving

Quando venne pubblicato il protocollo la Blockchain di Bitcoin non esisteva. Infatti, il primo blocco venne creato, *minandolo*, esattamente il 3 Gennaio del 2009.
Questa fu esattamente la volontà di Nakamoto: il suo intento era quello di far creare i Bitcoin (BTC) al protocollo stesso, donandoli come premio ai miner che riuscivano a minare un blocco.
Si era previsto, infatti, che venisse minato all'incirca 1 blocco ogni 10 minuti, e dal momento in cui Satoshi decise che questo premio sarebbe stato di 50 BTC a blocco, ogni giorno venivano creati circa 7.200 BTC.
E fu così che, a fine 2009, vennero creati più di 1,6 milioni di BTC. L'obiettivo iniziale era di 2,6 milioni, ma il ritmo con cui venivano minati i blocchi all'epoca era un po' più lento dell'attuale.

Ma se questo ritmo fosse rimasto costante, bitcoin non sarebbe mai diventato un bene scarso, ed infatti Satoshi decise che, proprio per rendere nel corso del tempo bitcoin un bene scarso, ogni 210.000 blocchi minati il premio sarebbe stato dimezzato.
Questo fenomeno è definito nel protocollo in sé e prende il nome di **halving.**
Dal momento in cui che questa impostazione è nativa, ed inserita direttamente a livello di codice, non è virtualmente modificabile, se non con un eventuale accordo della maggioranza degli utilizzatori del protocollo ed infatti non è mai stata modificata.

Per minare 210.000 blocchi al ritmo di un blocco ogni 10 minuti, occorrono circa poco meno di 4 anni, tanto che di halving ne sono già stati eseguiti tre: uno a novembre 2012, che portò il premio per i miner a 25 BTC per blocco minato, uno a luglio 2016, che lo portò a 12,5 e uno a maggio 2020 che lo portò a 6,25 BTC.

Il quarto avverrà inevitabilmente tra altri 210.000 blocchi, presumibilmente nella prima parte del 2024.
Procedendo in questo modo si riduce la creazione di nuovi BTC fino a che un giorno non se ne creeranno più.
L'obiettivo di questa politica monetaria è la cosiddetta **natura deflattiva**, ovvero creare una moneta la cui massa circolante non continui ad aumentare per sempre, come accade invece per le tradizionali valute fiat, ma che ad un certo punto inizi ad aumentare molto lentamente, fino a fermarsi.
Per esempio con il terzo halving, sono stati creati solamente 6,25 BTC ogni circa 10 minuti (900 al giorno), quindi l'inflazione della massa monetaria di bitcoin è scesa sotto all'1,8%, iniziando ad avvicinare questa moneta all'obiettivo di diventare una moneta deflattiva.

Dopo il terzo halving, la massa monetaria di bitcoin continuerà ad aumentare, ma molto lentamente, ciò farà crescere in modo significativo la sua scarsità**.**

Nel 2020 lo **Stock to Flow Ratio** di bitcoin, che misura il rapporto tra scorte e produzione, era già maggiore rispetto a quello dell'argento e attualmente è simile a quello dell'oro.
Si prospetta che già a partire dal 2022 lo Stock to Flow Ratio di bitcoin supererà anche quello dell'oro, diventando pertanto ancora più scarso sui mercati del prezioso metallo. (Cavicchioli, 2020)

2.1.2. Blocchi, Nodi e altri concetti chiave

Prima di proseguire è utile definire cosa e quali sono gli elementi che caratterizzano il funzionamento di Bitcoin.

Blocchi

Un blocco è come una pagina di un libro mastro o di un registro. Ogni volta che un blocco viene "completato", lascia il posto al blocco successivo nella blockchain. Un blocco si può quindi definire un archivio permanente di record che, una volta scritti, non possono essere modificati o rimossi. (KamilTaylan.blog, 2021)

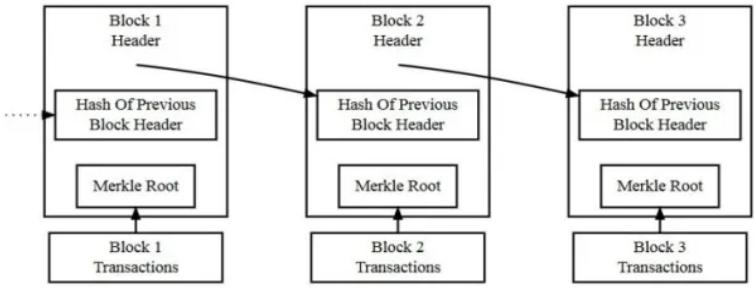

Figura 6: Rappresentazione della struttura dei blocchi caratterizzanti il protocollo Bitcoin

Nello specifico un blocco è composto da un *header* e da un *body*. Le transazioni sono racchiuse nel *body* del blocco e nell'*header* sono presenti sette campi di gestione del blocco stesso tra cui la versione, il timestamp, il Prev hash del blocco precedente, il Merkle root, il campo Bits, il nonce e il numero di transazione. (Alessi, s.d.)

- La *versione* è l'informazione relativa al protocollo utilizzato;
- Il *timestamp* è un piccolo dato memorizzato in ogni blocco come seriale univoco e la cui funzione principale è quella di determinare il momento esatto in cui il blocco è stato minato e convalidato dalla rete blockchain; (Casaburi, 2022)
- l'hash del blocco precedente è una funzione hash crittografica che genera una firma a 256 bit per identificare il blocco precedente;
- il *Merkle root* è l'*hash* di tutti gli *hash* di tutte le transazioni nel blocco, ossia è l'albero binario che identifica tutte le transazioni effettuate;
- il campo Bits si riferisce al numero di bit che si trovano all'interno di un bitcoin. Identifica la misura del blocco in byte e riflette il limite massimo in cui un blocco può includere transazioni; (Bit2Me, s.d.)
- il nonce è un valore a 8 byte che viene aggiunto al blocco in modo che l'output della funzione di *hash* cambi facendo in modo che risulti inferiore al valore *Bits* corrente, il valore viene ricalcolato

finché l'*hash* del blocco non contiene il richiesto numero di zeri principali. (Alessi, s.d.)

```
bitcoin@raspberrypi:/home/pi $ bitcoin-cli getblock
00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048 | jq
{
  "hash": "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048",
  "confirmations": 674337,
  "strippedsize": 215,
  "size": 215,
  "weight": 860,
  "height": 1,
  "version": 1,
  "versionHex": "00000001",
  "merkleroot": "0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098",
  "tx": [
    "0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098"
  ],
  "time": 1231469665,
  "mediantime": 1231469665,
  "nonce": 2573394689,
  "bits": "1d00ffff",
  "difficulty": 1,
  "chainwork": "0000000000000000000000000000000000000000000000000200020002",
  "nTx": 1,
  "previousblockhash":
"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "nextblockhash":
"000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddbd"
```

Figura 7: Esempio concreto di struttura e contenuto di un blocco tramite Bash

Nodi

Nel protocollo Bitcoin sono presenti due attori: il *nodo* e il *miner*. Il **nodo** ha la blockchain in locale e verifica le transazioni sintatticamente (verifica la firma) ma non mina, e non ha nessun incentivo a verificare le transazioni. Invece, il **miner** oltre a verificare la transazione ha anche la funzione di minare i blocchi in cambio di un *reward*.

In sostanza ci sono i seguenti nodi nel network:

- I **Full Node** sono quelli che applicano tutte le regole del protocollo Bitcoin e, quindi, sono quelli che forniscono robustezza, sicurezza e stabilità alla rete

- I **Miner Node,** come suggerisce il nome, sono quei full node che, oltre a memorizzare una copia completa della blockchain, eseguono anche l'algoritmo di mining

Si può dire quindi che i *full node controllano, i miners creano.* Infatti, i full node controllano le transazioni che hanno nella memory pool o transaction pool che è un contenitore di transazioni valide ma non minate. Per comprendere bene quanto espresso basta utilizzare un explorer, come Bitcoin Explorer[11], prendendo una transazione in maniera casuale nella transaction pool.

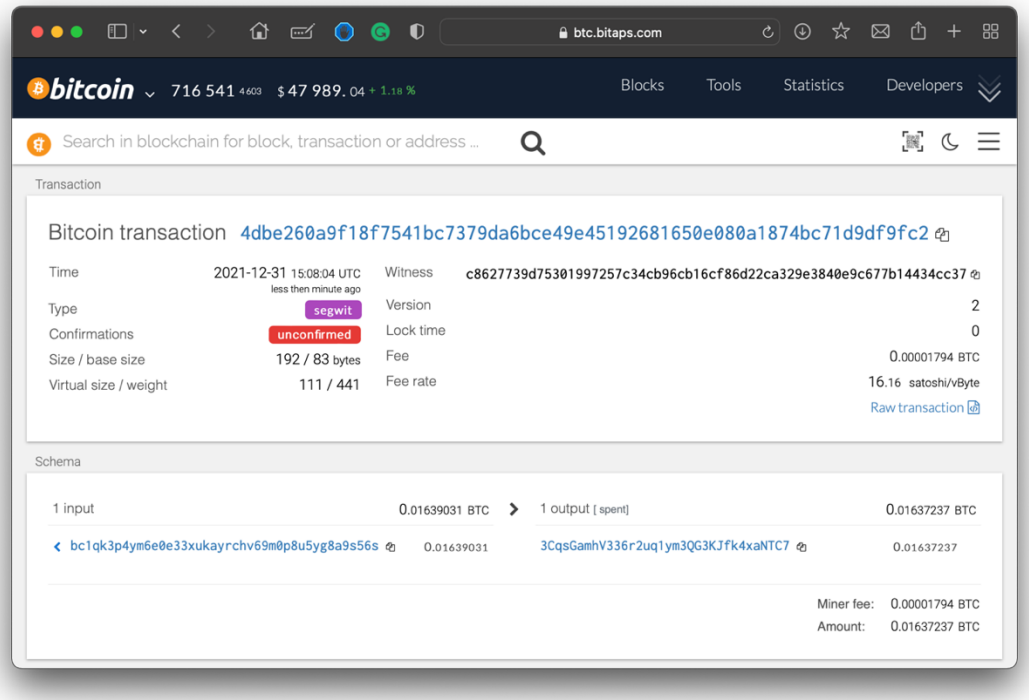

Figura 8: Rappresentazione analitica di una transazione casuale su Bitcoin Explorer.

Come si può notare nell'immagine (Figura 8) è indicato che la transazione è *unconfirmed.*

[11] https://btc.bitaps.com

Questo vuol dire che è valida, ma è in attesa di essere verificata dai full node.
Il momento in cui il miner va a prendere le transazioni che vuole includere nel proprio blocco, propone al network un cosiddetto **blocco candidato** o **candidate block**.

Miners e Processo di Mining

I **miners** sono una parte fondamentale di Bitcoin e sono coloro che si occupano della sicurezza della rete. Più miners sono presenti nel network più competizione c'è, più aumenta la difficoltà, più aumenta l'hashrate e più la rete si fortifica. E soprattutto sostengono la decentralizzazione.

Come illustrato precedentemente ogni 4 anni il premio per il miner si dimezza e questo fenomeno si chiama halving (vd. Paragrafo 2.1.1.). Nel protocollo c'è scritto che il massimo numero di blocchi sarà 210k.
Sono previsti solo 64 halving in Bitcoin e dopo l'ultimo il reward sarà pari a 0.

Il miner per eseguire la PoW ha una spesa in termini di hardware, PC con alta potenza di calcolo e GPU ottimizzati nell'eseguire SHA256 per risolvere l'hash del blocco.
Ovviamente più hash si creano in poco tempo e meglio è, ma è ovvio che per fare ciò occorre più energia, e più energia si consuma più si spende.
Il processo continua fin quando il reward copre quanto meno le spese sostenute.
Dopo il 64° halving il reward è 0, ma il miner continuerebbe a farlo per le *fees,* ossia le commissioni che gli utenti pagano e quindi ogni volta che un miner mina un blocco il reward è la somma delle fees.

Quindi si presume, e si spera, che il valore di Bitcoin salga sempre più in modo da reggere e alimentare questo criterio.

Il reward precisamente è la **coinbase,** ossia è la somma della ricompensa del block mining più le commissioni delle transazioni elaborate. Viene generalmente posizionata come prima transazione aggiunta all'interno di un nuovo blocco che il miner ha creato e ovviamente quella transazione deve essere sintatticamente corretta. Il miner prende di riferimento l'ultimo blocco, trova una soluzione e propone un candidate block da integrare nella pool, se la soluzione è corretta vince il reward altrimenti riparte da capo.

Transazioni

Una transazione è un trasferimento di un valore tra due parti. In Bitcoin, queste transazioni sono un flusso di informazioni che avviene tra i nodi del network. Si può dire quindi che esse siano semplici messaggi programmabili e **firmati digitalmente** attraverso la crittografia e inviati all'intera rete per la convalida.

La firma digitale viene usata nella transazione che è una sequenza di caratteri esadecimali chiamata anche **transaction data** che viene inviata in **broadcast** sulla rete e tutti i nodi devono verificare se è veritiera (**Gossip Protocol**).

La firma digitale consiste nell'applicazione della crittografia asimmetrica basata su chiave pubblica e chiave privata. Precisamente viene associata una chiave privata ad un messaggio e viene creata una chiave pubblica per identificare un nodo.

Quindi la chiave privata viene usata per la firma digitale e deve rimanere sempre segreta; invece, la chiave pubblica si può derivare.
Dalla chiave pubblica si può verificare effettivamente che un nodo abbia firmato o meno una transazione.
In conclusione si può dire che la chiave pubblica è l'address (equivalente dell'IBAN per un conto corrente) e la chiave privata è considerabile un PIN.
La chiave privata serve a risolvere il **non ripudio,** ossia, non si può disconoscere di aver fatto una firma.

Le transazioni sono composte da quattro elementi elencati e spiegati di seguito:

- **Entrate (inputs):** questo campo si riferisce ad un ammontare che si desidera trasferire e grazie ai dettagli contenuti negli input è possibile confermare l'origine degli asset che verranno utilizzati in una transazione e sono quelle che contengono l'indirizzo dove sono stati originariamente ricevuti i bitcoin.
- **Uscite (output):** qui viene definito l'address al quale viene inviato l'importo. Una transazione può contenere più di un output.
- **Identificatore (TXid):** questo elemento rappresenta la chiave unica ed irripetibile che identifica una transazione nella blockchain. Sarà composta da un hash ricavato dagli input e dagli output
- **Tasso di commissione (fee):** è il pagamento che i miners ricevono per l'elaborazione di una transazione. Dal momento in cui il miner che riceverà la fee non è noto a priori, le transazioni sono caratterizzate da una piccola commissione per il miner che minerà quel blocco.

Ci sono due tipi di transazioni esistenti in Bitcoin: la coinbase e le UTXO.

Una transazione **coinbase**, come descritto in precedenza, è quella che consente ai miners di generare o attivare nuove monete con cui possono ricevere i premi del mining.

Gli UTXO, Unspent Transaction Output, sono monete non spese. In particolare, in Bitcoin, gli input delle transazioni vengono chiamate anche UTXO di una transazione precedente, ossia l'output di una transazione non utilizzato. Si può dire semplicemente che l'UTXO sia il resto prodotto da una transazione.

2.1.3. Proof of work

Il concetto di Proof of Work, creato da Adam Back nel 1*997,* non è nient'altro che un problema matematico che consiste nel trovare i parametri che restituiscono un certo risultato. La particolarità di questo risultato è che si tratta di un *hash*, di cui è impossibile conoscerne i parametri iniziali, i quali possono essere generati solo attraverso tentativi casuali ed errori.

Questo meccanismo serve a garantire la sicurezza della blockchain perché rallenta la creazione di nuovi blocchi e viene utilizzata come algoritmo di consenso nella maggior parte delle criptovalute.

La Proof of Work prevede che un *miner* utilizzi potenza computazionale per generare l'*hash* dei dati del blocco fino a quando non viene trovata una soluzione al problema.
Nella PoW il miner deve fornire dati il cui hash corrisponda a determinate condizioni senza sapere come arrivarci. Per creare un nuovo blocco, e quindi ottenere questo hash, il miner deve avere a disposizione l'header e il *merkle root* dal quale si può capire quali transazioni sono inserite nel

blocco in quanto albero binario dello storico delle transazioni. Queste informazioni rimarranno invariate, infatti la vera difficoltà nel dimostrare il lavoro svolto sta nel trovare il *nonce* e l'unico modo che ha a disposizione per trovarlo è tirare ad indovinare fin quando l'hash creato non sia al di sotto di un valore prefissato dal protocollo.
Quando il miner ottiene il nonce corretto i nodi della rete controllano che quello che ha fatto è sintatticamente corretto. Se è corretto, il blocco diventa il **tip,** cioè il blocco più alto della catena.
Successivamente il blocco viene proposto e c'è una votazione fatta dai partecipanti della rete alla fine della quale si raggiunge un consenso emergente proprio perché emerge da vari nodi.
Quindi i nodi verificano il lavoro del miner, verificando la sintassi del blocco.
Il calcolo dello SHA256 è difficile, e bisogna fare tante prove per trovare l'hash adatto.

Inoltre, secondo il protocollo ogni blocco può essere minato ogni 10 minuti e valgono le seguenti regole:

- Non è possibile scegliere l'input
- Non può esserci collisione

Dal momento che ogni blocco può essere minato ogni 10 minuti è bene definire cosa è l'**Hashrate,** ossia, la potenza di calcolo che la rete può creare. Quindi l'hashrate varia a seconda di quanti miner sono presenti nel network.

Satoshi Nakamoto nel protocollo ha stabilito la difficoltà, cioè un limite di 2016 blocchi (2 settimane circa).

Ovviamente più persone provano a trovare la soluzione, più aumenta l'hashrate e più aumenta la difficoltà.
In conclusione, la Proof of Work è computazionalmente onerosa da effettuare perché è impossibile invertire un hash del blocco per ottenere i dati di input. Al contrario, conoscendo l'input, è semplice confermare che l'hash sia corretto. Occorre solo elaborare l'input attraverso la funzione e verificare che l'output sia lo stesso.

2.2. Ethereum

Dopo l'avvento rivoluzionario di Bitcoin, un giovane Vitalik Buterin il 28 Dicembre del 2013 propose tramite un Blog Post[12] alla comunità di Bitcoin di integrare un linguaggio di programmazione su protocollo.

Sul Blog, Buterin introduce per la prima volta *Ethereum: The Ultimate Smart Contract and Decentralized Application Platform* dove descrive l'idea di una blockchain Turing-completa[13] decentralizzata in grado, con il tempo e le risorse sufficienti, di eseguire qualsiasi tipo di applicazione. (Buterin, 2014)

Nel 2014 fonda la Ethereum Foundation e l'anno successivo ci sarà quella che viene chiamata Initial Coin Offering o ICO dove vennero raccolti circa 31.500 BTC, che corrispondevano a circa $18.450.000 per l'epoca.

[12] https://web.archive.org/web/20131228111141/https://vbuterin.com/ethereum.html
[13] Turing Complete si riferisce a una macchina che, dato abbastanza tempo e memoria insieme alle istruzioni necessarie, può risolvere qualsiasi problema computazionale, non importa quanto complesso. Il termine è normalmente usato per descrivere i moderni linguaggi di programmazione, poiché la maggior parte di essi sono Turing Complete (C++, Python, JavaScript, ecc.).

Per alcuni aspetti l'Initial Coin Offering (ICO) è assimilato al Crowdfunding.

Alcuni vantaggi sono i seguenti:

- portare valore in tempi strettissimi
- costi di attuazione e implementazione relativamente bassi.

La proposta di valore della blockchain di Ethereum è che è una piattaforma open source decentralizzata Blockchain-based, nata con l'obiettivo di creare un protocollo alternativo per la creazione di applicazioni decentralizzate (dApps).

Quindi l'idea alla base del protocollo Ethereum è che, oltre a scambiare moneta (Ether o ETH), gli sviluppatori possono creare e implementare codice che viene eseguito su reti distribuite, invece di esistere su un server centralizzato.

Queste applicazioni che si possono implementare su Ethereum vengono chiamate Smart Contract.

2.2.1. Ether

Esattamente come in Bitcoin, di cui alla base c'è l'asset nativo bitcoin o BTC, anche in Ethereum è presente un asset nativo chiamato ether o ETH. Analogamente al protocollo Bitcoin, in Ethereum è presente un processo di mining attraverso attraverso il quale vengono generati ether come compenso per i miner.

Una particolarità di questo protocollo di seconda generazione risiede proprio nella total supply dell'asset nativo.
Mentre per Bitcoin fu previsto un numero ben definito di token per definirne la scarsità e per definirne le modalità e le tempistiche di emissione (vd. Paragrafo 2.1.1.), per Ethereum questo rimane un punto aperto. Questo perché l'obiettivo per cui nasce il protocollo è quello di garantire la creazione, e il conseguente funzionamento, di applicazioni decentralizzate e quindi non si è stati ancora in grado di definire un programma di emissione di ether adatto a questo scopo. Nell'immagine che si trova di seguito (Figura 9) si può notare che al 1° Gennaio del 2022 l'emissione totale ammonta a circa 119 milioni di ether.

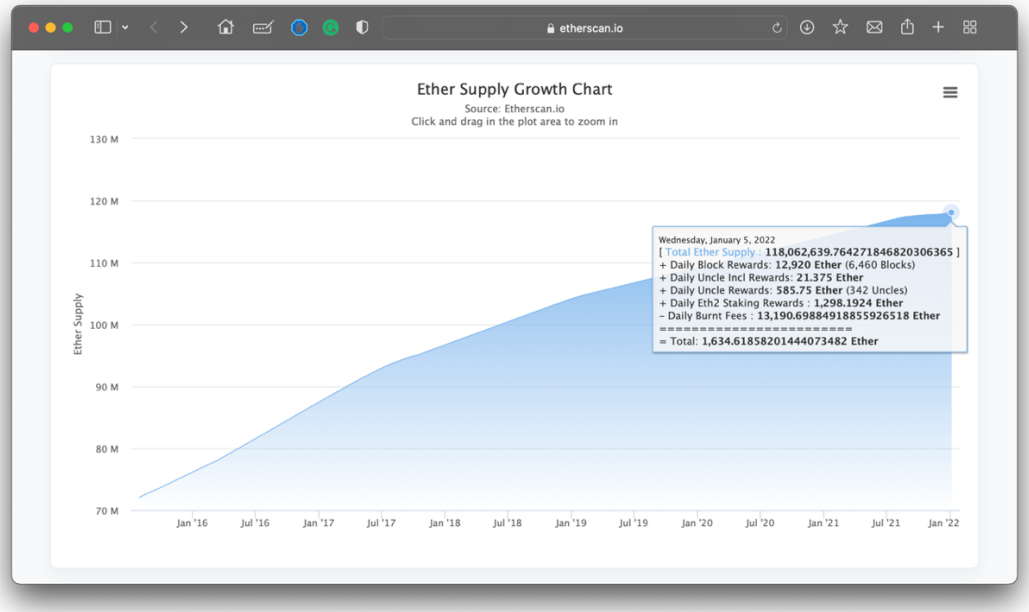

Figura 9: Rappresentazione grafica della Total Supply di Ether [Fonte etherscan.io]

2.2.2. Smart Contract

Gli Smart Contract eseguiti su Ethereum vengono attivati da transazioni. Quando un utente invia una transazione a un contratto, ogni nodo sul network esegue il codice del contratto e registra l'output. Per far questo si avvale della *Ethereum Virtual Machine (EVM)*, che converte gli smart contract in linguaggio macchina. (Binance Academy, 2020)

Quindi, uno *smart contract* non è nient'altro che un codice. Infatti, il termine "smart" viene usato impropriamente in quanto questo codice non è né intelligente, né un contratto nel senso tradizionale. Viene chiamato smart perché viene eseguito secondo determinate condizioni, e viene considerato un contratto in quanto regola dei rapporti fra i partecipanti di un network.

Come anticipato nel corso dell'elaborato, la concettualizzazione di quello che oggi viene chiamato Smart Contract è stata proposta dall'informatico Nick Szabo nel 1998. Egli usò l'esempio di un distributore automatico che per erogare un prodotto, quindi per eseguire il contratto, aveva bisogno di una moneta.
Uno Smart Contract applica esattamente questo tipo di logica, ma in un contesto digitale. Il paradigma con il quale vengono definiti è **IFTTT** (If This Then That).

Gli Smart Contract vengono eseguiti sulla **EVM** (Ethereum Virtual Machine) e sono programmati nella maggior parte in Solidity o Vyper.
Esso vengono azionati da una transazione e per poterli usare bisogna pagare delle commissioni di transazione in Ether, le cosiddette Gas fee.

2.2.3. Gas Fee

Il Gas è il carburante della rete Ethereum. È l'unità di misura per definire l'ammontare di computazione che viene richiesta alla rete. Sostanzialmente senza le Gas Fee non possono essere eseguiti gli Smart Contract.

Per ogni transazione è prevista una gas fee fissa, ma la quantità di gas di cui hai bisogno uno Smart Contract è direttamente proporzionale alla *complessità* dello Smart Contract stesso.

