LUISS

Dipartimento di Economia e Management
Cattedra di Informatica

FINTECH: dall'automazione bancaria alla finanza decentralizzata

Prof. Luigi Laura

RELATORE

Luca Negroni

Matr. 241351

CANDIDATO

Anno accademico: 2021-2022

SOMMARIO

1. Introduzione

La diffusione capillare di personal computer, tablet e smartphone, i cui prezzi si sono ridotti rapidamente nel corso degli anni, ha fatto sì che in ogni casa ci sia un computer ed ogni persona sia dotata di un dispositivo mobile. La digitalizzazione sta caratterizzando le maggiori trasformazioni e innovazioni degli ultimi decenni, coinvolgendo vari settori, tra cui quello finanziario.

Una velocissima trasformazione tecnologica sta rivoluzionando il mondo della finanza sia nei pagamenti che negli investimenti. Lo sviluppo delle tecnologie permette di effettuare le operazioni della vita comune in modo semplice ed efficiente. Nella prima parte della tesi parleremo quindi del tema Fintech, vedendo come questo abbia influito sulla vita di tutti noi. Possiamo ad esempio pensare al fatto che al giorno d'oggi è possibile acquistare la spesa, in modo completamente autonomo, se non per le colonnine per i pagamenti, senza aver bisogno di un cassiere a cui pagare o, addirittura, chiederne la consegna direttamente a casa, pagando tramite sito internet.

Saranno trattati gli strumenti finanziari più moderni ed innovativi, approfondendo in particolare il *crowdfunding* e come questo abbia rappresentato un passo verso la disintermediazione.

Dopo aver trattato il tema della finanza centralizzata, nella seconda parte della tesi, si parlerà dei sistemi decentralizzati. Dopo aver spiegato cos'è una *blockchain* ed il suo funzionamento, si parlerà dei Bitcoin (si spiegheranno concetti come il *mining* e la *proof of work*). Si spiegherà la storia di questa cripto valuta, per far capire il motivo per cui alcune persone hanno sentito l'esigenza di sviluppare questi sistemi decentralizzati, che possono essere visti come una reazione a quelli centralizzati.

Si tratterà, nella terza parte, della piattaforma Ethereum: la piattaforma decentralizzata più grande ed utilizzata al mondo. Si parlerà in questo capitolo del funzionamento odierno, ma anche dei suoi sviluppi futuri (si parlerà quindi del passaggio dalla *proof of work* alla *proof of stake*: in cui la seconda, può essere vista come un'evoluzione della prima). Si parlerà di Ether: la maggior criptovaluta di Ethereum, ma anche degli altri utilizzi della piattaforma.

Si vedranno in particolare gli NFT (*Not Fungible Token*), soprattutto da un punto di vista pratico, visto che la parte finale della tesi sarà una guida alla scelta di un portafoglio che permetta di operare in Ether, alla creazione e alla vendita di un NFT.

2. Fintech

Con il termine Fintech si intende l'applicazione della tecnologia ai mercati finanziari, che si traduce in nuovi modelli di business, applicazioni, prodotti o processi, andando così a modificare in modo concreto la fornitura di servizi finanziari.

La tecno finanza può essere applicata a vari ambiti, a partire dai servizi bancari, come i pagamenti o l'intermediazione finanziaria, fino ad arrivare alla valutazione e gestione del rischio finanziario e alle valute digitali. Questo fenomeno è in continua evoluzione, tant'è che in Italia per il biennio 2021-2022, sono previste spese di investimento nel settore per 530 milioni di euro[1]. Per capire quanto il fenomeno sia in crescita, basti pensare che nel biennio 2019-2020 la spesa di investimento nel "Fintec" era stata di 456 milioni di euro.