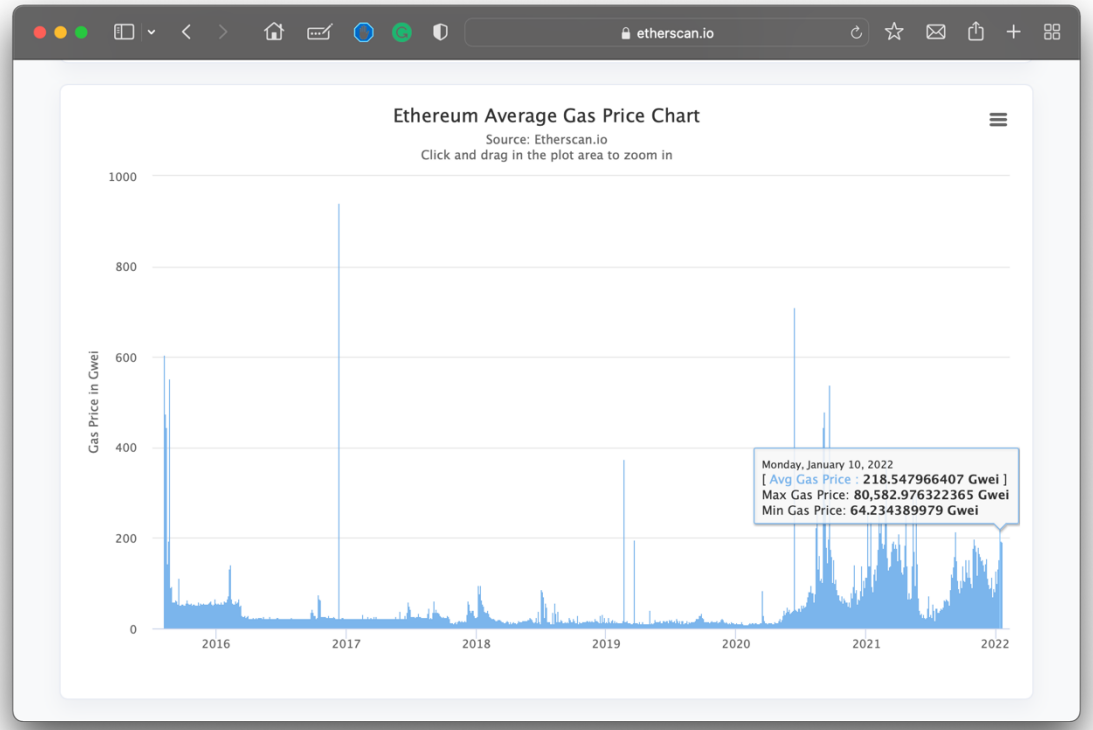

Figura 10: Prezzo medio del Gas al 10 Gennaio 2022, [fonte etherscan.io]

Generalmente, il gas costa una frazione di ether. Quindi viene usata un'unità più piccola quale il gwei. Si illustra nella tabella di seguito (Tabella 1) il valore di conversione gas-ether.

Un gwei corrisponde a un miliardesimo di un ether.

Unit	Wei Value	Wei	Ether Value
Wei	1 wei	1	10-18 ETH
Kwei	10^3 wei	1,000	10-15 ETH
Mwei	10^6 wei	1,000,000	10-12 ETH
Gwei	10^9 wei	1,000,000,000	10-9 ETH
Microether	10^{12} wei	1,000,000,000,000	10-6 ETH
Milliether	10^{15} wei	1,000,000,000,000,000	10-3 ETH
Ether	10^{18} wei	1,000,000,000,000,000,000	1 ETH

Tabella 1: Scala delle unità di conversione del valore della criptovaluta Ether

Complessivamente si può dire che il Gas contribuisce alla sicurezza della rete al fine di:

- prevenire loop infiniti accidentali o sprechi computazionali nel codice;
- evitare attacchi di SPAM;
- incentivare i miner a inserire i blocchi nella catena.

Un altro concetto rilevante sulle gas fee è il **Gas Limit**, ossia, una soglia massima di gas che si vuole pagare per eseguire uno smart contract. Questo perché c'è la possibilità che la quantità di gas necessaria per minare un blocco possa aumentare e definendo un limite si dichiara esplicitamente che al di sopra di quella soglia la transazione debba essere interrotta in modo che chi commissiona la transazione non paghi più di quanto ha indicato inizialmente.

Il prezzo del Gas è sottoposto alle leggi del mercato, quindi è variabile; più è alto il volume di transazioni, più la rete si congestiona, più il Gas Price sarà alto.

In conclusione il prezzo del gas rappresenta la velocità con cui i miner includeranno la transazione nella catena, e il limite di gas definisce la quantità massima che si è disposti a pagare. (Binance Academy, 2020)

2.2.4. Meccanismo di Consenso

Attualmente Ethereum utilizza, come Bitcoin, un meccanismo di consenso Proof of Work (PoW).
La PoW è caratterizzata, come definito nei capitoli precedenti, da nodi, che competono per creare ed aggiungere nuovi blocchi contenenti transazioni alla blockchain. Il vincitore condivide il nuovo blocco con il resto della rete e guadagna una percentuale di ETH appena minati. La gara viene vinta dal computer che riesce a risolvere più velocemente un rompicapo matematico: sostanzialmente questa risoluzione produce il collegamento crittografico tra il blocco corrente e il blocco che lo ha preceduto. (Ethereum, 2021)

Questo meccanismo ha come principali svantaggi i costi elevati e il rischio di attacco 51%, ma soprattutto la bassa scalabilità.
Ecco perché nella rete Ethereum è presente da tempo una proposta di transizione verso l'adozione di un meccanismo di consenso diverso, la Proof of Stake.
Quest'ultimo è stato introdotto nel 2011 con l'obiettivo di risolvere i problemi del sistema attualmente più diffuso, la Proof of Work, ma arrivare alla PoS è una sfida tecnica complessa e non è semplice come utilizzare la PoW per ottenere consenso in tutta la rete. (Binance Academy, 2018)

A differenza del PoW, l'algoritmo Proof Of Stake è caratterizzato da **validatori** che vengono scelti in maniera casuale per creare nuovi blocchi, condividerli con la rete e ottenere delle ricompense in ETH.
Per diventare validatore, a differenza della PoW, non è richiesta una potenza elevata di calcolo, ma bensì fare *stake* con gli ETH di cui si dispone nella rete. Il premio per il validatore invece non è la creazione di una nuova moneta, ma le commissioni sulle transazioni.

È opportuno precisare che in questo algoritmo di consenso il processo attraverso il quale viene aggiunto un blocco alla catena non è chiamato processo di mining, ma bensì processo di forging. Quindi si potrebbe dire che il blocco viene letteralmente forgiato.

I nodi che vogliono partecipare al processo di forging, e quindi diventare validatori, devono impegnare una certa somma di monete all'interno del network, precisamente 32 ETH, letteralmente 'puntando' o 'mettendo in gioco' quell'ammontare di monete (in inglese at stake).

Più è alto il quantitativo di monete che si mettono in stake, maggiore è la possibilità di essere selezionato come validatore e agire da forger del blocco successivo. Ma dal momento in cui questo processo potrebbe favorire solo i nodi che detengono più ETH, sono stati implementati processi di selezione casuale. I più noti sono **Randomised Block Selection** e **Coin Age Selection**. (Binance Academy, 2018)

Nel primo caso i validatori vengono selezionati cercando i nodi con una combinazione tra valore hash più basso e stake più grande. Dal momento che tutte le informazioni dei nodi, e dei rispettivi stake, sono pubbliche si possono fare anche previsioni sul potenziale nodo che verrà selezionato.

Il metodo Coin Age Selection, invece, come suggerisce il nome stesso sceglie nodi in base al tempo in cui i token sono stati impegnati nello stake. Questo calcolo avviene moltiplicando il numero di giorni per il numero di monete congelate. Quando un nodo forgia un blocco, la sua coin age viene resettata a zero e deve aspettare un certo periodo di tempo prima di poter essere selezionato. Questo meccanismo di reset impedisce ai nodi con grandi quantità di monete in stake di dominare la blockchain.

Il validatore del blocco successivo, esattamente come il nodo Miner in Bitcoin, deve verificare se le transazioni in esso contenute sono valide, firmare il blocco e aggiungerlo alla blockchain. Come ricompensa, il nodo riceve le commissioni associate alle transazioni nel blocco. (Binance Academy, 2018)

Ma qualora il validatore volesse accedere alle ricompense e al suo staking, e quindi smettere di partecipare al processo di forging, è previsto un periodo di attesa in cui il network controlla e verifica che nel suo periodo di attività non abbia aggiunto blocchi fraudolenti alla blockchain.

In sostanza, il funzionamento di questo meccanismo è garantito dallo stake stesso, perché il validatore è incentivato ad essere corretto nell'attestare che i blocchi siano sintatticamente corretti in quanto qualora il network individuasse un tentativo di frode il nodo forger perderebbe una parte del suo stake.
Quindi quello che si può perdere è, in ogni caso maggiore di quanto si può guadagnare.

Dal punto di vista della sicurezza l'algoritmo è sempre vulnerabile al **51% attack,** ma riuscire a raggiungere un controllo del 51% del network e approvare transazioni fraudolente, quindi possedere una stake

maggioritaria, resta un attacco quasi irrealizzabile dal momento in cui per ottenere il controllo del network sarebbe necessario acquisire il 51% delle unità in circolazione.

Come si può notare dal grafico a torta (Figura 10), il 51% delle unità in circolazione al 16/01/2022 è 60,215,240.69 ETH.

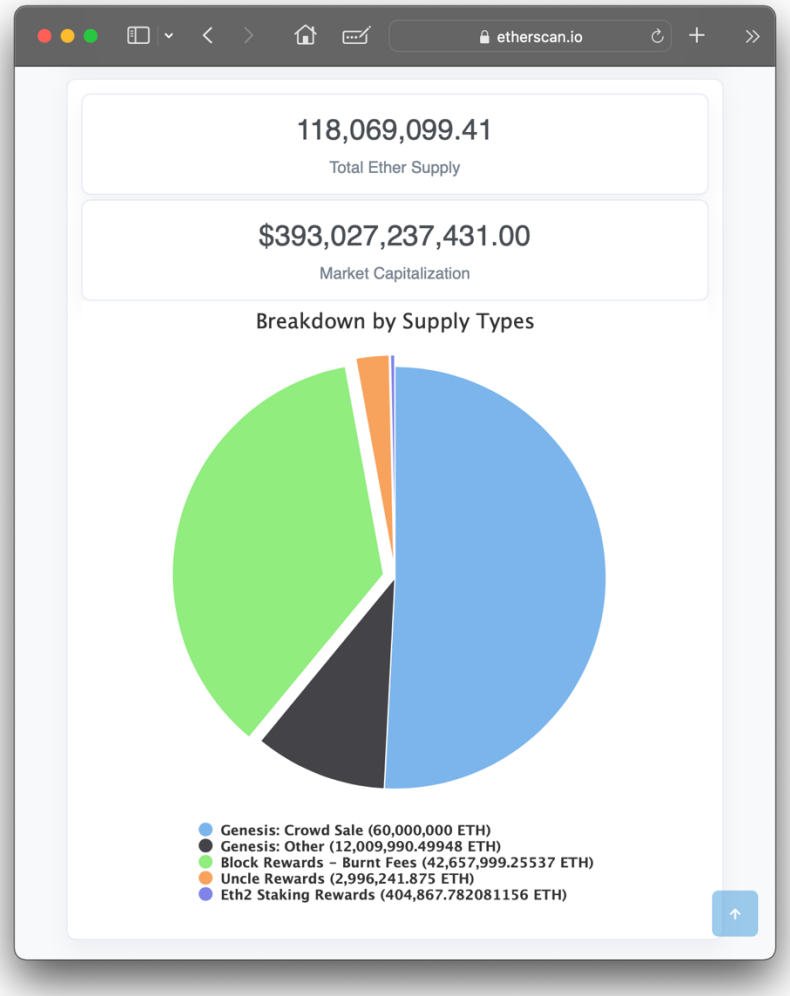

Figura 11: Rappresentazione grafica della quantità totale di Ether emesse a Gennaio 2022, [fonte etherscan.io]

La Proof of Stake, rispetto a PoW, offre tre principali vantaggi:

- migliore efficienza energetica per creare nuovi blocchi;
- minori barriere all'ingresso, perché non è necessaria un'elevata potenza di calcolo;

- maggiore garanzia alla decentralizzazione, garantendo un maggior numero di nodi.

2.2.5. Ethereum 2.0

L'obiettivo di Ethereum è quello di diventare un *computer globale* a supporto del sistema finanziario, ma attualmente il rate di transazioni per secondo (TPS) ammonta a 10 transazioni al secondo. Va da sè che è un rate molto basso e, pertanto, non sarebbe in grado di aiutare a raggiungere l'obiettivo.
Ecco perché è in atto la transizione verso una rete nominata Ethereum 2.0 in grado di incrementare la decentralizzazione, migliorare l'efficienza e rendere più scalabile la rete aumentando soprattutto la quantità di transazioni al secondo.

In Ethereum oggi ogni nodo possiede una copia della blockchain in locale e ogni volta che viene aggiunto un blocco devono impiegare risorse computazionali per scaricarne una copia aggiornata.
Tra i vari aggiornamenti proposti in Ethereum 2.0, uno di questi risolverebbe proprio questo problema dell'uso intensivo di banda larga e memoria, lo **sharding**.

Il processo di sharding consiste nel dividere il network in sottoinsiemi di nodi chiamati, appunto, shard. Ognuno di questi shard elaborerà in autonomia le proprie transazioni e smart contract, e allo stesso tempo comunicherà con gli altri shard del network. Dal momento in cui ogni shard convalida in maniera indipendente, non è più necessario conservare i dati da altri shard.
Praticamente questi shard possono essere considerati come delle vere e proprie blockchain separate, in cui i validatori si troveranno ad elaborare

transazioni e creare nuovi blocchi. Attualmente sono previste 64 shard chain che avranno una comprensione condivisa dello stato della rete.
Questo ovviamente comporterebbe un coordinamento maggiore a livello di infrastruttura, e per questo è stato ipotizzato di implementare una **beacon chain**[14] .
La beacon chain riceve informazioni sullo stato dagli shard e le rende disponibili ad altri shard, in modo che la rete possa rimanere sincronizzata. La beacon chain gestirà anche i validatori, dalla registrazione dei depositi di stake fino all'emissione delle ricompense o delle eventuali penalità. (Ethereum, 2022)

Quindi riassumendo, alla base della futura Ethereum 2.0 ci sarà una infrastruttura chiamata beacon chain che, attraverso un meccanismo di consenso Proof of Stake coordinerà e gestirà il network suddiviso tramite un processo di sharding[15].

[14] La beacon chain è stata lanciata nel 2020 il primo dicembre a mezzogiorno (UTC)
[15] È previsto il rilascio in produzione dell'aggiornamento relativo alla suddivisione in shard nel 2023

Capitolo 3
Finanza Decentralizzata

Da sempre le Istituzioni Finanziarie hanno avuto un ruolo chiave negli scambi di valore e nell'intermediazione finanziaria, soprattutto dal momento in cui risultò necessaria la presenza di un ente che certificasse la validità dello scambio. Ovviamente nel corso del tempo l'evoluzione tecnologica ha cambiato profondamente i modelli di business degli istituti finanziari, anche se la loro struttura e rigidità è rimasta relativamente invariata.

Come definito precedentemente l'obiettivo per cui è nato e continua a crescere Ethereum è quello di diventare un computer globale a supporto della finanza mondiale.
Infatti, è proprio grazie alle novità che vengono introdotte con Ethereum che nasce la cosiddetta Finanza Decentralizzata o DeFi.

Con DeFi si intende una sorta di ecosistema di servizi finanziari open source, permissionless e trasparenti, disponibili a chiunque senza un ente centrale sviluppati su tecnologie DLT.
Questi servizi finanziari alternativi hanno come obiettivo quello di rendere democratica la finanza stessa che da sempre è caratterizzata da una o più autorità centrali che intermediano e certificano i rapporti tra i singoli.
Con questo paradigma non occorrono intermediari o enti legali perché tutte le dinamiche sono previste a priori a livello di codice. Quindi questo si traduce subito in un abbattimento dei costi dovuti da eventuali ingaggi di forniture di servizi terzi.

Inoltre, essendo servizi distribuiti i dati sono condivisi con tutta la rete e questo garantisce una maggiore trasparenza rispetto le Istituzioni Finanziarie moderne.

Ultimo, ma non per importanza, alla base dei servizi di finanza decentralizzata c'è l'inclusione; infatti, grazie alla significativa riduzione dei costi ed alla facilità con la quale ci si può accedere, la DeFi si pone come obiettivo quello di aprire le porte alle comunità a basso reddito che, talvolta, hanno un'offerta finanziaria relativamente bassa.

Alla base della Finanza Decentralizzata quindi ci sono i seguenti elementi fondamentali: la *decentralizzazione* e la *disintermediazione*.

1) Decentralizzazione

Il termine decentralizzazione viene associato in particolar modo alla tipologia di accesso a questi servizi e soprattutto perché servizi costruiti su tecnologie distribuite. La decentralizzazione in genere si osserva su tre dimensioni:

- Governance: le decisioni relative all'erogazione, alle caratteristiche ed all'evoluzione del servizio sono assunte dalla comunità di utenti del servizio;
- Rischio: i diversi tipi di rischi associati ai servizi finanziari utilizzati sono a carico dell'utente ed il fornitore non ha garanzie;
- Gestione dei dati: i dati finanziari esistono in più copie su server diversi, appunto distribuiti, non di proprietà del provider e sono accessibili a tutti.

2) Disintermediazione

Gli intermediari finanziari hanno prevalentemente modelli di business incentrati sulle commissioni e tendono a ridurre l'efficienza delle transazioni nei settori in cui la spinta alla riduzione dei costi è forte e continua.
I servizi finanziari decentralizzati decidono di ridurre o eliminare alcuni o tutti gli intermediari dei servizi, consentendo agli utenti di interagire direttamente tra loro.
Alla base di queste applicazioni ci sono moltissime tecnologie che consentono la decentralizzazione dei servizi finanziari. Si possono individuare quindi due forme di servizi finanziari decentralizzati:

- La forma “debole” comporta una riduzione degli intermediari finanziari e un parziale decentramento dei servizi erogati. Il primo esempio di debole decentramento lo si può riscontrare nelle piattaforme peer-to-peer.
- La forma “forte” offre un decentramento completo senza intermediari finanziari e servizi. Il recente fenomeno DeFi ne è l'esempio migliore. Questo fenomeno è caratterizzato da servizi che esibiscono un forte decentramento su tutti e tre i fronti.

È intuitivo comprendere che la Blockchain è in grado di rivoluzionare tutti i settori finanziari a partire dalla concessione di mutui e prestiti, all’erogazione di servizi monetari, fino ai mercati decentralizzati e altro ancora rendendo più snelli i processi e, soprattutto, rendendoli di libero accesso.

3.1. Decentralized Applications

L'anima tecnologica di tutti i servizi finanziari decentralizzati risiede nelle Decentralized Applications, o dApps.
Esse sono applicazioni che girano su un sistema di calcolo distribuito, cioè una rete blockchain, e alla loro base ci sono gli Smart Contract che regolano le varie dinamiche dei processi tra i partecipanti della rete.
Ovviamente essendo costituite da tecnologie distribuite ereditano tutte le caratteristiche di quest'ultime, ossia:

- sono pubbliche e aperte a chiunque;
- non sono controllate da una singola entità o autorità, perché manutenute da più utenti (o nodi);
- non ci sono punti di fallimento, perché applicazioni protette crittograficamente ed equamente distribuite.

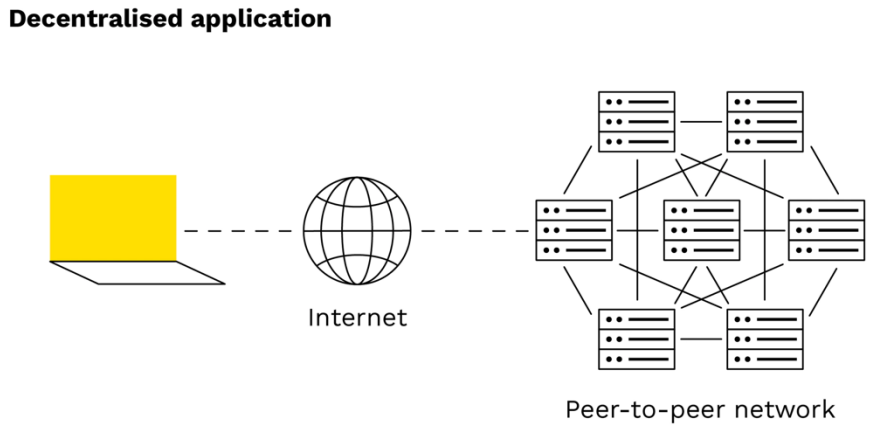

Figura 12: Rappresentazione esemplificata di una infrastruttura decentralizzata. [fonte: Bitpanda.com]

Ovviamente anch'esse hanno i propri svantaggi: infatti, queste applicazioni sono più difficili da realizzare e da manutenere, non sempre hanno alte performance soprattutto dovute ad una possibile congestione

della rete e occorre impiegare uno sforzo maggiore nella realizzazione della User Experience (UX).

Un'applicazione tradizionale, d'altro canto, è caratterizzata da un'architettura centralizzata che memorizza i propri dati su server controllati da una singola entità. In termini di sicurezza questo si traduce in un unico punto di fallimento (Single Point of Failure), che è suscettibile a problemi tecnici e attacchi malevoli.

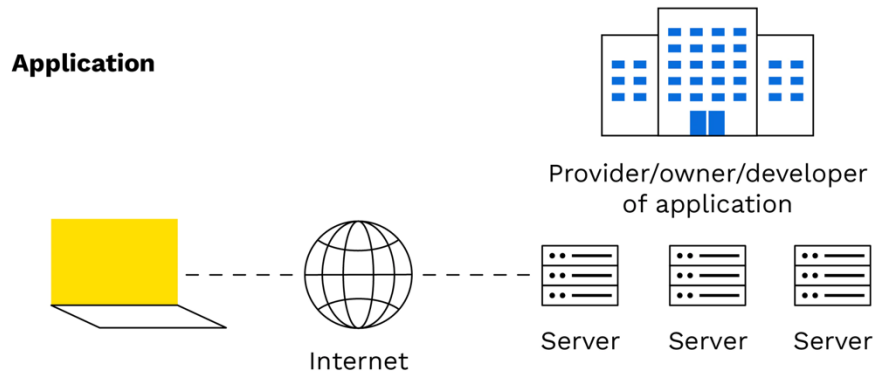

Figura 13: Rappresentazione esemplificata di una applicazione centralizzata tradizionale. [fonte: Bitpanda.com]

3.1.1. Oracoli

Queste applicazioni decentralizzate sono costituite principalmente da Smart Contract. Quindi si può assumere che le dApp siano a tutti gli effetti dei programmi eseguiti sulla blockchain, sviluppati in **Solidity** o **Vyper**[16]. Affinchè le dApps eroghino correttamente un determinato servizio, occorre che gli Smart Contract, che definiscono il funzionamento delle stesse, funzionino correttamente.

Ecco che si rende necessario introdurre una componente di vitale importanza per il funzionamento di un contratto intelligente: l'**oracolo**.

[16] Linguaggi di programmazione ad oggetti simili a Java, Javascript, C++ e Python per sviluppare Smart Contract sulla blockchain di Ethereum.

L’oracolo non è nient’altro che il ponte di collegamento tra il mondo esterno e la blockchain.
L’uso di questa componente è essenziale perché rende molto più ampio il raggio di azione degli smart contract. Questo perché un limite di quest’ultimi è quello di poter interagire solo con dati presenti sulla blockchain, o meglio on-chain. Quindi avere un modo per integrare dati da fonti esterne, o meglio off-chain, offre la possibilità di sviluppare svariate opportunità di business.
È importante definire che gli oracoli non sono la fonte stessa dei dati off-chain, ma componenti che forniscono dati provenienti da terze parti e che li certificano.
Va senza dire che la scelta dell’oracolo determina l’affidabilità delle informazioni e soprattutto la sicurezza dello smart contract e dell’applicazione stessa; un dato sbagliato potrebbe comportare errori computazionali nell’esecuzione del programma che si traducono poi in potenziali perdite economiche.
Questo appena descritto rappresenta il problema più grande che devono affrontare le applicazioni decentralizzate, e le blockchain in generale, perché introdurre un oracolo equivale a introdurre al loro interno un punto di debolezza.

A seconda delle quantità e tipologie di dati esistono diverse tipologie di oracoli. Prevalentemente le classificazioni si basano sulla fonte (hardware e/o software), sulla direzione (fonti in input e/o in output) e sulla fiducia (decentralizzata o centralizzata).

Di seguito vengono illustrati più nel dettaglio i vari casi d'uso:

- Oracoli hardware: integrano sistemi e tecnologie fisiche, come sensori, fornendo dati del mondo reale provenienti da quest'ultimi verso gli smart contract;
- Oracoli software: sono quelli maggiormente diffusi; recuperano dati online da programmi esterni e API[17];
- Oracoli in input: trasmettono dati esterni a contratti intelligenti o ad altri oracoli software.
- Oracoli in output: trasmettono i dati dagli smart contract a sistemi esterni, permettendo alle dApp di comunicare col mondo off-chain;
- Oracoli centralizzati: rappresentano l'unica fonte di informazioni verso gli smart contract e sono controllati da un'unica entità. Pertanto costituiscono un Single Point Of Failure;
- Oracoli decentralizzati: aumentano l'affidabilità delle informazioni ottenute basandosi su più fonti di verità. Lo smart contract interroga più oracoli per verificare validità e accuratezza dei dati. (Mou, 2020)

3.2. Token

Nel contesto delle dApp, e più ampiamente nella tecnologia blockchain, un token si riferisce generalmente a un'unità di valore di asset programmabili gestiti da contratti intelligenti e registri distribuiti sottostanti. I token sono sostanzialmente il mezzo principale per trasferire e memorizzare valore su una rete blockchain.

[17] Application Programming Interface: in un programma informatico, con API si indica un insieme di procedure atte all'espletamento di un dato compito; spesso tale termine designa le librerie software di un linguaggio di programmazione.

Di solito quando si parla di token si fa riferimento ad Ethereum: i token possono anche essere progettati per essere di due forme, fungibili o non fungibili, a seconda delle esigenze specifiche della rete.
I token possono, quindi, essere programmati, sono immutabili e sono definiti grazie agli smart contract e non hanno la possibilità di essere alterati in nessun modo.
Essi possono essere utilizzati per svariati casi d'uso, e in particolare per rappresentare una proprietà di un asset che è fuori dalla catena che può essere qualunque cosa, oppure possono essere nativi ma collegati a qualcosa scollegata dal mondo reale e quindi qualcosa di natura esclusivamente digitale.
I token sono importanti perché girano sulla blockchain, e quindi ereditano tutti i vantaggi della blockchain esattamente come un digital asset nativo, ma con la differenza appunto di poter essere programmati.

I token fanno parte a tutti gli effetti della famiglia dei digital asset, ed ecco quindi che occorre fare la prima distinzione fornendo due definizioni:

- *digital asset nativo*: esiste e funziona in modo indipendente e utilizza la propria Blockchain (Es. bitcoin, ether ecc.);
- *digital asset secondario* (token): è una rappresentazione di un valore o di diritti che possono essere elettronicamente trasferiti o conservati, programmato su una blockchain esistente.

Quindi in sostanza i token si possono definire come informazioni digitali registrate su un registro distribuito e rappresentative di una qualche forma di diritto, come per esempio la proprietà di un bene, l'accesso ad un servizio o la ricezione di un pagamento.

Una delle funzioni della Blockchain è permettere lo scambio di token in maniera sicura e senza intermediari: una volta creati i token, si possono inviare facilmente e senza bisogno di nessuno che tenga traccia dei diversi bilanci e delle transazioni, perché come ribadito più volte la Blockchain stessa garantisce trasparenza e tracciabilità. (Osservatori.net Digital Innovation, 2020)

3.2.1. Tipologie di Token

Per comprendere le due tipologie di token, è importante precisare cosa sono i beni fungibili: essi sono quei beni che possono essere sostituiti con qualcosa di identico.
I token possono avere infatti due nature, essi possono essere fungibili e non fungibili:

- Token fungibili: Sono quei token che non hanno particolari attributi e sono quindi intercambiabili tra loro.
- Token non fungibili (**NFT**): Ogni NFT avrà uno o più attributi, come ad esempio un codice identificativo che li rende unici. (Osservatori.net Digital Innovation, 2020)

Le differenze tra le due tipologie riguardano principalmente: intercambiabilità, trasferimento di valore e divisibilità.
In sostanza si può affermare che i token fungibili hanno riscontro pratico in ambienti in cui la tracciabilità non è una preoccupazione, come per esempio nel fornire liquidità al mercato; mentre gli NFT sono utilizzati in casi in cui l'unicità e la scarsità dimostrabile sono apprezzati, come per esempio nell'arte digitale.

Ovviamente affinchè si comprendano meglio i possibili utilizzi dei token è opportuno fare le dovute classificazioni:

- **Security token**: sono una rappresentazione digitale di un bene o utilità sottostante. Essi oltre ad avere caratteristiche specifiche e singolari rappresentano anche diritti di proprietà su qualcosa;
- **Tokenized security**: da non confondere con la categoria precedente, rappresentano un valore mobiliare tokenizzato. Quindi sono da interpretare come l'equivalente digitale del titolo sottostante, tipicamente progettato per essere facilmente scambiato, aggregato o utilizzato. In sostanza l'obiettivo di questo strumento è quello di ampliare l'accessibilità del mercato o la liquidità del titolo che viene tokenizzato, senza aggiungere ulteriori caratteristiche uniche programmate o crittografiche come quelle che si trovano nei security token;
- **Utility token**: rappresentano l'accesso ad un prodotto o servizio erogato su network blockchain. L'utilizzo principale è quello di alimentare lo scambio di valore all'interno di un network offrendo la possibilità di pagare commissioni di transazione, oppure offrendo la possibilità di garantire ai titolari di questi token il diritto di voto su sviluppi futuri di un determinato network;
- **Currency token**: sono token progettati unicamente per essere scambiati. Molte volte non hanno un vero e proprio valore sottostante e il loro valore è definito esclusivamente dalle modalità nelle quali vengono utilizzati.

3.2.2. Standard Token su Ethereum

La Blockchain di Ethereum essendo programmabile, permette di utilizzare gli smart contract per creare nuovi asset digitali (token).
Per farlo è necessario definire in uno Smart Contract tutte le sue caratteristiche fondamentali del token che si vuole creare, tra cui:

- Il numero di token in circolazione;
- Chi è abilitato a trasferirli;
- Chi può disporre dei token;
- Le regole di accesso ai token.

Ogni token, idealmente, può essere costruito in maniera diversa, ma nella pratica sono stati adottati alcuni standard comuni per semplificarne la creazione sia dal punto di vista tecnico che dal punto di vista normativo.
Di seguito sono illustrati tre dei principali standard: (Osservatori.net Digital Innovation, 2020)

- **ERC-20**: rappresenta uno standard token fungibile che può essere utility, security o payment; esso permette l'implementazione di un'API standard per i token all'interno degli smart contract. Inoltre, fornisce la funzionalità di base per trasferire i token, così come consente ai token di essere approvati in modo che possano essere spesi da un'altra terza parte on-chain. (Vitalik Buterin, 2015)
- **ERC-721**: rappresenta uno standard token non fungibile; più precisamente può essere la rappresentazione di un asset unico, fisico e/o virtuale. Questo standard permette l'implementazione di un'API standard per gli NFT all'interno degli smart contract. Esso fornisce funzionalità di base per tracciare e trasferire NFT. I possibili casi d'uso degli NFT sono riconducibili a oggetti da collezione virtuali, carte da collezione, prestiti, oneri ecc.
  In sostanza gli NFT sono distinguibili, tracciabili e garantiscono la proprietà dell'asset che rappresentano. (William Entriken, 2018)
- **ERC-1155**: rappresenta un Multi Token Standard, ossia un'interfaccia standard per contratti che gestiscono più tipi di token. Un singolo contratto può includere qualsiasi combinazione di token

fungibili, token non fungibili o altre configurazioni (ad esempio token ERC-20 o ERC-721). (Witek Radomski, 2018)

3.3. Nuove forme di finanziamento

Nell'economia globale le banche agiscono come intermediari gestendo e coordinando i sistemi finanziari attraverso i loro registri interni. Dal momento che questi registri non sono aperti per la revisione, ci si deve fidare delle banche e delle loro infrastrutture spesso obsolete.
La tecnologia blockchain ha il potenziale per rivoluzionare non solo il mercato valutario mondiale, ma l'intero settore bancario e finanziario riducendo questi intermediari e sostituendoli con un sistema senza fiducia, senza confini, trasparente e facilmente accessibile.
Attraverso la blockchain si può aiutare a rendere le transazioni più veloci ed economiche, aumentare l'accesso ai fondi, garantire una maggiore sicurezza dei dati, far rispettare accordi senza fiducia attraverso contratti intelligenti, rendere più semplice la conformità e altro ancora.

I principali vantaggi che si potrebbero riscontrare nel settore finanziario sono sicuramente trasparenza, sicurezza, fiducia, programmabilità, privacy e prestazioni, tutte caratteristiche proprie della blockchain.

3.3.1. Initial Coin Offering

Quando una società in una certa fase del suo ciclo di vita decide di aprire le porte ad un pubblico di investitori più ampio effettua un'operazione nota come IPO, Initial Public Offering. Sostanzialmente la società vende per la prima volta le sue azioni al pubblico contestualmente alla quotazione in Borsa.

Da questa operazione di finanziamento prende il nome la cosiddetta Initial Coin Offering (ICO), seppur operazione profondamente diversa dalla IPO. Infatti, mentre una IPO è un'operazione che viene effettuata da aziende già affermate sul mercato per espandersi ulteriormente, una ICO è una vera e propria forma di raccolta fondi per avviare una nuova opportunità di business.

Una ICO in sostanza è un nuovo modo per raccogliere capitali grazie alla tecnologia Blockchain. Più precisamente essa permette a piccole imprese o startup di raccogliere fondi vendendo token tramite degli Smart Contract promettendo un rendimento dagli stessi.
Quindi, questa operazione è in grado di semplificare e automatizzare il processo tradizionale che prevede di coinvolgere enti finanziatori, banche o investitori privati.
Inoltre, non è da sottovalutare il fatto che questa forma di finanziamento rende disintermediata e trasparente la raccolta e la distribuzione dei token.

Il ciclo di vita di una Initial Coin Offering si articola in tre fasi:

- **Pre-sale**: è la fase introduttiva poco prima dell'immissione al pubblico di un progetto blockchain. Consente di acquistare anticipatamente una certa quantità di token a un prezzo scontato;
- **ICO**: è la vera e propria fase di vendita e raccolta al pubblico di capitali per un progetto blockchain;
- **Listing**: consiste nella quotazione di un token in uno o più exchange. Tramite il listing è possibile scambiare il token in un mercato secondario.

Per mettere in pratica una Pre-sale, e successivamente la vera e propria ICO, è necessario delineare i Fundraising Terms nel Whitepaper in cui viene descritta nei minimi particolari la proposta di progetto.
Il Fundraising Term è composto dai seguenti attributi:

- **Ticker**: il codice univoco che andrà ad identificare il token che verrà emesso in cambio di capitali;
- **Token type**: la definizione della tipologia di token, per esempio un utility token standard ERC20;
- **ICO date**: data di inizio e fine della vendita al pubblico;
- **ICO price**: valore unitario del token alla vendita;
- **ICO Token Supply**: numero dei Token in vendita nell'ICO;
- **Soft Cap**: obiettivo minimo della raccolta;
- **Hard Cap**: obiettivo massimo della raccolta;

È da subito chiaro che i parametri riguardanti l'emissione di token del progetto blockchain che raccoglie capitali tramite ICO sono fondamentali: in particolar modo la Soft Cap che è necessaria affinché lo Smart Contract restituisca i capitali ricevuti in caso in cui non venga raggiunta.
Sulla base dei Fundraising Terms quindi ci sarà uno Smart Contract che coordinerà tutti i flussi. In pratica svolgerà le seguenti funzioni:

- dichiarerà un indirizzo dove potrà ricevere la valuta designata per la raccolta di capitale;
- indirizzerà i pagamenti degli investitori all'indirizzo designato in base a quanti token vogliono acquistare;
- distribuirà i token in base al valore definito dell'emittente e al capitale inviato all'indirizzo di raccolta.

La componente più importante di una ICO è quella di definire le dinamiche economiche del token: dalla crasi dei termini *token* e *economia* nasce la **Tokenomics.**

Nella tokenomics vengono esplicitate le funzionalità del token (generalmente utility token ERC-20) e come il token viene scambiato all'interno dell'ecosistema del progetto.

Il fondamento economico di base è rappresentato dalla domanda e dall'offerta. Inizialmente l'offerta del token, la supply, è limitata e garantita dallo Smart Contract e la scelta del prezzo è spesso condizionata al timing della raccolta tenendo conto di bonus percentuali mediante sconti:

- Sconto decrescente: il prezzo unitario del token viene scontato di una percentuale nella fase iniziale della raccolta, per poi raggiungere il suo prezzo unitario all'ultima fase della raccolta con 0% di sconto. L'obiettivo è incrementare la domanda grazie a una scontistica;
- Sconto crescente: il token viene venduto al suo prezzo unitario nella fase iniziale della raccolta e viene applicato uno sconto bonus percentuale con il passare del tempo. L'obiettivo è ottimizzare il valore della raccolta (essendo la domanda già alta, un prezzo elevato in fase iniziale permette di incrementare il risultato).

Dopo l'emissione e la conseguente quotazione (listing), più è alta la richiesta del token e più il prezzo cresce, al contrario, più bassa è la domanda più il prezzo si contrae (Figura 14).

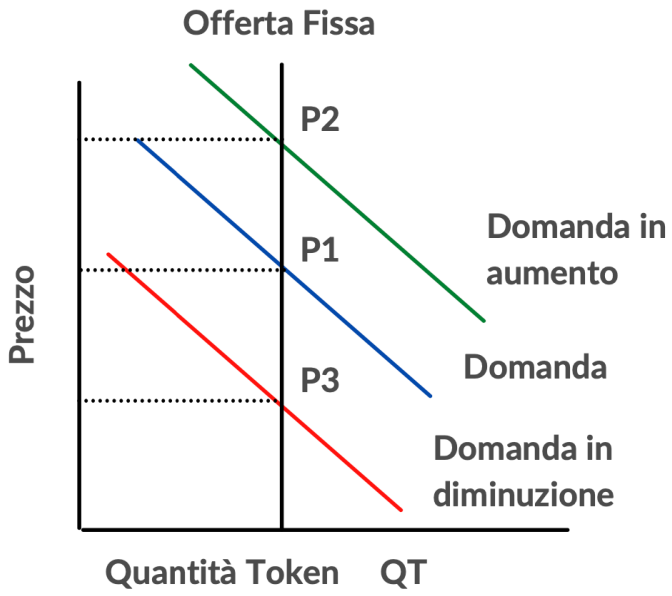

Figura 14: Andamento del prezzo di un token in funzione della quantità emessa.

Nell'aspetto economico è molto importante definire la funzionalità del token che si emette in quanto la speculazione è in grado di influenzare il valore del token nel breve termine. Ciò che determina il valore del token a medio-lungo termine è appunto il reale utilizzo dello stesso all'interno dell'ecosistema del progetto blockchain, un utilizzo che apporta vantaggio a tutti gli attori coinvolti nel progetto blockchain, gli users, i fruitori e i creatori del progetto.

3.3.2. Initial Exchange Offering

Sulla scia del boom delle ICO a cavallo tra il 2017 e il 2018 nasce una forma di investimento leggermente diversa, la cosiddetta Initial Exchange Offering (IEO).

Nel 2017, come si può vedere nel grafico illustrato in Figura 15 le ICO si sono affermate come forma di finanziamento raccogliendo un totale di 4,94 miliardi di dollari. Come descritto nel paragrafo precedente queste ICO hanno dato l'opportunità a molte startup e aziende emergenti di raccogliere capitali per espandere o avviare il loro business, ma purtroppo hanno anche dato la possibilità a malintenzionati di realizzare offerte ingannevoli realizzando truffe considerevoli.

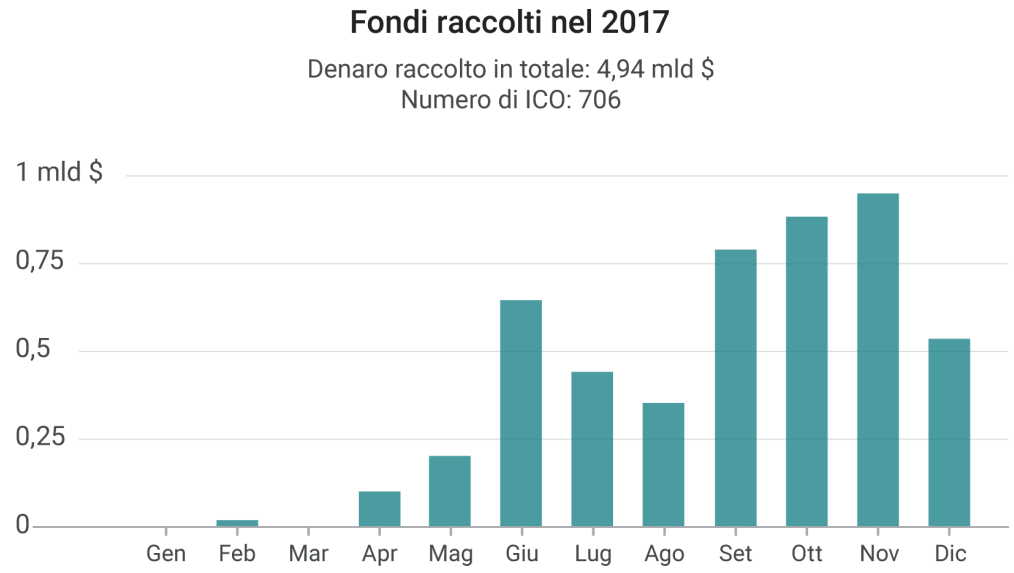

Figura 15: Fondi raccolti tramite ICO nel 2017. [Fonte: Forbes]

Ecco perché nasce l'esigenza di introdurre un punto di fiducia in questo processo di finanziamento. Infatti, una IEO non è nient'altro che una ICO che si realizza tramite un Exchange[18] di digital asset con il conseguente listing del token offerto su quest'ultimo.

Più precisamente quindi si può dire che una IEO è una vendita di token supervisionata e intermediata da un Exchange di digital asset e disponibile esclusivamente per gli utenti dell'exchange.

[18] Un exchange è una piattaforma tecnologica centralizzata, che permette di scambiare digital asset e token.

Quindi, proprio come le ICO, le IEO consentono agli investitori di acquistare token per finanziare promettenti progetti blockchain.

Il processo per avviare una IEO consiste in un primo screening delle startup da parte delle Exchange durante il quale vengono effettuate valutazioni sul progetto. Queste valutazioni sono necessarie in quanto l'Exchange, per avviare una IEO, si espone a molti rischi.
Il team di progetto in questa fase deve soddisfare diversi requisiti, come: avere un solido modello di business, membri esperti, buoni casi d'uso tecnici e un white paper dettagliato che è assolutamente fondamentale. Organizzare una IEO è come dichiarare un impegno a lungo termine per il successo di un progetto.
Successivamente in maniera analoga ad una comune ICO, occorre definire un obiettivo massimo della raccolta (hard cap) e un obiettivo minimo (soft cap) e infine, viene avviata l'offerta.

Il vantaggio principale di una startup nel ricorrere ad una IEO è quello di esporsi ad una platea di investitori qualificati[19] che già possiede crypto asset. D'altro canto, per gli investitori il processo di valutazione effettuato dall'Exchange rappresenta una "garanzia" sul progetto che avvia l'offerta. Ovviamente questa garanzia non è esente da rischi di non riuscita del progetto nel breve, medio o lungo termine. Inoltre, una ulteriore sicurezza per gli investitori è l'intermediazione dello scambio di valore dal wallet personale al progetto in quanto i fondi vengono inviati ad un wallet centralizzato.

[19] Persone che hanno effettuato un processo di profilazione all'interno di un Exchange immettendo dati reddituali e anagrafici definendo inoltre la loro propensione al rischio.

3.3.3. Security Token Offering

Una nuova forma di finanziamento che ha suscitato molto interesse nel contesto finanziario tradizionale è la Security Token Offering.

Prima di proseguire sarebbe opportuno fare una digressione su due tipologie di token trattate precedentemente: tokenized security e security token.
Infatti, entrambe le categorie di token rappresentano dei digital asset, ma esprimono concetti differenti:

- i **tokenized security**, o titoli tokenizzati, sono più semplici sia in termini di forma che di funzione. Praticamente un tokenized security è una rappresentazione digitale di un titolo mobiliare tradizionale con lo scopo di ampliare la sua portata di mercato e migliorare la liquidità del mercato. Quindi, i tokenized security funzionano allo stesso modo dei tradizionali titoli mobiliari off-chain, tranne per il fatto che possono essere immagazzinati, venduti e scambiati su reti blockchain;
- i **security token**, invece, attraverso le tecnologie DLT introducono una caratteristica aggiuntiva che i titoli tokenizzati non hanno: la programmabilità. Infatti, i secutity token devono anche affrontare un livello più alto di controllo normativo, dal momento che sono considerati titoli finanziari a tutti gli effetti e devono quindi essere emessi, scambiati e trattati in conformità con le leggi federali sui titoli pertinenti nelle giurisdizioni in cui è permesso emetterli e venderli. E, dal momento in cui i security token possono essere programmati con caratteristiche uniche e diritti di proprietà, si trovano a navigare in un territorio relativamente inesplorato sia dal punto di vista dell'innovazione che della regolamentazione. (Gemini, 2021)

Si intuisce da subito che il potenziale dei security token amplia di gran lunga le capacità dei titoli tokenizzati. Inoltre, i security token ereditano le caratteristiche della blockchain, quindi sono trustless, trasparenti e programmabili e questo significa che possono essere più facilmente trasferiti, scambiati e tracciati.

Quindi, sempre sulla scia dell'anno delle ICO, nel 2019 nascono le prime Security Token Offerings, o STO, che sono un metodo di distribuzione di security token a metà strada tra le Initial Coin Offerings (ICO) e le Initial Public Offerings (IPO).
In questa procedura i security token rappresentano una partecipazione di un bene o di una azienda, e qualsiasi forma di rendimento futuro associato alla stessa (dividendi).
La peculiarità delle STO sta nel fatto che bilanciano i benefici del crowdfunding basato sulla blockchain, come nelle ICO, con un livello rassicurante di supervisione normativa, come nelle IPO.
La supervisione normativa è derivante dal fatto che a differenza delle ICO, nelle quali vengono emessi utility token non ancora pienamente regolamentati, nelle STO vengono emessi security token equiparati per legge a titoli mobiliari.
Pertanto, solo alcune organizzazioni possono condurre una STO e solo alcuni soggetti possono acquistare security token. Ma a differenza di una ICO i soggetti che acquistano questi token sono maggiormente tutelati dalle regolamentazioni del contesto geografico di riferimento.

Tra i principali benefici di una STO rientrano sicuramente i minori costi per l'emissione del token con un conseguente aumento del capitale e una disintermediazione rispetto le istituzioni finanziarie.

Di seguito vengono elencati e descritti i vantaggi che le STO, e più nel dettaglio i security token, introducono nei sistemi finanziari:

- Sblocco del capitale e della liquidità del mercato: i security token possono essere negoziati senza limiti di tempo perché su reti blockchain e inoltre rendono accessibile l'investimento su scala globale;
- Aumento della disintermediazione: dal momento in cui lo scambio di valore avviene su reti distribuite, i security token permettono di bypassare gli intermediari di mercato. Tale evenienza riduce la complessità del sistema e abbatte i costi e i tempi di elaborazione di ogni transazione;
- Aumento della trasparenza e della tracciabilità: essendo ogni transazione crittograficamente verificabile i security token raggiungono un livello di affidabilità che altri asset non possono eguagliare.
- Automazione dei processi complessi: essendo programmabili, i security token hanno la possibilità di effettuare operazioni complesse in maniera automatizzata come per esempio distribuire dividendi o partecipazioni a chi li possiede con una determinata scadenza.

Per attuare una STO il primo passo consiste nell'emissione da parte di una azienda di security token seguendo le procedure standard per l'emissione di strumenti finanziari al pubblico, che in genere prevedono l'emissione di un prospetto, in questo caso di un White Paper. (Andriotto, 2019)
Successivamente occorre rappresentare i security token digitalmente attraverso la tokenizzazione del titolo tramite la blockchain e infine avviene la quotazione del token su Exchange.

Attualmente gli unici exchange che hanno finora consentito la quotazione di security token sono piattaforme dedicate agli investitori istituzionali, anche se molti exchange nel mondo hanno già avviato procedure per accettare offerte di titoli digitali messi a disposizione del pubblico.

Di seguito viene illustrato il processo appena descritto seguendo i vari step. (Figura 16)

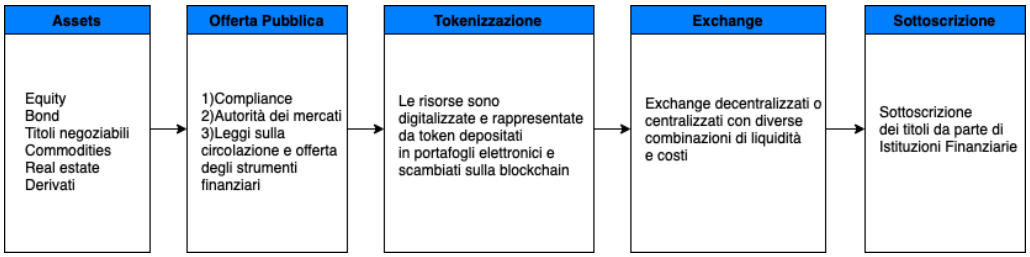

Figura 16: Rappresentazione grafica degli step di attuazione di una STO.