La digitalizzazione offre molteplici vantaggi, tra questi i più evidenti sono:

- La capacità di offrire in modo sicuro reportistiche immediate: Questa è una caratteristica fondamentale per le aziende, che possono sfruttarla, ad esempio, per avere in tempo reale tutte le informazioni riguardo ai propri clienti, o le informazioni necessarie per rispondergli in brevissimo tempo.
- La semplicità visto che le applicazioni Fintec hanno una *user-experience* evoluta. È tutto quindi estremamente semplice ed intuitivo. E' possibile disporre di una maggiore interazione con gli utenti, basti pensare a un'applicazione che invia, a chi la utilizza, la notifica per ricordargli di pagare una bolletta o un pro-memoria per un appuntamento.
- L'economicità: ci sono tutta una serie di costi di struttura che sarebbero risparmiati, basti pensare ai costi di filiale.
- Il fatto di poter disporre dei dati in tempo reale consente di accelerare i meccanismi decisionali offrendo cruscotti di controllo all'alta direzione, aumentando l'efficacia dei processi e delle attività aziendali.
- Rende possibile la personalizzazione dei servizi finanziari, basti pensare al fatto che, ad esempio, i contratti bancari o assicurativi possano essere facilmente modellati in base alle esigenze dei clienti.
- I pagamenti sono diventati più rapidi, basti pensare alle carte contactless o al fatto che si possano effettuare pagamenti semplicemente utilizzando gli smartphone o gli smartwatch, oltre alla possibilità, tramite applicazioni di home banking, di disporre sul proprio personal computer di un vero e proprio sportello bancario.

[1] dato fornito da indagini conoscitive della Banca d'Italia

- Dà anche la possibilità agli utenti di accedere a servizi che altrimenti gli sarebbero preclusi, basti pensare ai finanziamenti per le start up o ai crowdfunding.
- Si ha una maggiore trasparenza.

Oltre che vantaggi, vanno tuttavia illustrati i rischi: oltre a quelli legati ad ogni singola attività, bisogna considerare il fatto che si tratta di attività che avvengono tramite canali digitali, superando i confini nazionali e risultando perciò più complesse da regolamentare.

Bisogna considerare anche il rischio di attacchi informatici, delle frodi ed il fatto che tali modalità possano agevolare eventuali operazioni illecite. La difficile tracciabilità delle operazioni, che avvengono attraverso sistemi parzialmente regolamentati, è motivo di vulnerabilità. Bisogna prestare particolare attenzione alle valute digitali e al crowdfunding: queste attività, essendo relativamente nuove, non sono facilmente inquadrabili nelle categorie giuridiche già conosciute e quindi sono scarsamente regolate. La storia ci ha insegnato quanto la stabilità del sistema finanziario sia un interesse collettivo estremamente importante. È importante che l'efficienza di tempi e costi che viene portata dalla tecnologia, non vada a gravare sulla sicurezza e sulla trasparenza del settore.

Quando si parla al settore Fintech si pensa soprattutto alle banche, principali investitori, che sostengono il 76,5% della spesa complessiva. Queste, negli anni precedenti alla rivoluzione digitale, avevano innovato molto, ma esclusivamente nei sistemi interni degli istituti di credito o nei sistemi di regolamento a livello di rete interbancaria. Nulla era stato fatto nei confronti della clientela e nel rapporto banca-cliente.

Al giorno d'oggi ci si chiede quale possa essere il rapporto tra le banche tradizionali e i servizi bancari di tipo Fintec: se questi possano andare a completare la banca o a fargli concorrenza.

Le Fintech rappresentano un importante opportunità di innovazione e accelerazione per esse.

Chi vorrà continuare a fare la banca in modo tradizionale probabilmente fallirà, soprattutto se non è di macro-dimensioni; le banche di nuova generazione, saranno specializzate e dovranno dare ai loro clienti la possibilità di poter accedere ai prodotti terzi: avranno perciò dei partner agili che saranno in grado di valutare in modo rapido grazie alle proprie tecnologie e al fatto che le procedure saranno basate sui dati e l'analisi di questi. Quest'idea nasce dal fatto che forse, ad eccezione di banche colossali, sarà impossibile che una banca riesca autonomamente a fornire ai propri clienti il miglior servizio in ogni settore.

La Fintec sta inoltre creando dei competitor alle banche tradizionali: le *neo-bank* o *challenger bank*. Queste sono fruibili esclusivamente tramite dispositivi mobili e hanno come propri prodotti solamente delle carte di debito o di credito. Le filiali, che fino a qualche anno fa venivano viste come punti di forza, ora vengono viste come un costo aggiuntivo.

Il fatto che ci siano molte start-up causa un ingresso continuo di nuovi competitors nel mercato degli intermediari finanziari e questo fa sì che ci sia una sempre maggiore competizione. Questa situazione che si sta creando può anche essere vista come una spinta per le banche a innovarsi e a rivoluzionarsi continuamente: così facendo si crea un beneficio collettivo per tutti coloro che usufruiscono dei mercati finanziari.

2.1. Fintech e metodi di pagamento

Vediamo ora, nel concreto, come la tecnologia ha influenzato e cambiato i metodi di pagamento.

Il mercato dei pagamenti sta vivendo un periodo di grandi innovazioni che stanno portando gli utenti ai pagamenti digitali. Questo è una mega tendenza, il cui mercato è in continua crescita (oltre il 10% annuo) e che con la pandemia ha vissuto una rapida accelerazione.

Il pagamento digitale è il trasferimento di una somma di denaro che avviene per mezzo di strumenti elettronici (ad esempio i *wallet* o le carte di credito) o tramite addebito diretto sul conto corrente. Viene visto come un'opportunità in più per i clienti che, al giorno d'oggi, possono pagare in modo più efficiente e comodo: servendosi di cellulari, ma anche di orologi, fino ad arrivare agli addebiti automatici, che non richiedono alcuna operazione a chi ne usufruisce. Tra le forme di pagamento innovative più diffuse vediamo quelle *contactless*, il *mobile-commerce* e gli *e-commerce*. Ci sono inoltre gli *innovative payment*, di cui fanno parte i POS digitali, che permettono di effettuare pagamenti in modo autonomo, senza passare per la cassa o portafogli digitali (che non devono più essere necessariamente connessi ai circuiti delle carte).

Tramite il *device-free payment* è inoltre possibile effettuare i pagamenti senza alcun dispositivo di attivazione: per far ciò si utilizza la biometria e quindi sblocco facciale, tramite impronta digitale, ecc.

È sempre più frequente il fenomeno dei bonifici istantanei, grazie ai quali più soggetti possono trasferire denaro in tempo reale. Questa tipologia di pagamento è stata diffusa soprattutto da piattaforme come Paypal e Satispay.

Sono inoltre sempre più frequenti le collaborazioni delle big tech con gli attori finanziari, con lo scopo di ideare e sviluppare continuamente nuovi metodi di pagamento: si vede una forte focalizzazione sulla creazione di monete digitali, con una particolare attenzione allo studio delle tecnologie *blockchain*, in cui si ricerca di arrivare alla disintermediazione.

2.2. Fintech e sistema di raccolta dei capitali

Altra area che su è modificata notevolmente è quella della raccolta dei capitali. A tal proposito si sono creati molteplici alternative a quelle classiche. Tra di esse è importante citare servizi più convenzionali tra cui la raccolta di depositi online, lo sviluppo di applicazioni per gestire i conti di pagamento e di applicazioni che hanno anche lo scopo di migliorarne l'educazione finanziaria.

Per quanto riguarda la digitalizzazione nell'ambito del credito, si stanno rimodellando le varie fasi della filiera, a partire dall'*onboarding*, fino ad arrivare alla valutazione del merito creditizio, consentendo una crescente precisione nello stipulare contrati e nel monitorare il credito. In questo modo si riesce infatti sia a ottimizzare i processi di erogazione del credito, ma anche a migliorare il grado di soddisfazione del cliente. Questi vantaggi sono dati dall'efficienza maggiore nelle fasi di acquisizione dei documenti rilevanti, la maggiore rapidità nelle fasi di *onboarding* e all'utilizzo di algoritmi *credit scoring* evoluti. Si riesce perciò a valutare il metodo creditizio in modo automatizzato, sfruttando i *big data*.

Tramite i *supply chain finance* si riesce inoltre a rispondere in modo efficiente e garantendo una forte personalizzazione all'operatività delle imprese. Gli intermediari permettono alle aziende di ottenere il credito anche tramite marketplace (è un sito internet che serve per scambiare beni o servizi tra diversi venditori di diversi siti) in particolare di lending crowdfunding.