In conclusione mettendo a confronto le tre nuove forme di finanziamento analizzate finora si ottiene quanto rappresentato nella Tabella 2.

	ICO	**IEO**	**STO**
Natura del Token	Utility	Utility	Security
Grado di decentralizzazione	Alto	Basso	Basso
Mercato secondario	Si	Si	Si
Grado di regolamentazione	Basso	Basso	Alto
Trasferibilità del Token	Aperta	Aperta	Ristretta (KYC/AML)

Tabella 2: Confronto tra ICO, IEO e STO.

Ad oggi la forma di finanziamento più sicura e regolamentata è la STO che tra l'altro comprende sia i vantaggi delle ICO che delle IEO al netto della scarsa decentralizzazione.

Per completezza va precisato che non sono le uniche forme di finanziamento che stanno nascendo dalla costante adozione delle tecnologie blockchain based.
Infatti, esistono altre forme per raccogliere capitali nei progetti blockchain, che assumono nomi differenti ma che alla base del meccanismo di funzionamento, si rifanno alle tre categorie precedentemente illustrate.

Di seguito se ne elencano un paio che non verranno trattate in questo elaborato:

- IDO (Initial DEX Offering): è un innovativo metodo di raccogliere fondi per progetti blockchain in maniera permissionless e decentralizzata.
- IFO (Initial Farm Offering): è una nuova tipologia di raccolta fondi per progetti blockchain che utilizza gli eventi di farming in piattaforme exchange decentralizzate.

Capitolo 4
Regolamentazione

Riprendendo il concetto di Finanza Decentralizzata illustrato nel capitolo precedente, ci si trova in una delle frontiere più avanzate del Fintech e in un sottoinsieme dei protocolli delle applicazioni che girano su Blockchain. La DeFi, infatti, tra le principali caratteristiche ha quella di consentire delle transazioni finanziarie in maniera del tutto automatizzata senza la necessità di un soggetto che abbia la regia di queste transazioni e possa effettuare un controllo sugli asset che vengono intermediati.
Quindi questo è un sotto settore delle tecnologie blockchain che dal punto di vista giuridico pone non poche perplessità e attenzioni.

In particolar modo le caratteristiche che suscitano maggiore interesse per il regolatore sono:

- la natura *non custodial* di queste piattaforme*:* cioè l'assoluta assenza di un controllo sugli asset che vengono negoziati nella blockchain;
- la *governance distribuita:* quindi il fatto che i partecipanti a queste transazioni sono coloro che assumono le decisioni attraverso dei governance token[20] sulla gestione della piattaforma stessa.

Questo crea una sorta di collisione tra il ruolo dell'utente del servizio finanziario e quello del "proprietario" del servizio stesso, quasi definibile un "azionista" della piattaforma.

[20] Queste tipologie di token consentono ai possessori di influenzare le decisioni riguardanti il progetto blockchain di cui fanno parte.

Queste applicazioni decentralizzate sono entrate nel mirino dei legislatori a livello mondiale, e più precisamente nel contesto europeo sono diventate oggetto del MiCAR[21] (Markets in Crypto-Asset Regulation) che è un quadro giuridico che disciplina tutta la materia dell'emissione e delle prestazioni di servizi relativamente ai cripto asset che non sono riconducibili direttamente a strumenti finanziari: l'esempio più ovvio è quello appunto delle criptovalute.
Attraverso il MiCAR si è cercato di delineare alcuni elementi di disciplina della finanza decentralizzata. Infatti, per esempio, il Regolamento stesso al punto 12a recita come di seguito:

[…] Il presente regolamento si applica alle persone fisiche e giuridiche e alle attività e ai servizi svolti, forniti o controllati in qualsiasi modo, direttamente o indirettamente, da esse, anche quando parte di tale attività o servizi è svolta in modo decentralizzato. […] (Council of the European Union, 2021)

Quindi, il legislatore sta attivamente cercando di disciplinare questo fenomeno con la preoccupazione generale di distinguere la vera decentralizzazione, da una fittizia: cioè il rischio che determinate società si presentino come emittenti di servizi decentralizzati, ma hanno effettivamente un soggetto a cui è riconducibile la gestione della piattaforma.

In particolare, dal momento in cui il tema più critico che ruota attorno alle applicazioni di finanza decentralizzata è l'attività di investimento, il ruolo del regolatore e degli organi di vigilanza sostanzialmente è quello di

[21] Markets in Crypto-Assets è una proposta di regolamento nel diritto dell'Unione Europea. Ha lo scopo di aiutare a semplificare la tecnologia del registro distribuito e la regolamentazione delle risorse virtuali nell'Unione Europea, proteggendo al contempo utenti e investitori. [fonte: Wikipedia]

garantire l'emanazione di norme atte a ridurre al minimo il rischio che il risparmio degli attori venga collocato in maniera inconsapevole. Tali rischi riguardano soprattutto le incertezze sullo strumento (qualunque crypto-asset per esempio) e le caratteristiche delle piattaforme alle quali ci si rivolge.
La sfida quindi è quella di distinguere l'aspetto tecnologico dalla competenza necessaria da parte degli attori che intervengono su questi mercati decentralizzati che deve essere all'altezza di una consapevolezza totale di quelli che sono gli atti che compiono: il rischio è che nel momento in cui queste tecnologie crescano si crei confusione tra la qualità della tecnologia e l'affidabilità dello strumento in cui si investe.

4.1. Scenario legislativo Europeo

Nel contesto della DeFi è opportuno analizzare il comportamento che nasce intorno la domanda dei servizi stessi: il lato della domanda nelle dApp partecipa attivamente ai processi di produzione di offerta dei servizi alimentando il sistema e diventando a tutti gli effetti una sorta di co-produttore dei servizi di cui usufruisce e co-responsabile delle esperienze che gli vengono offerte.

Il ruolo del regolatore a fronte di un sistema governato attraverso l'operatività degli smart contract, in Europa, segue uno schema ben preciso e si muove prendendo di riferimento le dinamiche stesse della finanza decentralizzata: quando è incerto chi sia dal punto di vista soggettivo a fornire il servizio, perché la fornitura dello stesso viene gestita da sorgenti tecnologiche, quali smart contract, è il servizio offerto stesso a dover guidare la conoscenza dei rischi e delle regole e il rafforzamento delle stesse.

Questo principio è tipico e specifico della finanza decentralizzata ma anche della strategia europea adottata sulla gestione dei dati.

Un esempio nasce proprio dalla regolamentazione di mercati e servizi digitali, secondo cui l'assetto del regolatore europeo prevede un principio in base al quale tutto ciò che è illecito off-line è illecito on-line.
Quindi l'idea di fondo è quella di far corrispondere alle attività svolte su blockchain gli stessi rischi delle attività che vengono effettuate in maniera tradizionale nel mondo off-chain.

In conclusione, la strategia europea cerca di riconoscere ai servizi decentralizzati una chiave di lettura per orientare il regolatore nella definizione di uno schema attraverso il quale incentivare l'innovazione senza rinunciare ad un sistema di diritto.
Il legislatore europeo sembra abbia declinato una regolamentazione che lascia ampio spazio alla neutralità tecnologica, una regolamentazione in base alla quale se si individua una entità responsabile dietro un servizio basato su tecnologie distribuite, allora l'organo di vigilanza può intervenire rispetto a questo soggetto. Quindi è ruolo del vigilante andare ad indagare se il framework sia effettivamente decentralizzato oppure no.

Un altro aspetto di rilevante importanza sul quale si sta muovendo la normativa europea è quello della Compliance, nello specifico al trattamento dei dati.
La transizione tecnologica ruota attorno al dato ampiamente inteso, che sia il dato commerciale piuttosto che quello confidenziale.
Quindi il dato è centrale, ma grazie alle tecnologie esso assume sempre di più una valenza ibrida e acquista un valore non intrinseco, ma che dipende dalla combinazione e dall'uso che ne viene fatto.

Dal momento in cui il dato nelle applicazioni decentralizzate è di altrettanta importanza, è necessario interrogarsi su come la normativa a livello europeo affronta la valenza multiforme del dato, e si può pertanto affermare che essa si muove verso un paradigma generale e neutrale rispetto alla tecnologia.

In accordo con il GDPR, il trattamento dei dati è richiesto da un obbligo legale, o quando è funzionale all'esecuzione di un compito, o quando è di interesse generale, o quando è connesso all'esercizio di pubblici poteri.

Quindi, riprendendo il concetto che il regolatore europeo sta seguendo per definire la normativa, ossia l'intenzione di attribuire alla stessa attività lo stesso rischio e la stessa supervisione, il trattamento del dato si concilia molto bene perché grazie alla base giuridica della MiCAR si potrebbero fornire degli utili spunti consentendo e garantendo la legittimità del trattamento, e ben qualificando il principio appena citato con l'ulteriore regola secondo la quale si concede l'esternalizzazione, ma non l'immunità.
In sintesi si prevede che le regole vengano rispettate indipendentemente dal decentramento e dovranno essere rispettate da tutti i soggetti o dai modelli organizzativi che verranno ad essere attuati ed implementati senza sconti.

Uno dei problemi più grandi che si pone il legislatore è quello di adattare le regole esistenti ad un contesto tecnologico in continua evoluzione, e questo rappresenta una grossa difficoltà essendo un contesto estremamente dinamico. Inoltre, la difficoltà è nel volersi intromettere in un contesto tecnologico dove attualmente il garante non è uno Stato o un Regolatore, ma bensì il codice stesso che crea e distribuisce fiducia su tutto il network.

Una possibile soluzione potrebbe essere quella di sfruttare le dinamiche tecnologiche stesse delle applicazioni decentralizzate ed introdurre in ottica embedded all'interno degli smart contract la logica di quelle che poi saranno le normative.

4.1.1. Mercati primari e secondari di crypto-asset

La proposta del regolamento della Commissione europea MiCAR, dopo un attento periodo di studio e di analisi del mercato e dei principali stakeholder, prevede una disciplina sia per la fase primaria cioè la prima emissione di cripto-attività e la loro offerta a potenziali investitori, sia per la successiva circolazione delle cripto-attività dettando regole rivolte anche ai crypto-asset.

Sono diversi infatti gli ambiti coperti dalla proposta: per quanto concerne la fase di mercato primario si è utilizzato lo strumento della trasparenza prevedendo l'obbligo di redazione di un *whitepaper* destinato ad informare il pubblico sulle caratteristiche dell'offerta dei soggetti coinvolti e dei crypto-asset. È previsto un regime di autorizzazione e successiva vigilanza per lo svolgimento delle attività dei fornitori dei servizi su crypto-asset, questi servizi potranno essere prestati sia da *new entrant*, che da operatori *incumbent* senza dover richiedere, per quest'ultimi, un'ulteriore apposita autorizzazione. Infatti gli incumbent potranno immediatamente dopo l'entrata nel mercato, in applicazione al regolamento MiCAR, erogare questi servizi esattamente come gestori di mercato già autorizzati. Sono poi addirittura contemplate disposizioni specifiche di prevenzione relative agli abusi di mercato con particolare riferimento ai mercati di crypto-asset.

Dopo un attento esame degli ostacoli esistenti nelle discipline di settore rispetto lo sviluppo di un mercato primario e secondario di crypto-asset, ancora una volta si può dire che l'approccio della Commissione europea è

stato conservativo, basato sul noto principio citato in precedenza: stesse attività, stessi rischi, stesse regole.
Allo stesso tempo l'ambito di applicazione oggettivo è molto ampio; si va dalle criptovalute, sia che queste abbiano una principale funzione di mezzo di pagamento, sia che invece abbiano principalmente una funzione di investimento. Discorso diverso per quanto riguarda gli utility token in quanto è alquanto ambigua la loro correlazione e la loro idoneità nel rappresentare veramente una forma di investimento e del risparmio.
Inoltre, nell'attingere alle diverse discipline del settore finanziario ne emerge un quadro molto modulare per cui determinate attività e processi possono entrare nel radar del regolatore in momenti diversi del ciclo di vita del crypto-asset: per esempio, non c'è nessun collegamento tra mercato primario e secondario, token emessi offerti al pubblico e quindi soggetti all'obbligo di whitepaper potrebbero anche non accedere mai ad una piattaforma di scambio.
Pertanto, la MiCAR trova applicazione solo nella misura in cui sia individuabile un soggetto responsabile di un determinato processo o attività.

Pur offrendo una panoramica generale legislativa riguardo il mondo delle DLT, la normativa MiCAR non riesce a rappresentare la coerenza e la diversa natura di tipologia di token. È poco razionale nel momento in cui applicano ai token di pagamento misure ispirate alla finalità di servizi di investimento.
I token che possono essere acquistati come finalità di investimento, talvolta si trovano nel mezzo tra la qualificazione come strumenti finanziari soggetti a regolamentazione MiFID II[22] oppure strumenti appartenenti alla classe residuale definita da MiCAR.

[22] La direttiva dell'Unione Europea 2004/39/CE (conosciuta anche come direttiva MiFID, ove MiFID è acronimo di Markets in Financial Instruments Directive), atto normativo emanato dal

L’effetto negativo della normativa, quindi, si potrebbe avere sulla regolamentazione di token che non vengono acquistati con finalità di investimento su cui la logica MiCAR è sproporzionata in quanto c’è una logica di tutela degli investitori completa, ma che non è applicabile nel caso per esempio degli utility token.

4.1.2. Tipologie di token in MiCAR

È opportuno a questo punto osservare più nello specifico il regolamento, dove si può notare che esso divide il mondo dei crypto-asset in tre macro categorie.

Forme regolamentate di Crypto-Asset		
Utility Token	**Asset-Referenced Tokens (Stablecoins)**	**E-Money Token**
Forniscono l'accesso a un bene o servizio distribuito accettato solo dall'emittente del token. Gli utility token hanno uno scopo non finanziario legato al funzionamento di una piattaforma digitale.	Mantengono un valore stabile facendo riferimento a valute fiat, materie prime o cripto-asset. Vengono utilizzate come mezzo di pagamento per acquistare beni e servizi e come riserva di valore.	Principalmente un mezzo di pagamento, che stabilizza il valore facendo riferimento a una sola valuta fiat. La funzione di tali criptovalute è molto simile a quella della moneta elettronica.

Tabella 3: Classificazione dei token prevista dalla normativa MiCAR

Parlamento europeo il 21 aprile 2004, partecipa alla costruzione di un mercato finanziario integrato, efficace e competitivo nell'Unione europea definendone i principi generali, e si inquadra nel più ampio "piano di azione per i servizi finanziari" (FSAP), varato nel 1999 e concretizzatosi in ben 42 direttive. A tale direttiva è seguita la direttiva 2006/73/CE, attuativa della prima. [fonte: Wikipedia]

Come si può notare dalla Tabella 2 ci sono tre tipologie principali di token individuati all'interno della MiCA Regulation:

- Gli Asset-Referenced token hanno qualche analogia a strumenti di pagamento e in parte sono riconducibili alla categoria delle cosiddette Stablecoins;
- Gli E-money token che sono considerabili una analogia della moneta elettronica emessa su una tecnologia DLT;
- Gli Utility token, infine, sono la vera e propria novità introdotta nel regolamento per classificare dei "metodi di accesso" a delle piattaforme con uno scopo non finanziario.

La condizione interessante del regolamento in questione è il fatto che qualunque potenziale categoria di asset che non ricade all'interno delle precedenti classificazioni viene considerata *out of scope* della normativa e pertanto, quei crypto-asset verrebbero regolati con le componenti fondamentali del regolamento esistente dell'Unione Europea per i titoli (MiFID II / MiFIR) e Market Abuse (MAD II / MAR).

Questo punto di vista fornisce sicuramente un quadro chiaro per la protezione degli investitori e l'integrità del mercato, ma consente ancora diverse interpretazioni.

4.2. Scenario legislativo Svizzero

In materia di regolamentazione crypto, la Svizzera si può definire uno stato pioniere in quanto già nel 2017 inizia a provare a definire delle regole e distinzioni a riguardo.

Precisamente, l'Autorità federale di vigilanza sui mercati finanziari ha stabilito in un avviso di regolamentazione della FINMA come verranno gestite le richieste di presentazione relative alle Initial Coin Offering ai sensi del diritto vigente in materia di mercati finanziari. Nella sua attenta valutazione delle ICO, la FINMA segue un approccio incentrato sulla funzione economica e sullo scopo del token. In questo caso, dall'ICO, risultano determinanti la classificazione del token e l'emissione della liquidità o trasferibilità del token.

A livello funzionale, la FINMA distingue tre tipologie:

- Utility Token: sono token destinati a fornire l'accesso digitale a un'applicazione o un servizio.
- Security Token: rappresentano asset come partecipazioni a sottostanti fisici reali, società o flussi di utili o un diritto a dividendi o pagamenti di interessi. In termini di funzione economica, questi token sono analoghi ad azioni, obbligazioni o derivati.
- Payment Token: sono sinonimo di criptovalute e non hanno ulteriori funzioni o collegamenti a progetti di sviluppo o nel mondo "reale". (Finma, 2017)

Si possono subito notare delle analogie con la normativa europea, ma in particolare si può notare come il regolatore svizzero abbia definito i security token equiparandoli a strumenti finanziari, cosa che nella normativa MiCAR viene lasciata più all'interpretazione per le tipologie di token che vengono definite out of scope.

È interessante inoltre notare come la FINMA si impegna nel definire le ICO come dei mezzi attraverso cui raccogliere, in forma digitale, capitale per scopi imprenditoriali sulla base della tecnologia blockchain.

In particolare, con riferimento ai token che possono essere emessi in cambio di finanziamenti, la FINMA recita che:

[…] I token di utilizzo non sono classificabili come valori mobiliari nei casi in cui il token conferisce esclusivamente un diritto di accesso a un'utilizzazione o a un servizio digitale e il token di utilizzo è impiegabile in tal senso al momento dell'emissione. Tutti i casi in cui sussiste solo o anche la funzione economica di investimento sono trattati dalla FINMA come valori mobiliari (come token d'investimento) […] (FINMA, 2018)

Quanto illustrato precedentemente si traduce in due scenari:

Scenario 1.
Il progetto che raccoglie capitali mediante ICO ha un MVP[23].
In questo caso il progetto, con un prototipo funzionante, sta dimostrando l'effettiva utilità del token. Ad esempio l'utility token che la società emette con la ICO serve per accedere o per utilizzare la piattaforma.
Quindi per l'Autorità il token utilizzato per la raccolta di fondi è equiparato ad un token d'utilizzo.

Scenario 2.
Il progetto che raccoglie capitali mediante ICO non ha un MVP.
In questo caso non essendoci un prototipo funzionante, ma solo il whitepaper di un ipotetico progetto, l'emissione di un utility token è vista dall'Autorità come una promessa di possibili guadagni futuri e quindi assimilabile a uno strumento finanziario.

[23] Minimum viable product, è la versione di un prodotto con caratteristiche appena sufficienti per essere utilizzabile dai primi clienti, i quali possono quindi fornire feedback per lo sviluppo futuro del prodotto stesso. [fonte: Wikipedia]

4.3. Scenario legislativo Italiano

In Italia, con leggero ritardo rispetto la Svizzera, si iniziano ad analizzare più nel concreto le cripto-attività solo dal 2019.
Una delle evidenze si può riscontrare in un Occasional Paper pubblicato da Banca D'Italia di cui se ne riporta uno stralcio di seguito:

[…] Le "cripto-attività" analizzate in questo lavoro appartengono alla classe dei gettoni digitali (digital tokens) privati, senza diritti incorporati, convertibili, a prezzo variabile che operano attraverso un protocollo elettronico gestito in modo decentrato tramite una tecnologia denominata permissionless distributed ledger technology (DLT) detta anche blockchain. […] (Banca D'Italia, 2019)

Si può notare che nel contesto finanziario si inizia a parlare concretamente di digital token, e in aggiunta si inizia a definire l'aspetto tecnologico attraverso il quale vive il token stesso, ossia le tecnologie distribuite.
È interessante però notare che sempre nello stesso paper vengono fatte distinzioni sulle tipologie di token, e a differenza della normativa svizzera vengono individuate più forme.

Banca D'Italia definisce i token come gettoni digitali che rappresentano valore "al portatore", che fanno uso della crittografia e della DLT e che incorporano diritti finanziari, di proprietà o d'uso.
La definizione fornita è in linea con le altre analizzate in questo elaborato, ma in aggiunta questa pubblicazione identifica quattro tipologie:

1) DT1 – "valute virtuali": sono gettoni digitali che non possiedono e non rappresentano un diritto, ma sono gettoni che si possono negoziare e convertire sia in moneta legale di stato, la cosiddetta FIAT money (es.

Euro), oppure in valuta virtuale, ad un prezzo variabile (es. Bitcoin è una valuta virtuale)

2) DT2 – digital coins o payment tokens: sono monete digitali o gettoni che rappresentano un pagamento. In sostanza sono strumenti che cercano di replicare le stesse funzionalità della moneta mantenendo un valore fisso. Questi gettoni digitali sono un diritto oppure rappresentano una passività della stessa persona che emette il gettone (token). A loro volta hanno una ulteriore distinzione:
   a) privati a valore fisso (Stablecoins): sono emessi da una entità giuridica in cambio di una unità di moneta (uno-a-uno con euro, dollaro, ecc.); è segregata presso un soggetto regolato. Essi possono essere considerati 'moneta elettronica' se e solo se ne rispettano strettamente le caratteristiche, con la sola differenza che usano la DLT. Se invece, oltre alla funzione di moneta elettronica, incorporano altri diritti come diritto di proprietà o diritto d'uso, potrebbero ricadere nella categoria DT3 (security token);
   b) emessi da una banca centrale (CBDC - Central Bank Digital Currencies): si tratta di progetti ancora in fase di sperimentazione volti a creare moneta elettronica emessa proprio da un Banca Centrale che usa la DLT (ad esempio un euro in formato digitale emesso dalla BCE). Essi sono una passività della banca centrale;
   c) non convertibili: sono gettoni digitali che favoriscono lo scambio. Si distinguono da altri tipi di gettoni digitali poiché non sono convertibili con moneta legale (euro, dollaro ecc..) o con altre "valute virtuali" (bitcoin, ether, ecc).
3) DT3 – Token di investimento (asset o security), sono token digitali trasferibili e potenzialmente negoziabili su una piattaforma. Essi sono offerti ed emessi tramite un'operazione chiamata STO. Essi sono simili a titoli smaterializzati, che tuttavia vengono trasferiti tramite la DLT.

4) DT4 – utility tokens/consumer tokens: sono gettoni digitali non negoziabili (pur essendo talvolta trasferibili) che offrono unicamente diritti amministrativi o licenze d'uso, quali l'accesso a una piattaforma, a una facility, a un network di persone, a schemi di "fidelizzazione". (Banca D'Italia, 2019)

4.3.1. CONSOB e Initial Coin Offering

Analogamente alla giurisdizione svizzera, anche l'Autorità italiana per la vigilanza dei mercati finanziari si impegna nella definizione delle ICO.
Come per FINMA, anche la CONSOB definisce le ICO come delle forme di raccolta fondi che avvengono tramite la vendita di token al pubblico su tecnologie distribuite. Ma il lavoro fatto da CONSOB illustrato nel "*Le offerte iniziali e gli scambi di cripto-attività*" ha come scopo quello di iniziare a delineare le varie dinamiche che girano intorno a questa nuova modalità sottolineando la difficoltà relativa alla corretta regolazione per una maggiore tutela dei consumatori.
La CONSOB si esprime inoltre riguardo le Initial Exchange Offering, dicendo che è possibile effettuare una IEO regolarmente su portali di crowdfunding già iscritti alla CONSOB o su nuovi portali che permettono lo scambio di token.
Importante condizione è quella di redigere un whitepaper a disposizione dell'investitore a spiegazione del progetto, delle caratteristiche dei token , della loro emissione ed offerta.
Inoltre, verrà previsto un regime normativo ad hoc per queste piattaforme, compliance, business continuity, due diligence, monitoraggio delle transazioni, informazioni sulle crypto attività, cybersecurity.
Un'osservazione rilevante è quella da fare sul perimetro attribuito dalla CONSOB: il regolamento infatti ha ristretto il campo di azione delle IEO

alle sole raccolte che hanno come oggetto Utility Token, che attualmente sono in una zona grigia normativa a differenza dei Security Token.

L'approccio della CONSOB è di ricondurre le cripto attività nelle attività diverse dagli strumenti finanziari di cui all'art. 1 comma 2 TUF[24] e dai prodotti di investimento di cui al comma 1 lettere w-bis.1, w-bis.2 e w-bis.3 consistenti nella rappresentazione digitale di diritti connessi a investimenti in progetti imprenditoriali.