2.3. Crowdfunding

Il *crowdfunding* è uno strumento, che si sta sviluppando in modo esponenziale negli anni. Solamente in Italia, dal 2019 al 2020 i fondi erogati, nei primi sei mesi, sono passati da 517 a 908 milioni d euro.

Wikipedia definisce il *crowdfunding* (in italiano finanziamento collettivo) come "un processo collaborativo di un gruppo di persone che utilizza il proprio denaro in comune per sostenere gli sforzi di persone e organizzazioni". È una pratica di micro-finanziamento dal basso che mobilita persone e risorse.

Il web, in questo caso consente di rompere le barriere finanziarie tradizionali, fornendo un luogo in cui gli investitori o i risparmiatori si possano incontrare con coloro che propongono iniziative da finanziare. Invece di ricevere la somma di denaro da un'unica fonte, si riceve da più soggetti differenti. Questi soggetti possono essere persone comuni che credono nel progetto.

Le iniziative finanziate tramite il *crowdfunding* sono soprattutto quelle con scopi innovativi e di cambiamento sociale; possono riferirsi tuttavia a molti altri ambiti: dal sostegno per l'arte, all'imprenditoria, al giornalismo partecipativo ecc.

Noto utilizzatore di questo strumento fu Barack Obama, il quale finanziò la propria campagna elettorale grazie ai finanziamenti derivanti dai propri elettori.

Inizialmente il *crowdfunding* riguardava solamente le start up innovative, mentre al giorno d'oggi i campi di azione sono più ampie.

Esistono diversi tipi di *crowdfunding*

- *Equity crowdfunding*: consiste nel finanziamento di una campagna tramite capitale di rischio. In questo caso quindi gli investitori diventeranno dei soci e avranno diritto a delle quote. In questo caso i progetti sono solitamente medio grandi e le piattaforme devono essere necessariamente iscritte presso il registro della Consob, vista la similitudine con le azioni.
- *Landing crowdfunding*: consiste nel finanziamento di un'iniziativa tramite il capitale di debito. Ciò che avviene è quindi un prestito, solitamente a 12 mesi. In questo caso gli investitori sottoscrivono dei titoli di debito: non diventano soci e il loro guadagno sta negli interessi sul capitale prestato.
- *Donation Based*: chi finanzia il progetto lo fa come donazione, per sostenere una persona o un progetto. In questo caso l'investitore non riceverà nulla in cambio, se non la riconoscenza di chi riceve il denaro.
- *Reward Based*: Il finanziatore non riceve alcun tipo di compensi finanziari, ma avrà delle ricompense a seconda della somma versata. Potrà ad esempio ricevere un prodotto omaggio o uno sconto nel caso di lancio di un prodotto; potrà avere voce in capitolo durante lo sviluppo del progetto, o qualsiasi altra forma di riconoscenza (più o meno simbolica), che viene concordata nel momento del versamento.

Le piattaforme possono essere inoltre divise in:

- *All or nothing*: in questo caso si fissa una scadenza della ricerca dei fondi a massimo 90 giorni e, se la cifra necessaria non viene raggiunta, i contributi verranno restituiti agli investitori. Questa forma di finanziamento è consigliata per i progetti che non possono essere realizzati senza l'intero ammontare.
- *Keep it all*: si stabilisce anche in questo caso un massimo di 90 giorni, ma i contributi vengono accreditati anche nel caso in cui non si sia raggiunta la cifra prestabilita. Questo tipo di procedimento è indicato per i progetti che possono partire anche senza l'intera somma desiderata.
- *Fundrasing*: permette di avere un accredito istantaneo dei fondi, i quali non devono ne aspettare una scadenza, ne devono avere dei requisiti minimi circa l'ammontare. È stata questa la tipologia di raccolta prediletta dalle iniziative politiche.

È quindi evidente la caratteristica principale dello strumento finanziario, il quale oltre che coinvolgere la collettività riesce, grazie alla propria flessibilità, ad adattarsi facilmente alle esigenze di chi usufruisce del servizio.

Le operazioni di *donation* e *reward based crowdfunding*, in particolare, consentono ai progettisti di controllare maggiormente e in modo più libero le proprie iniziative.

Il fatto di rivolgersi alla comunità inoltre permette di ottenere un feedback sul progetto già da prima rispetto alla sua attuazione, infatti, il non riuscire a ottenere i fondi potrebbe essere un buon campanello d'allarme per quanto riguarda la validità del progetto. Inoltre, effettuare una buona campagna di crowdfunding, può aiutare l'imprenditore ad ottenere eventuali ulteriori forme di investimento dagli altri intermediari, presentandosi come maggiormente credibile.

Questa della credibilità è però un'arma a doppio taglio, visto che nel caso in cui la campagna non riscuota il successo desiderato, si rischia di danneggiare la reputazione: soprattutto nelle piattaforme *all or nothing* il non raggiungimento del capitale prefissato, causa l'obbligo alla restituzione degli importi ricevuti; così causando una perdita di tempo da parte sia degli imprenditori che degli investitori.

Bisogna inoltre considerare il fatto che diffondere il proprio progetto sul web consente di raggiungere molti utenti e attirare molti investitori. Anche quest'opportunità nasconde però una minaccia alla proprietà intellettuale dell'idea, che potrebbe essere sottratta da osservatori malevoli.

In Italia il *crowdfunding* è inoltre favorito da detrazioni fiscali che possono arrivare fino al 50% dell'investimento nel caso delle start up innovative.

Altra innovazione nel mondo di raccolta dei capitali è quella degli *Exchange-Traded-Fund (ETF)*. Questi sono dei fondi di investimento a gestione passiva quotati in borsa. Questi sono una sottocategoria degli *Exchange-Traded Products* (*ETP*). Questi fondi sono gestiti da un manager, a cui i soci delegano l'intera gestione. Il manager si occupa della compravendita di azioni, guadagnando dai dividendi o dalle plus valenze di queste. Sono solitamente legati a indici azionari (un esempio potrebbe essere quello dell'SPX 500).

2.4. Fintech e financial security

Il parlamento europeo, già a partire dal maggio 2017, ha individuato 4 aree nelle quali era necessario operare a livello di sicurezza e regolamentazione, queste erano:

- La *cybersecurity* e la protezione dei dati
- Il *level playing field*: ovvero creare situazioni in cui tutti quanti hanno le stesse possibilità di successo. Ad esempio, un obiettivo da questo punto di vista potrebbe essere quello di creare un

ambiente in cui le imprese operano equamente, anche se nei paesi ci sono regole e tassazioni diverse.

- Il controllo della sperimentazione di nuove tecnologie, promuovendo l'educazione finanziaria e delle competenze digitali
- L'interoperabilità dei servizi Fintech all'interno dell'unione europea.

Nel marzo 2018 la Bce ha pubblicato la "Guida alla valutazione delle domande di autorizzazione all'esercizio dell'attività bancaria degli enti creditizi Fintech". Questo è un testo privo di vincoli giuridici, che risulta neutrale al progresso tecnologico. Può essere visto come uno strumento per fornire supporto agli enti che ne hanno bisogno, con lo scopo di assicurare l'efficienza e l'efficacia nelle procedure di valutazione del credito.

Nel Comitato di Basilea, dopo consultazioni, si arrivò alla conclusione che l'innovazione non debba essere ostacolata, ma bisogna essere attenti visto che il Fintec ha portato un incremento dei rischi legati al settore.

Oltre alle normative europee ci sono anche quelle promosse dall*'International Organization of Securities Commissions (IOSCO)*. Questa è la prima organizzazione che, dopo aver studiato ed inquadrato il fenomeno del Fintech, ha pubblicato, nel 2017 una ricerca inerente ad esso. Trattando il tema della tecnologia e come regolamentarla, Anche qui si è cercato di costruire un adeguata regolamentazione, che assicuri standard di sicurezza e correttezza dei servizi, prestando attenzione a non soffocare le innovazioni.