4.3.2. Inquadramento degli aspetti tecnologici, tributari e antiriciclaggio

La tecnologia blockchain non ha limiti territoriali e i nodi di una blockchain essendo distribuiti esistono in diversi paesi e giurisdizioni.
Questo genera il problema di individuare la corretta legge applicabile e il foro competente. Una possibile soluzione potrebbe essere quella di individuarli alla base della transazione on-chain in modo da garantire autonomia delle parti.

Se le parti non hanno scelto diritto applicabile e foro competente allora si dibatte sull'applicabilità delle norme del diritto privato internazionale.

- Step 1: individuazione del foro competente (es. Bruxelles per i Paesi UE);
- Step 2: applicazione delle conflict rules (norme di diritto privato internazionale) previste dalla legislazione dello Stato ove ha sede il foro competente.

[24] Testo unico delle disposizioni in materia di intermediazione finanziaria (decreto legislativo 24 febbraio 1998, n. 58)

In Italia, nel 2019 è stato pubblicato sulla Gazzetta Ufficiale il "Decreto Semplificazioni[25]" nel quale si prova a dare una definizione chiara delle tecnologie DLT e dei vari componenti che la caratterizzano.

In particolare il Decreto in questione recita all'Art. 8-ter. (Tecnologie basate su registri distribuiti e smart contract) al Comma 1:

[…] Si definiscono "Tecnologie basate su registri distribuiti" 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. […] (Gazzetta Ufficiale della Repubblica Italiana, 2019)

Nel Comma 1, si può notare che è un primo formale riconoscimento che introduce effetti giuridici. Sicuramente è un incentivo per le imprese e la Pubblica Amministrazione per riconoscere l'esistenza e soprattutto la validità di queste tecnologie. In aggiunta questo testo colloca l'Italia tra uno dei primi paesi dell'Unione Europea ad aver intrapreso l'edificazione di un quadro normativo.
Con una maggiore attenzione, però, si può notare che viene definito il genus DLT, piuttosto che la species blockchain. Inoltre, la dicitura "architetturalmente decentralizzata" è opinabile in quanto le tecnologie DLT non sono architetturalmente decentralizzate ma bensì lo è solo l'accesso ai dati distribuiti sul network.

[25] D.L. 14 dicembre 2018, n. 135 convertito con legge 11 febbraio 2019, n. 12

La normativa italiana sta cercando di rendere più chiaro questo fenomeno delle DLT, e in particolare cerca di regolare i fenomeni che ruotano attorno i componenti principali delle Blockchain e più ampiamente delle DLT, i token.

Come visto precedentemente i token vengono classificati giuridicamente come:

- beni o beni immateriali
- mezzi di pagamento o moneta elettronica
- quote di OICR[26]
- strumenti finanziari
- titoli di credito
- prodotti di investimento

Da un lato le Banche Centrali vorrebbero considerare i token come un metodo di pagamento e di conseguenza normarli come se fossero una moneta elettronica; da un'altra prospettiva gli enti di regolazione li vorrebbero vedere come strumenti finanziari in modo da applicare le norme relative a questi fenomeni già esistenti e da un'altra ancora le Agenzie delle entrate vorrebbero tassarle.
Ogni regolatore sta cercando di interpretare questo strumento rappresentato da blockchain e dalle criptovalute.
Ma il problema individuato finora è che è impossibile regolare una stringa esadecimale alfanumerica che di per sé non ha nessun valore. Quindi l'obiettivo comune è quello di introdurre regole per gli attori del sistema,

[26] Gli organismi di investimento collettivo del risparmio, in acronimo OICR, in Italia, sono organismi con forma giuridica variabile che investono in strumenti finanziari o altre attività somme di denaro raccolte tra il pubblico di risparmiatori, operando secondo il principio della ripartizione dei rischi. [fonte: Wikipedia]

che nel concreto vorrebbe dire regolare i comportamenti dei nodi di un network, gli emittenti di una ICO, i miners per quanto riguarda Bitcoin ecc.

Un altro elemento chiave al centro dei ragionamenti del regolatore è rappresentato dagli Smart Contract.
Spesso vengono accostati ai contratti, ma non sono né intelligenti e né dei contratti, come afferma lo stesso ideatore Vitalik Buterin. Questo perché descrivono delle interazioni event-driven: uno smart contract serve a tradurre il linguaggio giuridico molto rigido in un linguaggio informatico semplificandolo secondo il principio della logica computazionale dell'If This Then That (ITTT).
Una caratteristica peculiare degli smart contract è quella di essere auto eseguiti (self-execution) per adempimenti automatizzati e per il suo self-enforcement in caso di inadempimento: esistono delle clausole che prevedono la risoluzione di eventuali problemi.

In Italia, il gruppo di esperti incaricato dal Ministero dello Sviluppo Economico per sviluppare una strategia nazionale riguardo le DLT ha formulato nel decreto-legge di semplificazione (D.l. n. 135/2018) una definizione di smart contract di cui all'Art. 8-ter. (Tecnologie basate su registri distribuiti e smart contract) al Comma 2:

[…] Si definisce "smart contract" un programma per elaboratore che opera su Tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia Digitale con linee guida

da adottarsi entro 90 giorni dall'entrata in vigore della legge di conversione del decreto legge. […] (Gazzetta Ufficiale della Repubblica Italiana, 2019)

Secondo il testo normativo, uno smart contract, per definirsi tale, deve avere simultaneamente le seguenti caratteristiche:

- essere un programma per elaboratore;
- operare su tecnologie basate su registri distribuiti;
- l'esecuzione vincola automaticamente due o più parti;
- gli effetti devono essere predefiniti dalle parti.

Analizzando queste tecnologie dal punto di vista tributario va precisato che per la normativa italiana attualmente i crypto asset, pur essendo mezzi di scambio/pagamento, sono assimilate a valute estere.
Pertanto, sono rilevanti ai fini IVA[27], ma sono esenti in quanto ricadenti nella casistica di cui all'art. 10 DPR 633/72 e art. 135, par. 1, lettera e), Dir. 2006/112/CE: operazioni su mezzi di pagamento.
Inoltre, viene specificato che se le transazioni riguardano esclusivamente operazioni "a pronti[28]" di modico importo e i clienti sono persone fisiche che detengono questi digital asset al di fuori dell'attività d'impresa, manca la finalità speculativa e quindi l'intermediario non è tenuto ad alcun adempimento come sostituto d'imposta.

In quanto assimilate a valute estere è interessante quanto espresso dall'Articolo 67 del Testo unico delle imposte sui redditi (TUIR) al Comma 1, lettera c) ter di cui si cita uno stralcio:

[27] Imposta sul valore aggiunto: è un'imposta generale sui consumi.
[28] Un'operazione in cambi a pronti è una transazione in cui si ha il trasferimento immediato di una somma espressa in una valuta in cambio di un'altra somma espressa in un'altra valuta sulla base dell'attuale valore del tasso di cambio (tasso di cambio a pronti) [fonte: Borsa Italiana]

[…] Le plusvalenze realizzate mediante cessione a titolo oneroso di partecipazioni qualificate. Costituisce cessione di partecipazioni qualificate la cessione di azioni, diverse dalle azioni di risparmio, e di ogni altra partecipazione al capitale od al patrimonio delle società […] (Decreto del Presidente della Repubblica, 1986)

Concretamente questo vuol dire che se su un wallet si detiene un ammontare che supera la giacenza media in euro di 51.645,69 per almeno 7 giorni lavorativi: sono soggetti ad imposta.
In questo caso se i digital asset sono detenuti all'interno di un custodial wallet c'è l'obbligo di dichiarazione e compilazione del quadro RW in accordo con l'art. 4 DL 167/90:

[…] Le persone fisiche, gli enti non commerciali e le societa' semplici […] residenti in Italia che, nel periodo d'imposta, detengono investimenti all'estero ovvero attivita' estere di natura finanziaria, suscettibili di produrre redditi imponibili in Italia, devono indicarli nella dichiarazione annuale dei redditi. […] (Gazzetta Ufficiale della Repubblica Italiana, 1990)

Invece, non è previsto il monitoraggio nel caso in cui un privato detiene dei digital asset su wallet fisico (hardware) ed è in possesso delle chiavi private.

Considerando invece l'aspetto legale relativo all'antiriciclaggio la normativa italiana di riferimento è oggi rappresentata dal decreto legislativo 21 novembre 2007, n. 231, da ultimo modificato dal D.Lgs. 4 ottobre 2019, n. 125, dove vengono introdotti quattro punti chiave nella regolamentazione delle attività crypto.

Di seguito alcuni stralci della normativa:

[…] Valuta virtuale: la rappresentazione digitale di valore, non emessa ne' garantita da una banca centrale o da un'autorita' pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalita' di investimento e trasferita, archiviata e negoziata elettronicamente. […] (Gazzetta Ufficiale della Repubblica Italiana, 2019)

[…] prestatori di servizi relativi all'utilizzo di valuta virtuale: ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute […] (art. 1, comma 2, lett. ff). (Gazzetta Ufficiale della Repubblica Italiana, 2019)

[…] wallet provider: ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche on line, servizi di salvaguardia di chiavi crittografiche private per contro dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali […] (art. 1, comma 2, lett. ff bis). (Gazzetta Ufficiale della Repubblica Italiana, 2019)

[…] operatori non finanziari: i prestatori di servizi relativi all'utilizzo di valuta virtuale (i) e i prestatori di servizi di portafoglio digitale […] (i-bis). (Gazzetta Ufficiale della Repubblica Italiana, 2019)

4.4. Scenario legislativo Mondiale

Come si è analizzato anche nei paragrafi precedenti la rapida diffusione delle criptovalute ha suscitato forti attenzioni nell'intero panorama governativo mondiale.

Ovviamente questo scenario è in continua evoluzione e costante crescita e di seguito si propone una disamina ad alto livello delle maggiori giurisdizioni.

Come si può notare nel grafico in Figura 17 la maggior parte delle giurisdizioni globali ha sviluppato un regolamento per cui è necessaria una licenza VASP (Virtual Assets Service Provider) per avviare cripto attività.

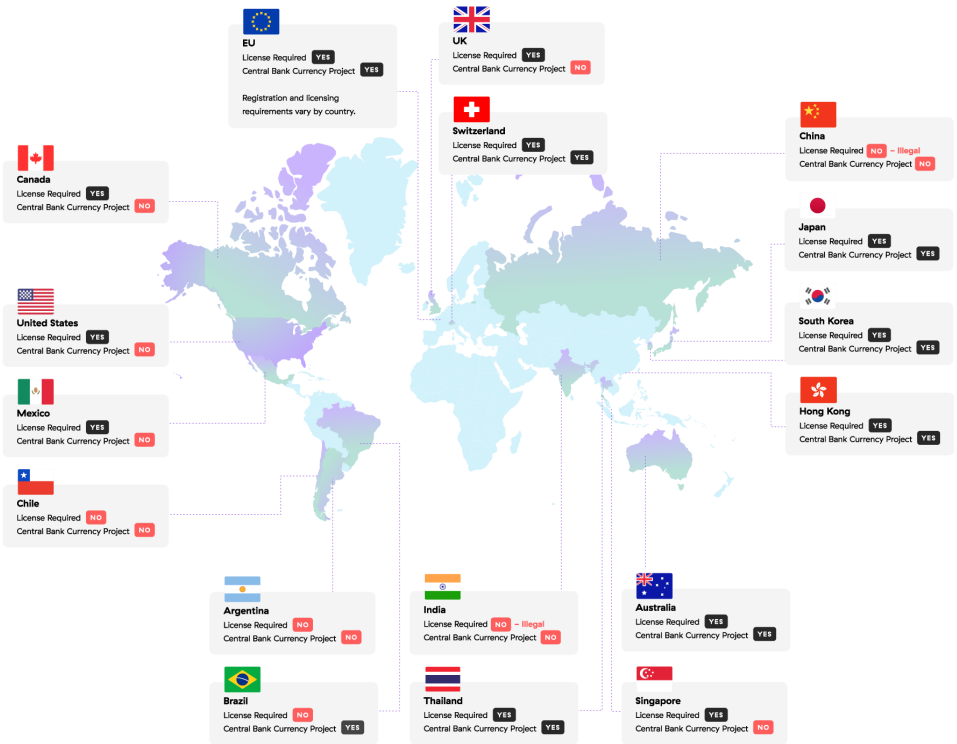

Figura 17: Rappresentazione geografica delle regolamentazioni globali sulle criptovalute. [Fonte: Comply Advantage]

Salta subito all'occhio però che alcune di esse sono ancora restie ad una adozione di tali attività. Infatti Cina, Cile, Argentina, Brasile e India hanno politiche molto restrittive riguardo le cripto attività.

4.4.1. Scenario Statunitense

Negli Stati Uniti, così come in molti altri stati, le criptovalute non sono considerate monete legali e ci sono molte norme per regolamentare gli Exchange.

Anche negli USA è molto difficile e tortuoso il percorso di regolamentazione, ma è molto interessante notare l'interpretazione dell'Agenzia governativa Financial Crimes Enforcement Network (FinCEN) per cui le criptovalute non sono considerate valute legali, ma gli scambi di quest'ultime rappresentano una trasmissione di denaro[29] sulla base del fatto che i token sono a tutti gli effetti "un altro valore che sostituisce la valuta".
D'altro canto l'Internal Revenue Service (IRS) non considera anch'esso le criptovalute come valuta legale, ma le definisce come "una rappresentazione digitale di valore che funziona come mezzo di scambio, unità di conto e/o riserva di valore" e ha emesso una guida fiscale di conseguenza[30].

Quindi, sebbene le criptovalute in sé non sono valute legali, gli scambi di quest'ultime sono legali e rientrano nell'ambito normativo del Bank Secrecy Act (BSA)[31]. In pratica, questo vuol dire che i fornitori di servizi

[29]https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering
[30] https://www.irs.gov/newsroom/irs-virtual-currency-guidance
[31] Il Bank Secrecy Act (BSA) è il più importante regolamento antiriciclaggio degli Stati Uniti: le banche e le altre istituzioni finanziarie devono assicurarsi di soddisfare gli obblighi di conformità che comporta.

di scambio di criptovalute devono ottenere la licenza richiesta dalla FinCEN, implementare un programma di antiriciclaggio (AML/CFT) e sanzioni, mantenere registri e presentare rapporti alle autorità con una certa frequenza.
Inoltre, negli Stati Uniti i cripto asset sono stati equiparati a titoli mobiliari dalla Securities and Exchange Commission (SEC), analogamente all'Europa, e quindi vengono applicate leggi su quanto detenuto e scambiato da e verso i wallet digitali.[32]

Molto interessante la considerazione del Commodities Futures Trading Commission (CFTC) che ha riconosciuto le principali criptovalute, quali Bitcoin e Ethereum, come materie prime e di conseguenza permettendo la creazione di derivati virtuali e criptovalute di essere scambiate pubblicamente su exchange regolamentati.

In conclusione si può affermare che le singole autorità presenti sul territorio americano si stanno muovendo per trovare il giusto compromesso per assicurare un'efficace protezione dei consumatori e una supervisione normativa più snella. (Comply Advantage, 2020)

4.4.2. Scenario Cinese

Completamente opposto invece l'approccio sul fronte Orientale. Infatti in Cina l'autorità principale, la People's Bank of China (PBOC) ha vietato alle istituzioni finanziarie di gestire le transazioni di Bitcoin nel 2013 ed è andata oltre vietando le ICO e gli scambi di criptovalute nazionali nel 2017. Nel giustificare il divieto, la PBOC ha descritto il finanziamento ICO (che raccoglie valute virtuali come Bitcoin o Ethereum attraverso la

[32] https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

vendita irregolare e la circolazione di token) come un finanziamento pubblico senza approvazione che è illegale secondo la legge cinese. Non sorprende che la Cina non consideri le criptovalute come valute legali, infatti il Paese ha una reputazione globale per le severe norme di controllo valutario sulla maggior parte delle valute straniere.
Con un emendamento del 2020 al codice civile cinese, il governo ha stabilito che le criptovalute approvate dallo stato hanno lo status di proprietà ai fini della determinazione delle eredità.

Nonostante l'illegalità totale delle criptovalute è interessante notare che le attività di mining sono consentite e inoltre è comunque consentito l'utilizzo di piattaforme crypto regolamentate al di fuori della giurisdizione cinese.

Sebbene possa sembrare che la Cina ponga un freno drastico all'adozione delle criptovalute, in verità l'obiettivo nel lungo periodo è quello di affermarsi come protagonista dello scenario crypto.

Infatti, sono in corso sviluppi che includono dichiarazioni di funzionari del governo cinese che approvano la tecnologia blockchain.
In particolare è da precisare che il governo cinese lavora all'introduzione di una valuta digitale ufficiale dal 2012: infatti è in corso un'ampia sperimentazione e test di una Central Bank Digital Curreny attraverso cui emettere uno yuan totalmente digitale.
Ci sono evidenze di avanzamenti anche attraverso una joint venture con SWIFT (il gateway di pagamento internazionale e transfrontaliero), e il continuo status del crypto mining.

Al fine di portare avanti queste attività, alla fine del 2020, il governo cinese ha redatto una legge che conferisce uno status giuridico allo Yuan digitale

della PBOC: la legislazione dovrebbe portare alla scomparsa della valuta fiat, e all'introduzione di controlli valutari su misura che coprono gli scambi e la fungibilità della valuta.

Secondo un rapporto pubblicato dall'Institute of Interationa Finance, il governo cinese ha anche espresso il suo sostegno per l'attuazione di un quadro normativo globale per le criptovalute. (Comply Advantage, 2020)

Capitolo 5
Caso Studio Sperimentale

Di seguito si propone la redazione di un Whitepaper relativo ad un potenziale caso d'uso della tecnologia Blockchain in ambito finanziario e commerciale.
L'elaborato consiste nella definizione di un piano di impresa comprensivo di analisi di mercato, definizione della soluzione tecnologica e rappresentazione del profilo finanziario.
Il nome della soluzione tecnologica è Green Renewable Energy Protocol.

5.1. Executive Summary

5.1.1. Business Statement

Green Renewable Energy Protocol è una soluzione basata su blockchain Polygon che garantisce un anticipo sui flussi di cassa a istituti di credito che erogano finanziamenti per progetti di transizione energetica, attraverso la tokenizzazione dei finanziamenti stessi, rendendo il debito liquido e spendibile in un mercato retail.

5.1.2. Problema

Anche se attualmente sono presenti forti incentivi a livello governativo in tutte le giurisdizioni per promuovere sempre di più le fonti di energia rinnovabili, le aziende di produzione di energia elettrica sono ancora molto ancorate all'uso e all'emissione di fonti non rinnovabili come quelle carboniche, quali gas e petrolio: per esempio in Asia l'utilizzo di fonti di energia non rinnovabili copre il 70%.

Nel contesto europeo è presente la Direttiva 2009/28 del Parlamento europeo e del Consiglio sulla promozione dell'uso dell'energia da fonti rinnovabili (FER), la quale assegna ai singoli Paesi membro degli obiettivi nazionali. In particolar modo relativamente all'Italia:

- una quota dei consumi finali lordi complessivi di energia coperta da fonti rinnovabili almeno pari al 17% (obiettivo complessivo, o overall target);
- una quota dei consumi finali lordi di energia nel settore dei Trasporti coperta da fonti rinnovabili almeno pari al 10% (obiettivo settoriale trasporti).

L'Italia ha dimostrato di aver raggiunto gli obiettivi imposti, fino ad arrivare a coprire il 18,2% dei consumi finali lordi complessivi nel corso del 2019[33]. (Gestore Servizi Energetici, 2021)

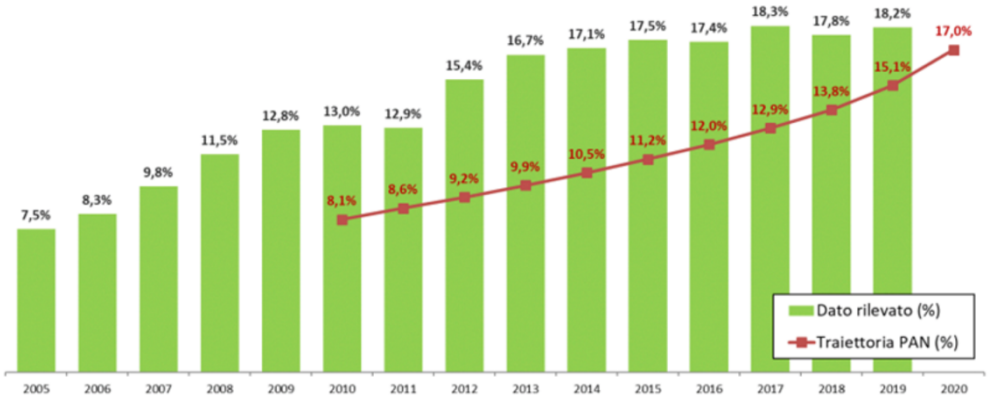

Figura 18: Quota dei consumi finali lordi di energia coperta da FER (Overall target fissato dalla direttiva europea 2009/28/CE). [fonte: GSE]

33 https://www.gse.it/documenti_site/Documenti%20GSE/Rapporti%20statistici/Rapporto%20statistico%20di%20monitoraggio%20di%20cui%20al%20DM%2011-5-15%20art%207_anni%202012-2019.pdf

Ma questo non basta a velocizzare il processo di innovazione. Infatti, le aziende energetiche sostengono costi molto elevati per implementare impianti performanti e sostenibili, quindi le tempistiche per rientrare negli investimenti sono spesso molto lunghe e pertanto alcune aziende decidono di accelerare il processo indebitandosi sul mercato ricorrendo a forme di finanziamento come i Corporate Bond o obbligazioni societarie.
Inoltre, molte aziende ricorrono a finanziamenti sostenibili presso Istituti di Credito.
In una obbligazione societaria l'emittente, ossia il debitore, è rappresentato da una società privata (non appartenente alla pubblica amministrazione). Ogni titolo rappresenta una frazione di uguale valore nominale e con uguali diritti, di un'unica operazione di finanziamento. Il possessore dell'obbligazione diventa creditore della società emittente e ha diritto di ricevere il rimborso a scadenza dell'importo previsto dal regolamento del prestito più una remunerazione a titolo di interesse. (Borsa Italiana, s.d.)
Ma queste operazioni, bond o semplici prestiti, sono spesso onerose in termini di tempo (scadenze lunghe) e non sempre convenienti dal punto di vista delle aziende (interessi in genere alti). Inoltre, sono molto complesse dal punto di vista burocratico.

Un'altra modalità per incentivare la Ricerca e lo Sviluppo consiste nell'investire, da privato, in fondi tematici sostenibili appellandosi ad una Società di Gestione del Risparmio o ad una Istituzione Finanziaria, oppure investire autonomamente in titoli mobiliari direttamente nelle aziende energetiche quotate.
Va senza dire che questa, come tutte le forme di investimento comporta un certo grado di rischio e inoltre, l'azienda è condizionata da trend di mercato e da "esseri umani" i quali possono commettere errori compromettendo l'andamento effettivo del business dell'azienda. Si investe nelle persone piuttosto che nella causa.

5.1.3. Call to Action

Secondo un report di BloombergNEF, nel 2021 gli investimenti per la transizione energetica hanno toccato quota $755 miliardi (+27% rispetto al 2020). A ciò si aggiungono ben $165 miliardi investiti in aziende del settore attraverso il mercato azionario e venture capital/private equity.

Energia rinnovabile e trasporti sono le due categorie che hanno beneficiato maggiormente del capitale a disposizione, con rispettivamente $366 miliardi (+6.5% vs 2020) e $273 miliardi (+77% vs 2020). (Starting Finance, 2022)

La regione dell'Asia-Pacifico si conferma leader con ben $368 miliardi investiti (49% del totale). Tra tutti spicca la Cina, prima a quota $266 miliardi, con un aumento del 60% rispetto all'anno precedente. A completare il podio Stati Uniti ($114 miliardi) e Germania ($47 miliardi).

Per raggiungere l'obiettivo net-zero emissions entro il 2050, saranno necessari circa $125 000 miliardi. Per tale motivo, nei prossimi anni gli investimenti dovranno crescere a tassi più sostenuti.

In Italia, sono sempre di più le aziende che stanno valutando l'emissione di climate bond, con un mercato che conta 18.8 miliardi di dollari. (BloombergNEF, 2022)

Entro il 2023, si prevede che il mercato dei green bond avrà un valore di 1 trilione di dollari.