Nel 2020, inoltre, lo *IOSCO* ha deciso di soffermarsi sull'intelligenza artificiale, approfondendo particolarmente il *machine learning*.

Le regole impartite dalle autorità non devono limitarsi alla sola difesa da eventuali abusi o attacchi criminosi. Le leggi devono essere emanate da un punto di vista costruttivo, indirizzando così le imprese verso vie più sicure e sostenibili, per proteggere gli operatori più virtuosi da quelli meno. Il fine deve perciò essere quello di creare un sano e corretto equilibrio, non solo delle imprese, ma di tutti gli stakeholders coinvolti.

Le regole che erano state stabilite in epoca predigitale risultano ora obsolete e quindi si ha il bisogno di riscriverle in chiave digitale. Per far ciò si procede secondo le seguenti tappe:

- Studiare i fenomeni per verificare se ci sia la necessità di intervenire
- Applicare il quadro regolamentare vigente, dove possibile
- Dove non sia possibile applicare il quadro regolamentare vigente, bisogna introdurre nuove leggi col fine di cogliere le specificità dei nuovi fenomeni.

L'approccio utilizzato in questo ambito è detto *wait and see* e consiste nel non introdurre nuove regole fino a quando il nuovo prodotto finanziario non comporti rischi rilevanti per il sistema finanziario, dovuti dal fatto che ne aumenti la diffusione. Nel frattempo, possono però essere emanati avvertimenti e comunicazioni per sensibilizzare e indirizzare il mercato.

Questo approccio ha come vantaggio quello di evitare che le autorità intervengano troppo presto, senza aver avuto il tempo di informarsi in modo adeguato. D'altro canto, nel periodo in cui non si hanno regolamentazioni, si è esposti a maggiori rischi.

Un altro principio è detto *same business, same risks, same rules*, secondo cui se un'attività innovativa ha la stessa funzione di un'attività già regolamentata, verranno applicate le stesse leggi alle due. Questo principio serve per garantire condizioni uniformi agli operatori nuovi e vecchi, con lo scopo di rimanere neutrali.

Nel caso in cui la tecnologia sia in grado di offrire nuovi servizi, si adotta il principio *new functionality, new rules* che serve a regolare prodotti innovativi che portano rischi non sufficientemente presidiati o di cogliere opportunità che vengono limitate dalla regolamentazione esistente.

Questi tre approcci sono utilizzati in modo complementare o in successione, in base al grado di evoluzione del fenomeno innovativo.

La commissione europea, si è fatta, negli ultimi anni, promotrice di varie iniziative inerenti ai cripto-assets. Queste servono sia a introdurre nuovi presidi regolamentari, che ad applicare le norme vigenti ad attività simili a quelle già esistenti. In particolare, la Commissione Europea sta svolgendo due piani di attività:

- La strategia circa la materia di finanza digitale per l'Unione Europea: si parte dal presupposto che il futuro della finanza sia digitale e si cerca di facilitare, tramite norme, la transazione digitale. Tra le proposte principali ci sono quelle dei regolamenti della commissione sui mercati delle attività in cripto e sulla resilienza operativa digitale nel settore finanziario
- La strategia che riguarda i pagamenti al dettaglio: Qui si parte dal presupposto che i pagamenti siano uno dei fattori abilitanti dell'innovazione dei settori finanziari e commerciali e ha come scopo quello di promuovere un'industria dei pagamenti innovativa e efficiente. I quattro pilastri di questa strategia sono: l'adozione di soluzioni di pagamento digitali e istantanee; promozione di mercati innovativi e competitivi dei pagamenti retail, sfruttando a pieno le possibilità della PSD2; Una revisione della PSD2; Definire l'intelligenza artificiale in un quadro europeo.

2.5. Machine Learning

L'intelligenza artificiale si ha quando un computer imita, in qualche modo, il comportamento umano. È una disciplina che risale al 1956 e che nasce con lo scopo di far svolgere ai computer ruoli che richiedono l'intelligenza, è che quindi venivano considerati come univocamente umani.