5.1.4. Soluzione

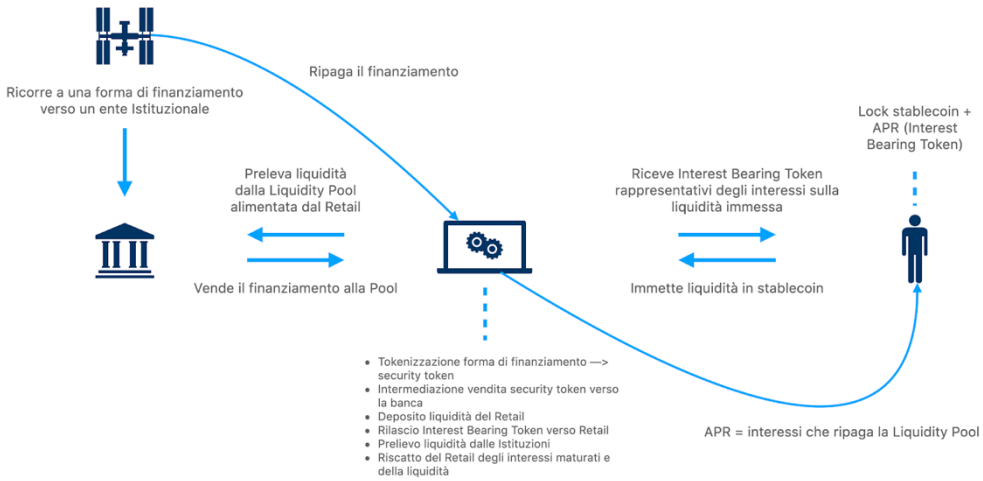

Figura 19: Rappresentazione ad alto livello del funzionamento dell'applicativo. [fonte: elaborazione personale]

L'obiettivo è quello di creare una piattaforma che permetta agli Istituti di Credito di tokenizzare finanziamenti nella transizione energetica al fine di ottenere un ritorno sul capitale investito in tempi più brevi e concedere la possibilità al Retail di sentirsi parte attiva nella corsa alla sostenibilità alimentando il network.

5.2. Organizzazione

5.2.1. Mission Aziendale

Sostenere una maggiore sensibilizzazione delle Istituzioni Finanziarie e dei Privati in materia di sostenibilità e temi ESG con focus sulla transizione energetica creando una nuova forma di investimento in grado di accelerare il processo di riduzione delle emissioni dannose.

5.2.2. Scopi e obiettivi dell'azienda

- Sviluppo e gestione della piattaforma;
- Promozione della piattaforma attraverso attività di engagement e sensibilizzazione dei key partners;
- Raccolta ed analisi dei dati;
- Stringere partnership con aziende tecnologiche per incrementare il traffico sulla piattaforma.

5.3. Soluzione Tecnologica

5.3.1. Scelta della Blockchain

Polygon è un layer di secondo livello che opera sulla blockchain di Ethereum. Questa soluzione funziona su una blockchain esistente anziché utilizzare una blockchain di layer 1 o costruita ad hoc. In questo caso, Polygon funziona sulla base di Ethereum, diventato più lento e costoso (GAS fee troppo alte per operazioni semplici/quotidiane) proporzionalmente all'incremento dell'utilizzo.

Il progetto di Polygon è nato con l'obiettivo di risolvere questa problematica ma sta facendo progetti più ampi per il futuro: l'obiettivo è fornire un framework per le reti blockchain. Gli utenti sarebbero in grado di creare reti blockchain che si interconnettono tra loro ed evitare di creare bridge per lo scambio di informazioni inter-chain.

Questo potrebbe offrire agli sviluppatori il meglio di entrambi i mondi. Possono creare le proprie blockchain standalone con tutti i vantaggi che offrono, tra cui scalabilità e flessibilità. Avrebbero anche i vantaggi offerti da Ethereum, inclusa la sua sicurezza e gli strumenti disponibili attraverso di esso.

Ethereum Virtual Machine (EVM) è una macchina virtuale che gli sviluppatori possono utilizzare per creare le proprie app decentralizzate. In parte a causa della facilità d'uso dell'EVM, in parte per la popolarità della blockchain stessa, Ethereum è diventata la piattaforma più popolare per le app decentralizzate.

Polygon è compatibile con EVM, quindi gli sviluppatori possono facilmente trasferire le loro app sulla piattaforma. (Comandini, 2021)
Ciò è possibile grazie all'architettura tecnica sottostante di Proof-of-Stake (PoS) e alla soluzione di scalabilità L2 More Viable Plasma (MoreVP). La blockchain basata su PoS ha attirato circa 80 dApp sulla piattaforma, la quale non ha subito eccessivi rallentamenti per l'utilizzo della rete.

Polygon prevede di destinare 100 milioni di dollari del finanziamento a un "fondo ecosistemico" a sostegno dello sviluppo di nuovi progetti sulla sua rete. Il resto servirà come "denaro tampone" per aiutare il team di 240 persone di Polygon a continuare a costruire la piattaforma negli anni a venire.

La scelta dell'utilizzo di Polygon risolve i seguenti requisiti:

- Bassi costi di transazione: i costi di transazione per l'utilizzo di questa soluzione sono molto bassi;
- Bassi consumi di utilizzo: i validatori di Polygon consumano circa 0,00079 TWh di elettricità all'anno con un consumo continuo approssimativo di 0,00009 GW, ordini di grandezza inferiori al consumo energetico delle principali reti blockchain PoW;
- Integrazione con DEX: l'ecosistema Polygon è integrato con diversi DEX che possono permettere lo scambio di token (con stablecoin o viceversa). È possibile determinare lo scambio per stablecoin attraverso DEX già esistenti o è possibile costruirne uno ad hoc che però si basi su una blockchain già chiara ed operativa, con grande documentazione e casi d'uso funzionanti operativi sul mercato;
- Scambio per StableCoin: Polygon prevede lo scambio di stablecoin per token ERC-20. I token scambiati saranno quelli contenuti nella pool di UT verso i portafogli Metamask degli utenti. Sono disponibili sia USDT sia USDC;
- Smart Contract: la possibilità di programmare smart contract direttamente sulla blockchain è fondamentale per delineare i processi automatici del progetto, quali gli strumenti di validazione e gli strumenti di intermediazione tra portafogli. In questo caso, pur avendo delle fee di transazione molto basse, il rischio di attacchi Ddos è limitato in quanto lo smart contract per l'approvazione della tokenizzazione del debito funziona solamente dopo KYC e whitelist mentre per il lock/unlock delle stablecoin i tempi di scelti per evitare speculazioni fanno si che questo tipo di attacco sia impossibile da attuare.

Il fatto di essere basata su Ethereum, in secondo luogo, amplia la base informativa tecnologica e fa sì che, essendo questo servizio offerto in primo step alle istituzioni finanziarie, crei fiducia nel mezzo. E' stato ipotizzato di utilizzare anche altre blockchain (ad es. Terra) che risolve tutti i requisiti e ha già progetti simili che usano quasi lo stesso modello di processo (ad es. Anchor) ma per questioni di affidabilità e fiducia si è deciso di restare su Polygon che mantiene tutti i vantaggi sopra elencati basandosi sulla EVM.

5.3.2. Funzionamento Generale

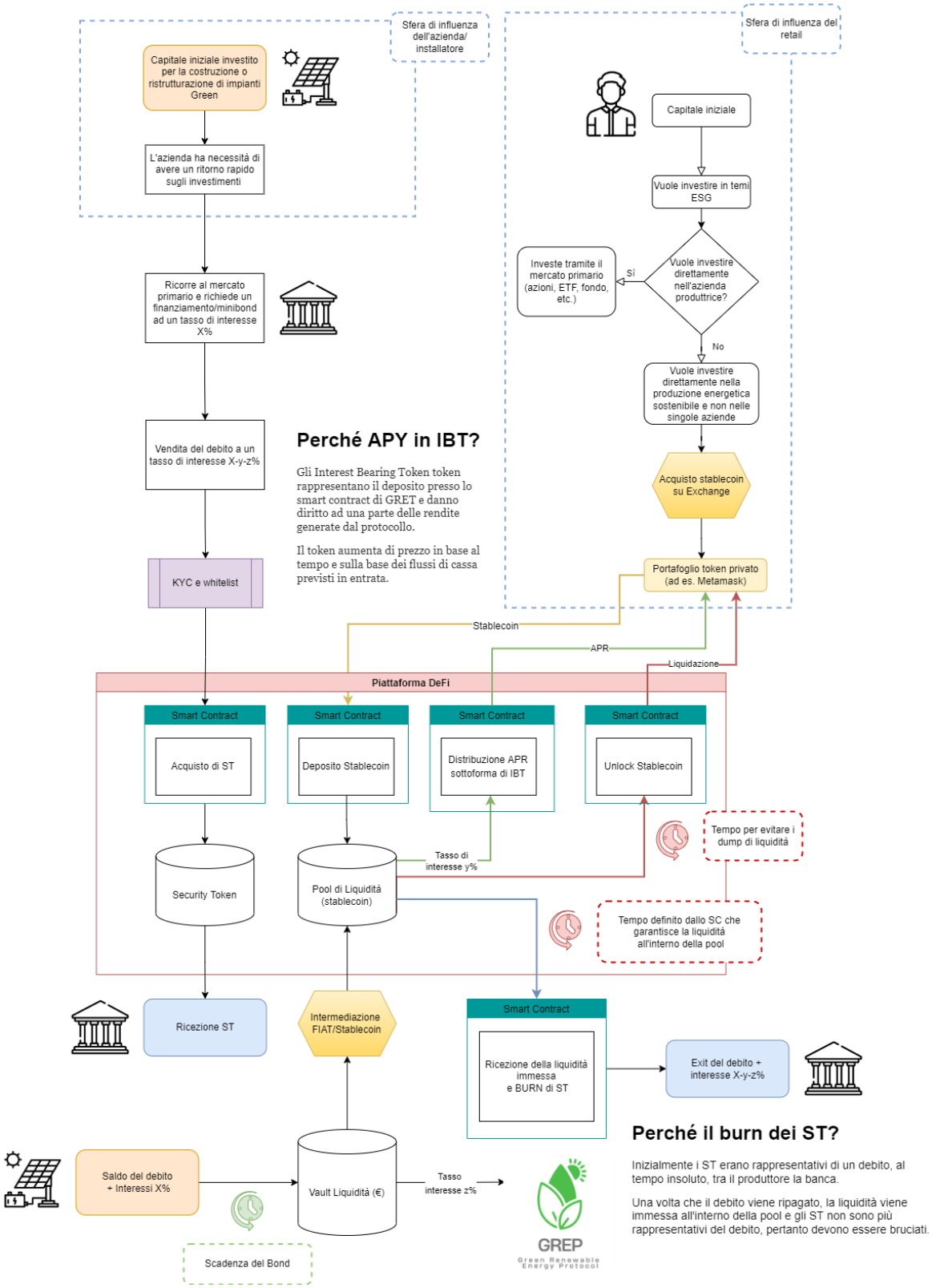

Figura 20: Rappresentazione di dettaglio della soluzione tecnologica. [fonte: elaborazione personale]

5.3.3. Funzionamento di dettaglio

Premessa: la decisione di collateralizzare solamente debiti volti all'innovazione/costruzione di impianti di energia rinnovabile è una scelta arbitraria che in caso di modifica dell'ambiente macroeconomico può essere cambiata e adattata alla situazione corrente. Il protocollo di collateralizzazione debiti è sufficientemente flessibile per lavorare con diverse tipologie di finanziamento (bonds, loans, etc.) e con diverse fonti di ingresso capitale lato SGR/IdC/Fondi di investimento.

Produttore Impianto

Le aziende di produzione energetica sostengono costi molto alti di implementazione e il riammodernamento degli impianti, di conseguenza hanno bisogno di molto tempo per raggiungere il break even point. La piattaforma dà la possibilità di collateralizzare il nuovo impianto, sulla base dei debiti contratti per finanziare queste installazioni/ammodernamenti per abbattere le emissioni di CO2 e/o l'impatto ambientale.

Questo attore è di fatto trasparente al flusso, in quanto non si approccia mai ai funzionamenti interni di tokenizzazione e/o "holda" token, ma ripaga un debito con un interesse di X% che ha stipulato con un istituto di credito attraverso uno strumento finanziario come ad esempio un bond.

Il produttore di energia elettrica, alla fine del processo, ripagherà questo debito non più sul conto corrente "dell'istituto di credito" ma su un conto corrente concordato. Il contenuto sarà poi trasferito all'interno della liquidity pool attraverso la conversione del valore FIAT in stable coin.

Una parte di quel valore (lo z% degli interessi pagati dal produttore e descritti all'interno del bond) saranno il guadagno che l'azienda GREP tratterà come revenue.

Istituto di credito

L'istituto di credito, a prescindere dalla presenza del flusso sopra disegnato, può emettere dei bond per finanziare la costruzione/ammodernamento di impianti di energia elettrica con fonti rinnovabili e/o sostenibili.
Uno degli elementi che potrebbe discernere gli investimenti accettabili da quelli non accettabili è l'aderenza alla tassonomia green europea che spiega ed elenca quali sono le fonti di energia considerate "green" a livello ambientale. (European Commission, s.d.)

Il bond, tuttavia, ha spesso una scadenza che può essere stimata in anni: solitamente, i bond nel settore privato hanno un tempo di maturità che varia da 1 a 30 anni, dove mediamente i bond a medio termine sono in preponderanza (5-12 anni). (Kelly, 2021)
La banca, per poter fare una exit prematura da questa scadenza prefissata, potrebbe decidere di "cedere il debito" ad una pool di liquidità in cambio di una perdita sul guadagno calcolato sugli interessi.
Ad esempio, sapendo che il bond è stato firmato con un tasso di interesse di X%, l'istituto di credito potrebbe decidere di accettare e cedere il debito avendo una percentuale di:

- **X%** = interesse definito nel bond
- **y%** = interesse da destinare alla pool di liquidità per l'acquisto del debito e successiva liquidazione
- **z%** = interesse da destinare come revenue alla società di GREP

Pertanto cederà il debito e incasserà un interesse che sarà definito da (X-y-z)%.

L'istituto di credito, una volta ceduto il debito alla pool di liquidità, riceverà in cambio dei Security Token (GRET) che rappresentano il debito ceduto. Ad esempio, calcolando che 1 GRET = 1 USD, potremmo definire che l'istituto di credito che cede un debito di 5 mln di USD + 5% di interessi sulla quota capitale, potrà avere 5mln di GRET + 2% di GRET sulla quota capitale, potendo stimare che il 2% sarà l'interesse in revenue della pool di liquidità e l'1% sarà il guadagno dell'azienda di GREP.

La liquidazione dei GRET non potrà essere attuata immediatamente in quanto il pool di liquidità deve poter sostenere l'exit dell'azienda pur mantenendo all'interno la possibilità di garantire l'exit degli investitori retail. Pertanto, possono vedersi applicati due scenari:

- **Best scenario**: l'azienda vende il debito alla liquidity pool e farà l'exit del debito ad un tasso di interesse X-y-z% ad un tempo minore di quello posto alla maturity date del bond
- **Worst scenario**: la liquidazione del debito potrà avvenire alla maturity date del bond ad un tasso di interesse di X-y-z%.

Una volta poste le condizioni nella liquidity pool per la liquidazione della società e lo scambio dei GRET per USDT/USDC, l'azienda riceverà le stablecoin sulla base dei GRET detenuti. Lo smart contract, di conseguenza, brucerà un GRET per ogni USDT/USDC ricevuto in cambio (in quanto GRET era rappresentativo di un debito che è stato saldato).

Retail

Il retail, attraverso questa piattaforma DeFi, cerca un rendimento a lungo termine tenendo in uno stato di lock la propria liquidità (stablecoin) all'interno di una liquidity pool. La liquidità del retail servirà per garantire un anticipo sull'exit dell'istituto finanziario in modo da coprire il tempo t0 -> t maturity date.
Il pool di liquidità sarà successivamente reintegrato al maturity date dell'ammontare del debito + y% di interessi che viene destinato alla pool come revenue.

Questi interessi andranno a capire le APR dei retail (revenue per aver partecipato al locking della liquidità) che saranno pagate in a-gret.
a-gret sono interest bearing token, ossia prove che il retail ha prestato dei soldi al pool di liquidità. Gli a-GRET sono "mintati" al momento del deposito e vengono bruciati quando riscattati, sono ancorati 1:1 al valore dell'asset sottostante che è depositato nel protocollo di GREP.
Mentre l'asset sottostante viene liquidato agli istituti finanziari (in attesa di essere rifinanziato dal saldo del debito da parte dell'impresa di produzione energetica), gli a-gret accumulano interessi in tempo reale, direttamente nel portafoglio del retail. Di fatto rappresentano una quota in un pool di prestiti che cresce di dimensioni man mano che i mutuatari pagano gli interessi.

Il retail potrà decidere di uscire una volta terminato il periodo di lock delle proprie stablecoin all'interno del pool (inizialmente sarà più alto per evitare il drenaggio della liquidity pool, potenzialmente con l'aumento del capitale in ingresso e con la stabilizzazione dei flussi di cassa, questo periodo di lock potrà considerarsi sempre più breve). Una volta ricevuti il

capitale precedentemente bloccato, non riceverà più a-gret in quanto non sono più rappresentativi di un capitale messo a disposizione della pool.

I token a-GRET potranno essere scambiati per USDT/USDC in qualsiasi momento da parte del retail.

La percentuale di a-GRET ricevibili varia al variare degli interessi disponibili alla distribuzione (y% trattenuto all'istituto finanziario) all'interno della liquidity pool.

5.3.4. Smart Contracts

Gli smart contract presenti all'interno della piattaforma avranno diversi ruoli:

- **Intermediari**: gli smart contract faranno da intermediazione standardizzata e meccanizzata tra ingresso e uscita nelle pool di token e nella liquidity pool. Questi faranno da ponte per quanto riguarda l'assegnazione dei Security Token agli istituti di credito, ponte per gestire la collateralità tra ST e UT e regolatori per il prelievo/immissione di liquidità nella liquidity pool.

- **Lock per APR**: lo smart contract per il calcolo del lock per le APR provvederà, per ciascun utente che decide di "lockare" i propri token per ricevere le APR, a definire il periodo di lock e di unlock dei token.

- **Lock Liquidity**: lo smart contract calcolerà la porzione di liquidità emissibile verso l'istituto finanziario in modo da

iniziare/completare l'estinzione del debito contratto dalla banca. Il calcolo sarà fatto in modo tale da garantire una exit a tutti i retail.

- **Distribuzione IBT (a-GRET)**: lo smart contract calcolerà, per ciascun retail partecipante al pool di liquidità, la quantità di a-GRET emettibili sul singolo wallet.

Nello specifico, nel modello possiamo trovare:

- **Smart Contract - Collateralizzazione del debito**: dopo il KYC e il whitelist dell'istituto di credito, quest'ultimo può avere accesso alla piattaforma per poter vendere il debito che l'impresa produttrice ha precedentemente stipulato con l'istituto. Questo debito viene collateralizzato dallo smart contract con l'emissione di un numero di GRET (security token) equivalente all'ammontare del debito comprensivo dei nuovi interessi calcolabile come X-y-z% (dove X sono gli interessi originari del bond, y sono gli interessi destinati alla liquidity pool, z sono gli interessi destinati all'azienda emettitrice di GREP).

- **Smart Contract - Deposito stablecoin**: uno smart contract definirà il periodo di lock (variabile in base alle condizioni di funzionamento dell'ecosistema) in modo tale da evitare bruschi e repentini drain della liquidity pool che potrebbero causare ritardi notevoli nella ricezione della liquidità da parte dell'istituto di credito. E' possibile supporre che il periodo di lock sia inversamente proporzionale alla quantità di liquidità presente nella pool, in quanto in capitale più alto è in grado di garantire una stabilità dei flussi di cassa maggiore.

- **Smart Contract - Distribuzione di APR sotto forma di a-gret**: il retail ha interesse nell'investimento in quanto bloccando le proprie stablecoin all'interno del protocollo di liquidità potrà ricevere in cambio un interest bearing token definito a-gret. Questi token rappresentano la prova che il retail ha prestato dei soldi al pool di liquidità. Lo smart contract, pertanto, inizierà a "mintare" questi token direttamente nel portafoglio del retail nel momento del deposito della liquidità e continuerà l'emissione con questi fattori:
    - **Frequenza**: la frequenza è possibile definirla in modo algoritmico per poter garantire stabilità all'ecosistema
    - **Quantità**: la quantità di a-gret "mintati" nel portafoglio del retail dipende dalla quantità di stablecoin messe in liquidity pool dal singolo. Pertanto, volendo dividere l'anno in secondi, è possibile immaginare che il retail alla fine del periodo riceverà una quantità di a-gret (o frazione di a-gret) che segue una formula come:

$$qGRET = (t_1 - t_0) * qRetail$$

      dove qGRET indica il totale di IBT ricevuti dal retail, (t1 - t0) è il numero di secondi passato dal momento del lock delle stablecoin al momento dell'unlock e qRetail è la quantità di stablecoin lockate all'interno del pool di liquidità dal retail.
    - **Valore**: il valore di a-gret è collateralizzato dalla liquidità immessa da parte dell'azienda produttrice e non dovuta all'istituto finanziario, rappresentata nel flusso dalla percentuale y%. Il valore, pertanto, è variabile sulla base di quanta liquidità di y% è rimasta all'interno del pool di liquidità.

- **Smart Contract - Ricezione liquidità**: al verificarsi di alcune condizioni, ossia il momento in cui lo smart contract ha calcolato che è possibile estrarre liquidità dalla liquidity pool garantendo ai retail coinvolti di poter estrarre i loro capitali tenendo in considerazione dei periodi di lock di ciascuno di questi, sarà possibile per la banca "prelevare" il capitale immesso inizialmente per pagare il debito dell'impiantista fino a una percentuale da definire. L'exit potrebbe essere anche parziale in quanto devono essere bruciati i GRET sulla base del capitale ricevuto in cambio. Ad es. se l'istituto finanziario ha ricevuto in un tempo t1 2mln $ su un debito di 5 mln $ inizialmente collateralizzato da GRET, dovrà bruciare 2 mln di GRET sul totale dei 5 mln attualmente in possesso. La percentuale y% sugli interessi inizialmente definiti sarà sempre lasciata nella pool per garantire le APR degli utenti retail che di, fatto, hanno partecipato ad un anticipo di flusso di cassa verso l'istituto di credito.

5.4. Modello Matematico

A sostegno del funzionamento generale della piattaforma si illustra di seguito il modello matematico che garantisce un corretto bilanciamento delle pool di liquidità che alimentano il flusso descritto precedentemente.

Si considerino le seguenti variabili:

- d = 1, 2, …D → Debiti
- p = 1, 2, …P → Privati
- b = 1, 2, …B → Banche

e l'istante corrente dell'anno rappresentativo dell'unità temporale (secondo), ossia:

- t = (1/ 31,536,000)

$I_{\{X\}}$ →Funzione indicatrice dell'evento "X"

y_d → tasso interesse a cui rinuncia la banca in favore della pool (fonte di APR)

z → tasso di commissioni GREP pagate dalla banca

ST → security token mintati a monte, valore 1:1 con USDT/USD

$Rata_{d,t}$ = rata del debito d pagata al tempo t

$Interesse_{d,t}$ = quota interesse, della rata del debito d, pagata al tempo t

$L_{p,t}$ = Stable coin versate dal privato p al tempo t

$LB_{p,t}$ = Liquidity Balance del privato p al tempo t

$\mu_{y,t}$ = Media dei tassi di interesse destinati ai privati, pesata per la quantità di debito nominale a cui afferiscono, su quella di debito totale

$w_{p,t}$= percentuale richiesta di prelievo dal privato p, dalla propria $LB_{p,t}$

$w_{b,t}$= percentuale richiesta di prelievo dell'istituto b, dalla propria $LB_{p,t}$

max_W^t = soglia massima di prelievo dalla pool calcolata istante per istante

ND_d= debito nominale del contratto d

TND_t= totale debito nominale in piattaforma

APR = Rendimento Percentuale Annuo (Annual Percentage Return)

Innanzitutto si definiscono le funzioni dei flussi in entrata (c.d., Inflows) o in uscita (c.d., Outflows) dalla pool, come:

$$LP_{INFLOWS_t} = \sum_{d}^{D} (I_{(rata_{d,t})} * rata_{d,t} - z_{GREP} * interesse_{d,t} + \sum_{p}^{P} L_{p,t}$$

$$LP_{OUTFLOWS_t} = \sum_{p}^{P} LB_{p,t}\ (\mu_{y,t} * t + w_{p,t} * I_{\{w_{p,t}LB_{p,t} \leq max_W^t\}}) + \sum_{b}^{B} STB_{b,t} * w_{b,t} * I_{\{w_{b,t}STB_{b,t} \leq max_W^t\}}$$

Di conseguenza, ad ogni istante t, la Liquidity Pool si alimenta nel seguente modo:

$$LP_t\ = LP_{t-1} + LP_{INFLOWS_t} - LP_{OUTFLOWS_t} = LP_{t-1} + \Delta LP_{FLOWS_t}$$

Ed infine si identifica come tasso di interesse medio per l'investimento del privato, la media dei tassi y, pesata per la quantità di debito a cui afferiscono, su quello totale:

$$\mu_{y,t} = \sum_{d}^{D} \frac{ND_{d,t}}{TND_t} * y_d$$

$$APR = \sum_{t}^{T} \mu_{y,t}$$

Il Rendimento Percentuale annuo è quindi calcolato secondo per secondo sulla media dei tassi di interesse destinati ai privati, pesata per la quantità di debito nominale a cui afferiscono, su quella di debito totale.

5.5. Analisi di Mercato

5.5.1. Metodologia

La metodologia si basa sull'analisi di 7 competitors che sono stati valutati e selezionati secondo una scala basata sulla maturità del mercato e l'importanza della proposta di valore.
Come primo passo sono state prese in considerazione più di 15 startup coinvolte nel trading P2P senza considerare il settore in cui operano. Successivamente, è stato avviato uno screening selettivo basato sul mercato dell'energia e sull'importanza dell'energia solare, consolidando un totale di 7 concorrenti. La selezione ha preso in considerazione variabili come: proposta di valore, punti di forza, debolezza, soluzione di servizio, strategia e decisioni chiave, stato economico e finanziario, scala delle partnership e dimensione dei clienti - assegnando a ciascuno delle variabili un punteggio da 5 a 15 considerando 5 basso, 10 medio e 15 alto in termini di maturità e importanza. Questa analisi ha permesso di strutturare una classifica delle startup che si può vedere nella matrice dove si apprezza l'impatto in termini di valore di business e di readiness del mercato italiano e internazionale considerando le barriere all'entrata e le dipendenze del mercato.

5.5.2. Matrice dei Competitor

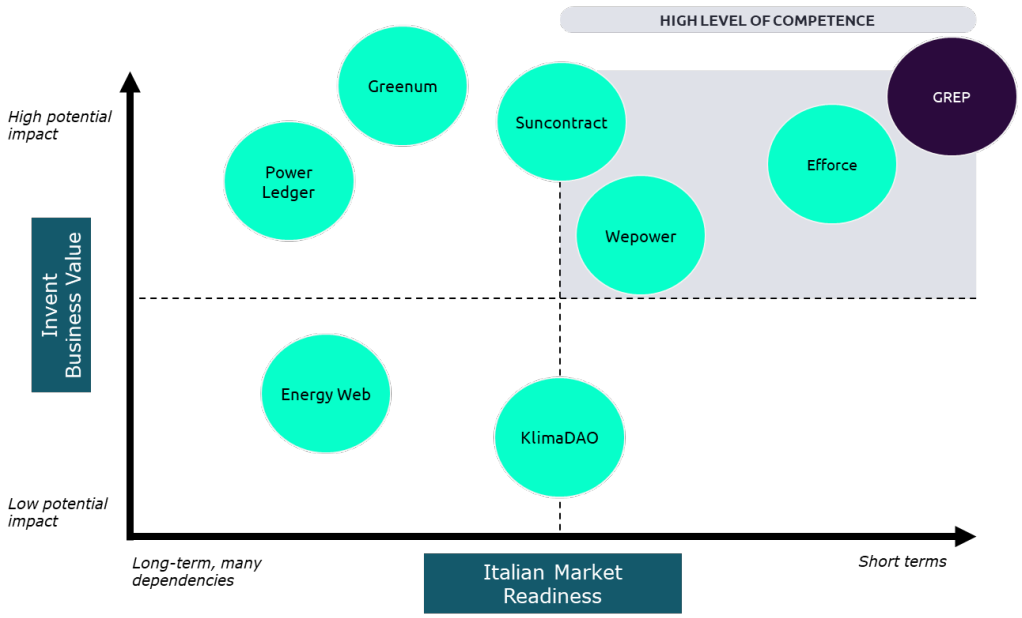

Figura 21: Matrice dei Competitor. [fonte: elaborazione personale]

Considerando altri fattori come la quota e l'attrattiva di mercato, durante la valutazione sono stati identificati tre potenziali concorrenti diretti:

Figura 22: Analisi di dettaglio dei tre competitor principali. [fonte: elaborazione personale]

Per quanto riguarda altri concorrenti, come EnergyWeb, operano su una piattaforma open source progettata per sostenere lo sviluppo di applicazioni del settore energetico che costruiscono un sistema energetico

più tracciabile, democratizzato e decarbonizzato. Gli obiettivi dei nostri concorrenti, in questo caso indiretto, possono variare in: fornire l'infrastruttura digitale che collega gli operatori di rete, i clienti e i beni fisici (come pannelli solari, termostati e veicoli elettrici) oppure attuare progetti di efficientamento energetico a favore di industrie o altri utilizzatori di energia, e tokenizzare il risparmio futuro.

5.5.3. Target e Posizionamento

Per posizionarsi in un buon quadrante rispetto al Retail, è necessario creare una strategia di identità e di visual identity. Verranno realizzate azioni e strategie pianificate in termini di comunicazione per attirare la visibilità e far sì che gli investitori abbiano interesse nella transizione energetica.
Dato l'alto interesse verso la sostenibilità e gli incentivi creati per l'investitore in termini di profittabilità, il posizionamento di mercato sarebbe alto in quanto si concentra su un attributo della piattaforma che la fa differenziare considerando altri concorrenti diretti, come per esempio l'emissione propria di security token. Attraverso la creazione di una pool decentralizzata il progetto permette agli investitori di sentirsi parte del processo di investimento in tematiche relative alle energie rinnovabili, il tutto disintermediando completamente il processo tramite la blockchain.

Il target primario sono le istituzioni finanziarie, in questo caso GREP è posizionato in un contesto istituzionale altamente specializzato, senza concorrenti nazionali, dove gli istituti bancari potrebbero beneficiare di un'alta competitività in un ambiente di business sempre più digitale. Il primo passo per coinvolgere gli istituti bancari, è la consapevolezza: esplorare come GREP può aiutarli ad attrarre nuovi clienti e prevenire la migrazione di quelli esistenti. Uno dei maggiori impedimenti nel settore

bancario è l'incoerenza normativa, quindi le banche devono sviluppare le proprie linee guida, che consistono in:

- Creare una mappa di calore regolamentare (strumento di ottimizzazione dei rischi) e condurre un'analisi delle lacune. Questo esercizio combinato dovrebbe coprire i regolamenti più rilevanti, anticipare i cambiamenti futuro, così come identificare la differenza tra i requisiti esistenti e i cambiamenti potenziali in ogni regione.
- Condurre una diagnosi di gestione del rischio per la propria attività. In questo esercizio, dovrebbero identificare e dare priorità alle iniziative con fondamenti blockchain.

Queste linee guida possono aiutare le istituzioni finanziarie a promuovere e incoraggiare la partecipazione a progetti come GREP, gestendo la maggior parte dei rischi materiali e tenendo conto dei regolamenti attuali e futuri.

5.5.4. Market Size

Per individuare la dimensione del mercato è stata fatta una analisi sulla dimensione del mercato attuale.

Secondo la fonte Bloomberg già citata nel corso del White Paper gli investimenti per la transizione energetica a livello globale ammontano a circa 755 miliardi di dollari. Di questi 755 miliardi di dollari il potenziale target di mercato relativo agli investimenti per le energie rinnovabili ammonta a 366 miliardi di dollari.

Il **Total Addressable Market** o il mercato disponibile totale considerato è prevalentemente quello europeo che ammonta a circa 61 miliardi di dollari.

Invece, sulla base di analisi statistiche del settore condotte da SNAM, il **Served Available Market** raggiungibile è presumibilmente quello italiano per un valore di 23 miliardi di dollari nel periodo 2021-2030.
Più precisamente come citato dal report di SNAM, nel medio periodo (2021-2025) sono stati previsti 8,1 miliardi di euro di investimenti, con un incremento complessivo di circa 700 milioni rispetto ai 7,4 miliardi di euro del Piano 2020-2024.
Il piano prevede la manutenzione, l'ammodernamento e lo sviluppo della propria infrastruttura, investimenti per il net zero e l'accelerazione della transizione energetica. Gli investimenti allineati alla tassonomia europea sono pari al 47% del totale (in aumento rispetto al 40% del precedente piano). (SNAM, 2021)

Di conseguenza il **Serviceable and Obtainable Market** o mercato realisticamente ottenibile che è stato ipotizzato ammonta al 5% del SAM (23 miliardi di dollari sul lungo periodo) per un totale di 1,15 miliardi dollari.

In figura si può notare graficamente l'analisi effettuata sulla dimensione del mercato target.

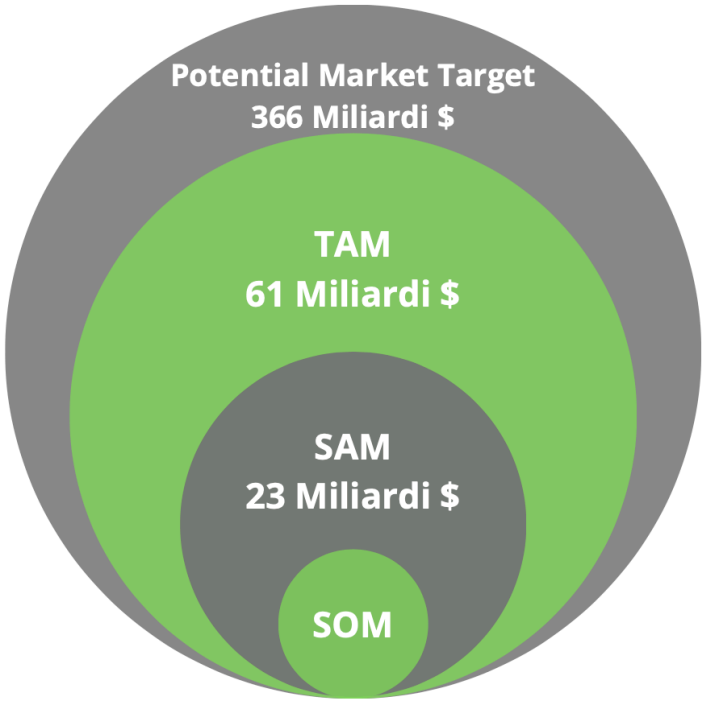

Figura 23: Rappresentazione grafica della dimensione del mercato attraverso l'analisi TAM, SAM, SOM. [fonte: elaborazione personale]

5.6. Strategia e Implementazione

5.6.1. Milestone di progetto

Il primo obiettivo che ci si pone è quello di realizzare un prototipo funzionante della piattaforma GREP tenendo in considerazione le principali fasi di un progetto di sviluppo software ponendo particolare attenzione allo studio di fattibilità e analisi dei requisiti.

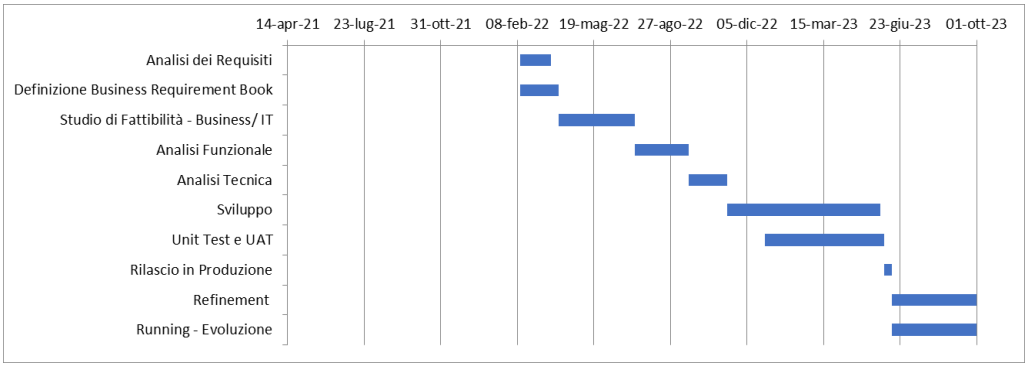

Figura 24: GANTT di alto livello elaborato con Excel. [fonte: elaborazione personale]

Si ipotizza la data di fine implementazione verso gli inizi di Ottobre 2023, mentre la parte di Refinement e Running sarà continua sulla base delle esigenze e requisiti.

5.6.2. Acquisizione Clienti Retail

È essenziale adottare tecniche di Search Engine Optimization, quindi su canali Web, affinchè la "Buyer Persona" target sia attratto dalla piattaforma. Ma, inoltre, il web è uno strumento essenziale per ottenere i dati dei potenziali clienti. Deve essere semplice, chiaro, di facile utilizzo e costruito mettendo l'utente al centro.

5.6.3. Acquisizione Istituzioni Finanziarie

Il problema principale relativo alle varie forme di finanziamento per progetti di natura efficientamento energetico sono spesso i lunghi tempi (dai 2 ai 5 anni per i prestiti, oltre i 5 per i bond) per ottenere indietro il capitale investito comprensivo di interessi.
Per cui l'obiettivo di GREP è proprio quello di ridurre queste tempistiche permettendo alle Istituzioni di vendere il proprio asset nella piattaforma in modo da recuperare più velocemente il capitale investito in fase iniziale

comprensivo di interessi e di conseguenza accelerare il processo di reinvestimento.

5.6.4. Strategia di prezzo e Revenue Streams

- Finanziamenti erogati da enti pubblici e privati;
- Attività di pubblicizzazione e sponsorizzazione da/verso terzi (negli anni a seguire);
- Commissioni su depositi di liquidità da parte del Retail;
- Commissioni sui flussi entranti da Aziende e Istituti Finanziari.

5.7. Piano finanziario e proiezioni

5.7.1. Spese di avvio e finanziamento

Le spese di avvio del progetto illustrate nella seguente tabella sono state ipotizzate tenendo conto del luogo geografico (Milano, Italia) e dei costi medi dei settori di riferimento. Per esempio per il costo dell'affitto è stato considerato un costo medio di 23,2€ al metro quadro e per i servizi professionali IT è stata considerata una media di mercato di 400€/gg uomo prendendo in considerazione le principali aziende operanti sul territorio Italiano.

Spese di avvio	
Costi Fissi	
Permessi e Spese Legali[34]	4.000 €
Costituzione SRL	3.000 €
Contabilità (1° anno)	4.000 €
Servizi Professionali IT	8.000 €
Deposito Cauzionale Affitto[35]	4.000 €
Allestimento e Arredamento Ufficio[36]	27.000 €
Sviluppo della Piattaforma (Comprensivo UI/UX)	25.000 €
Licenze Software (lunga durata o lifetime)	1.000 €
Strategia e Marketing	30.800 €
Operations	15.000 €
Allaccio Utenze (Internet, Elettricità, ecc.)[37]	500 €
Totale costi fissi	122.300 €
Costi medi mensili	
Affitto	2.000 €
Utenze (Luce, Gas, Acqua, ecc.)[38]	300 €
Stipendi / Salari	10.000 €
Tasse sui Salari (26%)	2.600 €

[34] https://www.lexdo.it/d/costituzione-societa-srl-srls/costi-srl-costituzione-gestione-annuali/

[35] https://www.mercato-immobiliare.info/lombardia/milano/milano/quotazione-ufficio.html
[36] https://www.ernesto.it/prices/arredare-un-ufficio
[37] https://luce-gas.it/trasloco/allacciamento
[38] https://www.facile.it/energia-luce-gas/tag/costo-kwh-aziende.html

Assicurazione sulla Salute	650 €
Assicurazione sulla Proprietà	650 €
Pubblicità digitale	400 €
Materiale Pubblicitario	350 €
Licenze Software (aggiuntive)	400 €
Ripari e Manutenzioni	200 €
Costi mensili medi totali	17.550 €
x Numero di mesi:	12
Costi mensili totali	210.600 €
Totale delle spese di avvio	332.900 €

Per cui al fine di avviare l'attività si considerano i seguenti Start-up asset:

Start-up Assets	
Finanziamento dei proprietari	
Fondi Proprietari	10.000 €
Finanziamento totale dei proprietari	10.000 €
Equity crowdfunding	
10% equity + ricavi futuri	170.000 €
10% equity + ricavi futuri	170.000 €
Totale altri finanziamenti	340.000 €
Totale attività di avvio	350.000 €

5.7.2. Analisi di pareggio

Considerando i parametri indicati nella tabella precedente rappresentante i costi di avvio si avranno dei costi fissi pari a **122.300 €,** costi mensili pari a **17.550 €** per un totale di **332.900 €.**

Dopo una attenta analisi di mercato sono stati definiti i seguenti parametri come assunzioni in entrata dal momento del lancio della piattaforma in produzione:

- Tasso X medio annuale dei finanziamenti tokenizzati = 6%
- Percentuale z interessi GRET = 1,5%
- Accantonamento in riserve/incentivi = 50%
- Durata media finanziamento (anni) = 5
- Tasso annuo di crescita dei finanziamenti tokenizzati = 20%

Sulla base dei parametri precedentemente indicati si evince nel grafico una crescita notevole delle Revenue.

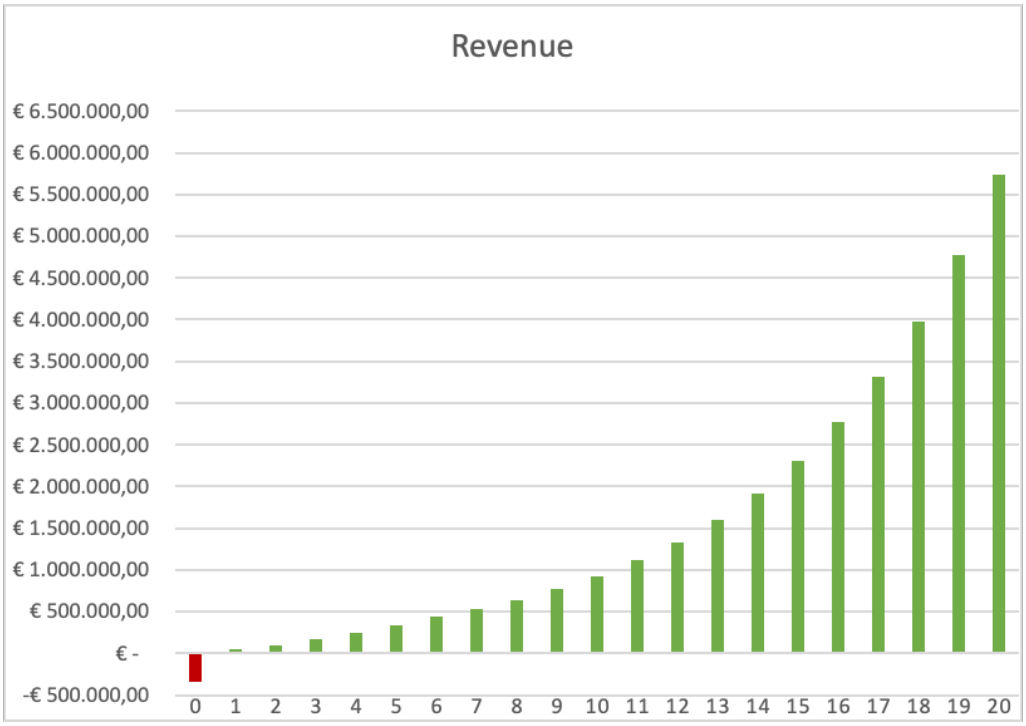

Figura 25: Elaborazione delle Revenue tramite Excel. [fonte: elaborazione personale]

Andando più nel dettaglio è stata condotta una breakeven analysis considerando i costi fissi e i costi medi mensili per un totale di circa 333k€.

Si può notare nel grafico come potenzialmente si raggiunga il break even già a partire dal terzo anno di attività.

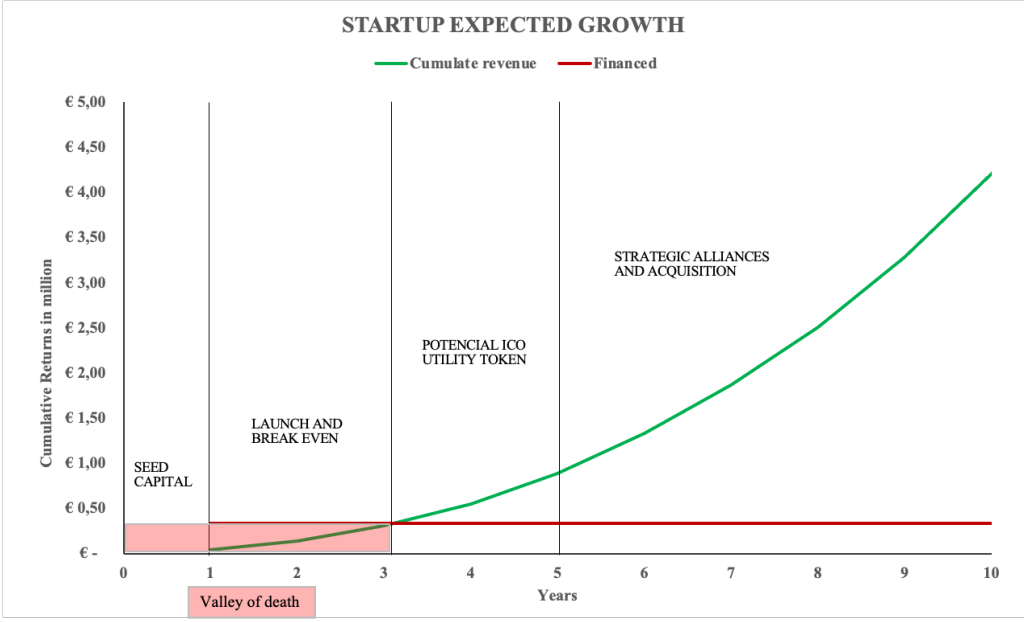

Figura 26: Elaborazione dell'aspettativa di crescita della Startup tramite Excel. [fonte: elaborazione personale]

5.8. Aspetti Legali

Al fine di un corretto inquadramento giuridico (riportato su scala europea) del progetto, occorre prendere in considerazione quattro aspetti principali:

- Realizzazione dell'impianto;
- Qualificazione giuridico fiscale dei token;
- Definizione elementi essenziali smart contract valutatori;
- Stablecoin – Nuove valutazioni della Banca Centrale Europea

5.8.1. Realizzazione dell'impianto

Il soggetto ("Produttore") che sia interessato alla costruzione / ristrutturazione di un impianto energetico green, ed alla sua successiva tokenizzazione, dovrà, in primis, munirsi di un capitale iniziale idoneo alla realizzazione del progetto.

Oltre a rivolgersi ad un istituto di credito che gli fornisca sufficiente autonomia economica, il Produttore potrà far affidamento anche sulle

proposte scaturite a seguito del Green Deal Europeo. (Commissione Europea, 2019)

Tale strategia, adottata dalla Commissione Europea, mira a trasformare l'Unione Europea in una economia moderna, efficiente sotto il profilo delle risorse e competitiva, garantendo che nel 2050 non siano più generate emissioni nette di gas serra e che la crescita economica sia dissociata dall'uso delle risorse.

Tra le tante iniziative promosse dalla Commissione Europea a sostegno di questo piano ecologico, occorre prendere in considerazione, in relazione a quanto sopra esposto, la comunicazione della Commissione Europea avente ad oggetto il "Piano di investimenti per un'Europa sostenibile. Piano di investimenti del Green Deal europeo". (Commissione Europea, 2020)

Tale documento prevede che nel prossimo decennio il piano di investimenti per un'Europa sostenibile permetterà di mobilitare, attraverso il bilancio dell'UE e gli strumenti associati, investimenti sostenibili privati e pubblici per almeno €1000 miliardi.

Il Produttore, pertanto, potrà (ove sia in possesso dei requisiti necessari per adirvi) ricevere finanziamenti da parte dell'Unione Europea e disporre così di risorse economiche iniziali maggiori.

Va però tenuto presente che tali fondi non saranno sufficienti a sanare il fabbisogno economico di ogni potenziale Produttore, ma fungeranno comunque da trampolino per la crescita e sviluppo del progetto, incentivando sempre più soggetti ad avvicinarvisi.

Una volta che il Produttore sia entrato in possesso del capitale iniziale, occorre che lo stesso ponga attenzione a:

leggi e relativi permessi necessari per la realizzazione di un impianto energetico;

qualifiche necessarie per poter produrre ed immettere sul mercato energia.

Tali certificazioni/permessi/documentazioni variano in base al paese in cui si vorrà realizzare l'impianto. Occorre pertanto che il Produttore faccia riferimento alle singole normative interne degli stati di riferimento.

5.8.2. Qualificazione giuridico fiscale dei token

Prima di procedere con la disamina fiscale dei token coinvolti nel progetto, occorre premettere che, pur in assenza di una definizione universalmente riconosciuta ed accettata in merito a come debbano essere giuridicamente qualificati i token, l'Autorità federale di vigilanza sui mercati finanziaria elvetica ("FINMA") ha proposto una condivisibile classificazione di tali strumenti, che essenzialmente attribuisce rilievo alla funzione economica ad essi, di volta in volta, sottostante. Più in particolare, occorre distinguere:

- i c.d. "payment token" o "currency token" → categoria di token equiparabile ad una valuta virtuale;
- i c.d. "utility token" → consentono l'accesso digitale ad un bene o ad un servizio;
- i c.d. "asset token" o "security token" o "investment token".

Rapportando la qualificazione fornita dalla FINMA al progetto, emerge come lo stesso preveda due distinte tipologie di token:

- security token: l'IdC, attraverso il security token GRET, finanzia il Produttore collateralizzando il debito con ST (comprensivi degli interessi al lordo della % da lasciare in liquidity pool e la % fee considerata revenue di GREP). I security token sono, pertanto, rappresentativi di porzioni di debito;
- Interest-Bearing Token.

Inquadramento fiscale "security token"

L'orientamento giuridico prevalente ha determinato che i security token attribuiscono ai titolari un diritto di partecipazione, patrimoniale o amministrativo, ovvero un diritto di credito nei confronti dell'emittente. Il loro scopo è, quindi, quello di essere utilizzati come forma di investimento e/o di creare flussi di cassa futuri. Gli stessi sono connessi a un'attività sottostante, ma sono rappresentativi soltanto di una frazione del suo valore complessivo. Ai titolari dei security token vengono, pertanto, offerti diritti sugli utili futuri dell'iniziativa sottostante e, a seconda delle categorie rinvenibili nei vari ordinamenti giuridici, possono essere considerati come prodotti finanziari, strumenti finanziari, valori mobiliari, etc.
La normativa italiana di riferimento prevede che ai security token si applichi quanto previsto dal Testo Unico delle Imposte sui Redditi relative agli strumenti finanziari e, in particolare, degli strumenti similari alle azioni o alle obbligazioni, a seconda delle caratteristiche in concreto dei token, con i conseguenti effetti fiscali che ne derivano, sia per gli emittenti che per i sottoscrittori[39].

Note fiscali

[…] Nella breve disamina sopra effettuata si è cercato di dar conto di alcuni principi generali in materia di fiscalità di cryptoasset, alla luce degli orientamenti dell'Amministrazione finanziaria e delle norme tributarie.
Al riguardo, occorre considerare che il quadro al momento non può certamente definirsi completo, e ci si aspetta che l'ulteriore espansione ed evoluzione di tali asset possa condurre ad una regolamentazione più precisa e sistematica, anche alla luce del fatto che eventuali incertezze

[39] Cfr. Artt. 44, 112 e ss. del Testo Unico delle Imposte sui Redditi

normative e fiscali potrebbero frenare sensibilmente lo sviluppo del mercato in questione.
Nondimeno, sembrano potersi valutare con favore le iniziative dell'Unione Europea volte a fornire un quadro normativo comune in materia. Infatti, l'Unione ad oggi ha formulato due proposte, ovverosia il framework Markets in Crypto-Assets (MiCA) (Commissione Europea, 2020) e il Digital Operational Resilience Act (DORA) (Commissione Europea, 2020). Un comune contesto normativo per gli Stati dell'Unione potrebbe indubbiamente favorire lo sviluppo del settore ed eviterebbe possibili arbitraggi ed inefficienze. […] (Agenda Digitale, 2022)

5.8.3. Definizione elementi essenziali smart contract valutatori

Il funzionamento del processo vede quale primo smart contract quello in cui "in base ai pesi condivisi con tutti gli impianti e i valori di ciascun impianto presi in ingresso, tradurrà quei valori in ammontare di Security Token (in questo caso, rappresentativi del debito dell'impiantista)."
Pertanto, il soggetto che intenderà realizzare l'impianto dovrà, al fine di tokenizzarlo, far riferimento a dati certi e quanto più attendibili circa i parametri energetici di funzionamento, soprattutto, perché questi ultimi verranno tradotti in un "ammontare di debito potenziale" che viene stimato in quantità di security token a valore fisso.
Per ridurre il rischio di incorrere in qualificazioni energetiche dell'impianto falsate, occorrerà richiedere (onere di chi realizza l'impianto) che venga fatta, da un soggetto / ente accreditato, una perizia energetica o, in alternativa, che un organo istituzionale, in possesso dei dati di interesse, li comunichi a chi vuole realizzare l'impianto al fine di rapportare gli stessi a dei precisi criteri valutativi e determinare, così, la total supply dell'impianto stesso.

5.8.4. Stablecoin – Nuove valutazioni della Banca Centrale Europea

L'Unione europea intende procedere rapidamente, ma con coscienza, verso la regolamentazione dei servizi basati su crypto asset, compresi i gettoni digitali il cui valore è ancorato a monete "ufficiali": le stablecoin. L'UE si prepara a farlo delineando vincoli piuttosto stringenti. Il 24 novembre 2021 i ministri delle Finanze europei riuniti nel Consiglio Ue hanno raggiunto l'accordo sulle due sopra citate proposte di regolamentazione che costituiranno la base di un negoziato con il Parlamento europeo. (Battaglia, 2021)

L'obiettivo è duplice: "creare un ambiente stimolante per le imprese e per l'innovazione", ma anche "mitigare i rischi per gli investitori e i consumatori"[40].

"Il mercato delle crypto-asset è di dimensioni modeste e non rappresenta ancora una minaccia alla stabilità finanziaria", si legge nelle note introduttive della proposta, "è tuttavia possibile che un sottoinsieme di crypto-asset", le stablecoin, "possa essere ampiamente adottato dai consumatori al dettaglio". E se questo passaggio avvenisse, afferma il Consiglio Ue, "potrebbe sollevare ulteriori sfide alla stabilità finanziaria, al buon funzionamento dei sistemi di pagamento, alla trasmissione della politica monetaria o alla sovranità monetaria".

Stablecoin – Restrizioni in vista

Al fine di perseguire il corretto funzionamento del progetto occorre tenere presenti le restrizioni proposte in tema stablecoin.

Difatti, Il Consiglio dell'Unione Europea teme che le stablecoin possano diventare una riserva di valore concorrente ai depositi bancari: questo

[40] Cfr. Dichiarazione del ministro delle Finanze sloveno, Andrej Šircelj

ridurrebbe le risorse disponibili per le attività di credito con impatti negativi sull'economia. Per disincentivare questa migrazione da deposito bancario a gettoni virtuali l'articolo 36 (MiCA) stabilisce che gli emittenti di token “non possono offrire interessi” a chi decide di detenere questi asset. Vale la stessa cosa per eventuali remunerazioni assimilabili alla corresponsione di interessi.

Inoltre, una delle più importanti restrizioni riguarda il limite massimo sull'utilizzo giornaliero delle varie stablecoin “come mezzo di scambio”. Per ciascun token il numero di transazioni giornaliere medie (nel trimestre) non deve superare il milione di unità e i 200 milioni di euro in valore, all'interno di una singola area valutaria (ad esempio, l'Eurozona). Se il tetto viene sforato, l'emittente deve “cessare l'emissione del token” e “presentare un piano entro 40 giorni” alle “autorità competenti” per assicurare il rientro nei limiti fissati dall’art. 19b.

Nella soluzione finale proposta dal Consiglio “I token basati su asset possono anche rappresentare una minaccia alla sovranità monetaria e alla politica monetaria”, si afferma senza mezzi termini nelle premesse della nuova proposta di legislazione. Se il rischio si concretizza, "le banche centrali dovrebbero essere in grado di chiedere all'autorità competente di ritirare l'autorizzazione ad emettere token, nel caso di minacce gravi”. Questo proposito trova realizzazione nell'articolo 20: le “autorità competenti” possono ritirare l'autorizzazione agli emittenti di stablecoin qualora “l'attività ponga una seria minaccia alla stabilità finanziaria, alle regolari operazioni del sistema dei pagamenti o all'integrità del mercato”. (Battaglia, 2021)

Conclusioni

Attraverso il caso specifico di startup trattato nel capitolo precedente si è voluto dimostrare come la Blockchain è in grado di creare nuovi paradigmi economici e nuovi modelli di business, mettendo in relazione aspetti tecnologici, economici, finanziari e giuridici apparentemente scollegati tra loro.

Come è stato dimostrato, l'elemento chiave di un modello di business di una applicazione decentralizzata è l'utilizzo di smart contract che gestiscono le interazioni tra i vari stakeholder distribuendo valore all'interno del network.

In conclusione si può affermare che le tecnologie DLT, e in particolare Blockchain, hanno il potenziale per rivoluzionare ogni contesto di business e in particolare il settore finanziario.

Tuttavia, l'applicazione della Blockchain è molto frenata dal peso delle incertezze a livello normativo.

Ma nonostante ciò è estremamente rilevante la costante adozione di questa tecnologia che, di fatto, segue la scia che ha avuto Internet nel tempo.

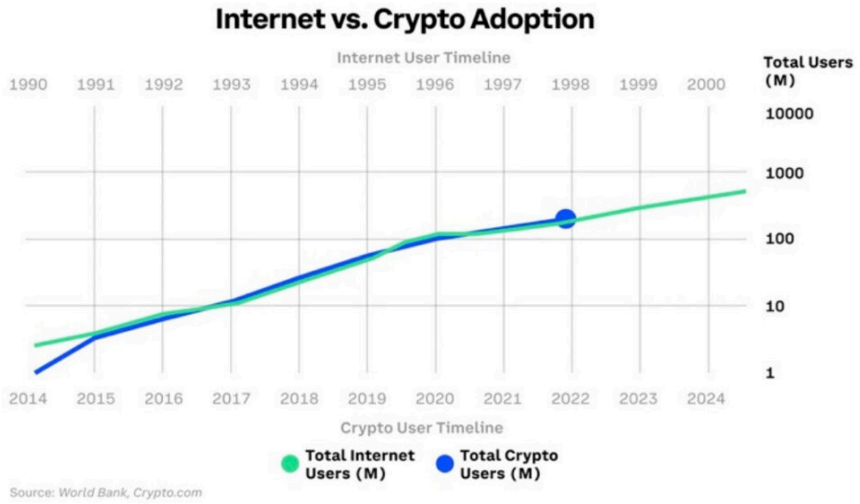

Figura 27: Trend di adozione delle crypto confrontato all'adozione di Internet. [fonte: World Bank, Crypto.com]

Indice delle Figure

Figura 1: Topografia di una infrastruttura centralizzata 9
Figura 2: Topografia di una infrastruttura decentralizzata 10
Figura 3: Topografia di una infrastruttura di rete distribuita 10
Figura 4: Rappresentazione di una catena di blocchi, sulla sinistra il Blocco di Genesi. 13
Figura 5: Screenshot rappresentante il tweet di Hal Finney riguardante l'esecuzione del software Bitcoin per la prima volta. 20
Figura 6: Rappresentazione della struttura dei blocchi caratterizzanti il protocollo Bitcoin 23
Figura 7: Esempio concreto di struttura e contenuto di un blocco tramite Bash 24
Figura 8: Rappresentazione analitica di una transazione casuale su Bitcoin Explorer. 25
Figura 9: Rappresentazione grafica della Total Supply di Ether [Fonte etherscan.io] 34
Figura 10: Prezzo medio del Gas al 10 Gennaio 2022, [fonte etherscan.io] 36
Figura 11: Rappresentazione grafica della quantità totale di Ether emesse a Gennaio 2022, [fonte etherscan.io] 41
Figura 12: Rappresentazione esemplificata di una infrastruttura decentralizzata. [fonte: Bitpanda.com] 47
Figura 13: Rappresentazione esemplificata di una applicazione centralizzata tradizionale. [fonte: Bitpanda.com] 48
Figura 14: Andamento del prezzo di un token in funzione della quantità emessa. 59
Figura 15: Fondi raccolti tramite ICO nel 2017. [Fonte: Forbes] 60

Figura 16: Rappresentazione grafica degli step di attuazione di una STO. 65
Figura 17: Rappresentazione geografica delle regolamentazioni globali sulle criptovalute. [Fonte: Comply Advantage] 88
Figura 18: Quota dei consumi finali lordi di energia coperta da FER (Overall target fissato dalla direttiva europea 2009/28/CE). [fonte: GSE] 94
Figura 19: Rappresentazione ad alto livello del funzionamento dell'applicativo. [fonte: elaborazione personale] 97
Figura 20: Rappresentazione di dettaglio della soluzione tecnologica. [fonte: elaborazione personale] 102
Figura 21: Matrice dei Competitor. [fonte: elaborazione personale] ... 114
Figura 22: Analisi di dettaglio dei tre competitor principali. [fonte: elaborazione personale] 114
Figura 23: Rappresentazione grafica della dimensione del mercato attraverso l'analisi TAM, SAM, SOM. [fonte: elaborazione personale] 118
Figura 24: GANTT di alto livello elaborato con Excel. [fonte: elaborazione personale] 119
Figura 25: Elaborazione delle Revenue tramite Excel. [fonte: elaborazione personale]..... 124
Figura 26: Elaborazione dell’aspettativa di crescita della Startup tramite Excel. [fonte: elaborazione personale] 125
Figura 27: Trend di adozione delle crypto confrontato all'adozione di Internet. [fonte: World Bank, Crypto.com] 132

Indice delle Tabelle

Tabella 1: Scala delle unità di conversione del valore della criptovaluta Ether..... 37
Tabella 2: Confronto tra ICO, IEO e STO..... 65
Tabella 3: Classificazione dei token prevista dalla normativa MiCAR . 74

Bibliografia

Agenda Digitale. (2022, Gennaio 31). *Criptoasset: come criptovalute, token e NFT vengono classificati dal fisco italiano*. Tratto il giorno Febbraio 12, 2022 da Agenda Digitale: https://www.agendadigitale.eu/mercati-digitali/criptoasset-come-criptovalute-token-e-nft-vengono-classificati-dal-fisco-italiano/

Alessi, A. (s.d.). Tratto il giorno Gennaio 14, 2022 da https://www.andreaalessi.it/dizionario/

Andriotto, M. (2019, Aprile 2). *Cos'è e come funziona una STO? intervista a Mauro Andriotto*. Tratto il giorno Gennaio 24, 2022 da Fintastico: https://www.fintastico.com/blog/cosa-e-come-funziona-una-security-token-offering/

Banca D'Italia. (2019, Marzo). Aspetti economici e regolamentari delle «cripto-attività». *Questioni di Economia e Finanza*.

Battaglia, A. (2021, Novembre 26). *Stablecoin, l'Ue prepara la stretta normativa: cosa prevede*. Tratto il giorno Febbraio 13, 2022 da We Wealth: https://www.we-wealth.com/news/fintech/criptovalute/stablecoin-lue-prepara-la-stretta-normativa-cosa-prevede#:~:text=Se%20il%20tetto%20viene%20sforato,19b).

Binance Academy. (2018, Dicembre 6). Tratto il giorno Gennaio 19, 2022 da Binance Academy: https://academy.binance.com/it/articles/proof-of-stake-explained

Binance Academy. (2020, Marzo 18). Tratto il giorno Gennaio 17, 2022 da Binance Academy: https://academy.binance.com/it/articles/what-is-ethereum

Bit2Me. (s.d.). Tratto il giorno Gennaio 5, 2022 da Bit2Me: https://academy.bit2me.com/it/cos%27è-il-blocco-della-genesi/

Bit2Me. (s.d.). Tratto il giorno Gennaio 16, 2022 da Bit2Me: https://academy.bit2me.com/it/Blockchain-Explorer-Explorer-blocca-completamente/

BloombergNEF. (2022, Gennaio). Tratto il giorno Gennaio 28, 2022 da Bloomberg: https://assets.bbhub.io/professional/sites/24/Energy-Transition-Investment-Trends-Exec-Summary-2022.pdf

Borsa Italiana. (s.d.). Tratto il giorno Febbraio 14, 2022 da GLOSSARIO FINANZIARIO - CORPORATE BOND: https://www.borsaitaliana.it/borsa/glossario/corporate-bond.html

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform.* White Paper (Open Source).

Casaburi, L. (2022, Gennaio 5). Tratto il giorno Gennaio 15, 2022 da RicercAttiva: https://www.ricercattiva.it/vita-da-programmatore/blockchain-la-struttura-dati-alla-base-delle-criptovalute/#:~:text=Il%20timestamp%20è%20un%20piccolo,quindi%20ne%20parliamo%20più%20avanti.

Cavicchioli, M. (2020, Maggio 5). *Cos'è e cosa significa halving di bitcoin*. Tratto il giorno Gennaio 12, 2022 da The Cryptonomist: https://cryptonomist.ch/2020/05/05/cose-cosa-significa-halving-di-bitcoin/

Comandini, G. (2021, Novembre 20). Tratto il giorno Febbraio 12, 2022 da TradingTop: https://www.tradingtop.it/criptovalute/comprare-polygon/

Commissione Europea. (2019, Dicembre 11). *COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI.* Tratto il giorno Gennaio 29, 2022 da Il Green Deal europeo: https://eur-lex.europa.eu/resource.html?uri=cellar:b828d165-1c22-11ea-8c1f-01aa75ed71a1.0006.02/DOC_1&format=PDF

Commissione Europea. (2020, Settembre 24). Tratto il giorno Febbraio 4, 2022 da REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937: https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0008.02/DOC_1&format=PDF

Commissione Europea. (2020, Gennaio 14). *COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI.* Tratto il giorno Febbraio 2, 2022 da Piano di investimenti per un'Europa sostenibile Piano di investimenti del Green Deal europeo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0021&from=EN

Commissione Europea. (2020, Settembre 24). *REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014.* Tratto il giorno Febbraio 4, 2022 da REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

Comply Advantage. (2020, Febbraio 6). *Cryptocurrency Regulations Around The World*. Tratto il giorno Febbraio 14, 2022 da Comply Advantage: https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

Council of the European Union. (2021, Novembre 19). Market in Crypto-Asset Regulation. Bruxelles.

Curzi, F. (2021, Gennaio 28). *IL funzionamento della Blockchain e il Quantum Collision Attack.* Tratto il giorno Gennaio 4, 2022 da Red Hot Cyber: https://www.redhotcyber.com/post/blockchain-e-quantum

Decreto del Presidente della Repubblica. (1986, Dicembre 22). Testo unico delle imposte sui redditi (TUIR). *Art. 67, 917(Comma 1, lettera c)*. Roma, Italia.

Dwyer, G. P. (2014). *The Economics of Private Digital Currency.*

Ethereum. (2021, Dicembre 22). *Meccanismi di Consenso*. Tratto il giorno Gennaio 18, 2022 da Ethereum: https://ethereum.org/it/developers/docs/consensus-mechanisms/

Ethereum. (2022, Gennaio 13). *PROOF-OF-STAKE (POS)*. Tratto il giorno Gennaio 19, 2022 da Ethereum: https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/

European Commission. (s.d.). *EU taxonomy for sustainable activities*. Tratto il giorno Gennaio 17, 2022 da https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/eu-taxonomy-sustainable-activities_en

Finma. (2017, 04). Trattamento secondo il diritto in materia di vigilanza delle initial coin offering.

FINMA. (2018, Febbraio 16). *La FINMA pubblica una guida pratica sulle ICO*. Tratto il giorno Gennaio 30, 2022 da FINMA: https://www.finma.ch/it/news/2018/02/20180216-mm-ico-wegleitung/

Gazzetta Ufficiale della Repubblica Italiana. (1990, Giugno 30). Decreto-legge del 28/06/1990 n. 167. *Rilevazione ai fini fiscali di taluni*

trasferimenti da e per l'estero di denaro, titoli e valori., Articolo 4, Comma 1. Roma.

Gazzetta Ufficiale della Repubblica Italiana. (2019, Febbraio 12). *(36), 160*, 13. (R. Italiana, A cura di) Roma, Italia.

Gazzetta Ufficiale della Repubblica Italiana. (2019, Ottobre 4). Decreto Legislativo n. 231. *Decreto Legislativo n. 125(Art. 1, Comma 2, lett. qq)*. Roma.

Gazzetta Ufficiale della Repubblica Italiana. (2019, Ottobre 4). Decreto Legislativo n. 231. *Decreto Legislativo n. 125(Art. 1, Comma 2, lett. ff)*. Roma.

Gazzetta Ufficiale della Repubblica Italiana. (2019, Ottobre 4). Decreto Legislativo n. 231. *Decreto Legislativo n. 125(Art. 1, Comma 2, lett. ff bis)*. Roma.

Gazzetta Ufficiale della Repubblica Italiana. (2019, Ottobre 4). Decreto Legislativo n. 231. *Decreto Legislativo n. 125(Art. 1, Comma 2, lett. i-bis)*. Roma.

Gemini. (2021, Giugno 21). *What Are Security Tokens?* Tratto il giorno Febbraio 5, 2022 da Cryptopedia: https://www.gemini.com/cryptopedia/security-token-offering-vs-initial-coin-offering-stos

Gestore Servizi Energetici. (2021, Luglio). Tratto il giorno Febbraio 13, 2022 da GSE: https://www.gse.it/documenti_site/Documenti%20GSE/Rapporti%20statistici/Rapporto%20statistico%20di%20monitoraggio%20di%20cui%20al%20DM%2011-5-15%20art%207_anni%202012-2019.pdf

KamilTaylan.blog. (2021, Maggio 3). Tratto il giorno Gennaio 13, 2022 da https://it.kamiltaylan.blog/block-bitcoin-block/

Kelly, G. (2021, Maggio 5). Tratto il giorno Gennaio 17, 2022 da https://www.fe.training/free-resources/portfolio-

management/average-maturity/#:~:text=The%20maturity%20of%20most%20corporate,issued%20100%2Dyear%20bonds%20too.

Mione, M. (2017, Dicembre 15). *STORIA DEL BITCOIN, DELLA BLOCKCHAIN E DELLE ALTRE CRYPTOCURRENCIES*. Tratto il giorno Gennaio 10, 2022 da Funds People: https://fundspeople.com/it/storia-del-bitcoin-della-blockchain-e-delle-altre-cryptocurrencies/

Mou, V. (2020, Gennaio 22). *Gli Oracoli Blockchain Spiegati*. Tratto il giorno Gennaio 22, 2022 da Binance Academy: https://academy.binance.com/it/articles/blockchain-oracles-explained

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Osservatori.net Digital Innovation. (2020, Febbraio 5). Tratto il giorno Gennaio 22, 2022 da Osservatori.net Digital Innovation: https://blog.osservatori.net/it_it/token-blockchain-come-funzionano

Osservatorio Politecnico di Milano. (s.d.). *La Blockchain spiegata semplice*. Tratto il giorno Gennaio 2, 2022 da Definizioni, funzionamento, applicazioni e potenzialità: https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni

SNAM. (2021, Dicembre 15). *EVOLUZIONE PREVEDIBILE DELLA GESTIONE*. Tratto il giorno Gennaio 20, 2022 da https://www.snam.it/it/investor-relations/la-strategia/evoluzione-prevedibile-della-gestione/index.html

Starting Finance. (2022, Gennaio). Tratto il giorno Febbraio 15, 2022 da LinkedIn: https://www.linkedin.com/posts/starting-finance_emissions-activity-6898542247345016832-jOGI

Treccani. (s.d.). Tratto il giorno Gennaio 6, 2022 da Treccani: https://www.treccani.it/enciclopedia/fiat-money/

Vella, G. (2019, Gennaio 30). *Distributed Ledger Technology: definizione e caratteristiche*. Tratto il giorno Gennaio 2, 2022 da https://blog.osservatori.net/it_it/distributed-ledger-technology-significato

Vitalik Buterin, F. V. (2015, Novembre 19). *Ethereum Improvement Proposals*. Tratto il giorno Gennaio 29, 2022 da EIP-20: Token Standard: https://eips.ethereum.org/EIPS/eip-20

Wallace, B. (2011). *The Rise and Fall of Bitcoin.* Wired Magazine.

Wikipedia. (s.d.). *Peer-to-peer*. Tratto il giorno Gennaio 3, 2022 da Wikipedia: https://it.wikipedia.org/wiki/Peer-to-peer

William Entriken, D. S. (2018, Gennaio 24). *Ethereum Improvement Proposals*. Tratto il giorno Gennaio 29, 2022 da EIP-721: Non-Fungible Token Standard: https://eips.ethereum.org/EIPS/eip-721

Witek Radomski, A. C. (2018, Giugno 17). *Ethereum Improvement Proposals*. Tratto il giorno Gennaio 29, 2022 da EIP-1155: Multi Token Standard: https://eips.ethereum.org/EIPS/eip-1155

Ringraziamenti

A conclusione di questo elaborato, è doveroso menzionare le persone, senza le quali questo lavoro di tesi non esisterebbe nemmeno.

Ringrazio il mio relatore Roberto Caldelli, che si è dimostrato sin da subito disponibile ed interessato alle tematiche trattate nell'elaborato.

Ringrazio di cuore la mia compagna, Amarita, per avermi sempre sostenuto lungo il percorso e alla quale purtroppo ho sottratto tantissimo tempo per stare insieme.

Ringrazio i miei genitori, Pina e Crescenzo, e mio fratello Saverio per aver creduto nelle mie scelte lavorative e accademiche.

Ringrazio anche Andrea B., Francesco, Andrea P., Riccardo, Daniele, Anna e Pietro, compagni di un percorso di formazione parallelo che hanno contribuito con le loro idee e le loro intuizioni a dare un tocco di originalità a questo elaborato sviluppando insieme un caso studio sperimentale che spero diventi un'azienda un giorno.

Infine, ma non meno importante, voglio ringraziare me.
Voglio ringraziarmi per aver creduto in me, per aver lavorato duro e per non aver mai mollato.

Questo è solo un altro piccolo traguardo raggiunto.