Il *machine learning* si inizia a diffondere negli anni 80'. È un termine che indica un sottoinsieme dell'intelligenza artificiale che si riferisce alle macchine e ai sistemi che imitano l'intelligenza umana. Viene ideato con il fine di risolvere dei problemi che non potevano essere affrontati tramite le prime forme di intelligenza artificiale. Si capì che i computer non dovessero limitarsi a imitare esclusivamente l'essere umano e i suoi comportamenti, ma anche a simulare il processo di apprendimento delle persone. Noi elaboriamo un gran numero di dati ed impariamo da essi ed è proprio questo il processo che è alla base dell'apprendimento automatico su cui si fonda il machine learning.

Il *machine learning* può quindi essere definito come "quella tecnica che, una volta implementata, consente ad un computer di imparare a effettuare delle operazioni, senza che ci sia bisogno di programmare un software specifico che le effettui". Facciamo un esempio con il riconoscimento delle immagini: I computer a tal proposito, dopo aver immagazzinato un gran numero di foto, sono in grado di riconoscere degli elementi all'interno di esse, anche se non gli viene specificato. Ad esempio, gli elaboratori riescono a distinguere all'interno delle immagini gli elementi differenti (lampioni, persone, alberi, ecc.). Negli smartphone è addirittura possibile effettuare delle ricerche di immagini in galleria tramite una funzione che, dopo aver analizzato i tratti distintivi di varie persone, le riesce a distinguere, raggruppandole in modo autonomo.

Un computer, quando elabora delle immagini non ne vede, a differenza nostra, il contenuto ma rileva delle informazioni binarie. Le tecniche più adottate per "allenare" i dispositivi a fare ciò sono:

- Il *supervised learning*: In questo caso vengono forniti al computer sia degli input, che degli output che ci si aspettano in base agli input. Si realizza così una lista di regole che possono poi essere applicate ai singoli casi in futuro. Questi processi di apprendimento si ripetono fino a quando la percentuale di errore non risulti estremamente bassa.
- *Unsupervised learning*: In questo caso al computer vengono dati una serie di input, senza dire l'output che ci si aspetta. Sarà quindi il computer ad analizzare i vari dati e a capire quali saranno le tipologie di output da dare; Questo è utilizzato per l'esempio di divisione delle foto nelle gallerie fatte in precedenza.
- Semi *supervised learning*: In questo caso viene fornita solamente una parte degli output rispetto agli input, mentre per gli altri non si dà alcuna informazione.

- Il *reinforcement learning* è un approccio che si può d tradurre come “rinforzo positivo”, che consiste nel dare “dei premi o delle punizioni” nel caso in cui sia svolgendo bene, oppure male, una determinata funzione. Ad esempio, se si sta sperimentando la guida autonoma, ci sarà un software che fornisce continuamente dei feedback alla vettura in base alle decisioni che prende inerenti a eventuali stop, precedenze ecc. Così facendo il computer imparerà a prendere sempre la scelta giusta.

Il *machine learning* ha inoltre aumentato la propria importanza, incrementando il proprio interesse, grazie a fattori come l’aumento della quantità e della varietà dei dati, oltre che al fatto che i processi di archiviazione, come gli spazi di archiviazione, sono sempre più economici.

Tutto ciò ha reso possibile realizzare modelli di analisi di dati sempre più grandi e complessi; permettendo così elaborare in modo sempre più efficiente risultati sempre più accurati. Ciò consente alle aziende di identificare più opzioni, riuscendo così a evitare rischi non preventivati e di riuscire a comparare un numero sempre più elevato di opportunità di profitto.

3. DEFI e Criptovalute

Tradizionalmente i processi di transazione sono supportati da operatori centrali, che registrano i dati all'interno di un libro mastro, e hanno una visione coerente sui diritti di proprietà dei diversi utenti coinvolti. I dati sono perciò gestiti da degli intermediari, che rappresentano l'ente centrale e che devono avere un'ottima reputazione. L'ente esercita un controllo diretto, che espone però gli utenti a un grande rischio: l'intermediario rappresenta un punto unico di fallimento e quindi è esposto alla perdita delle informazioni che conserva.

Una novità è inoltre rappresentata dalla DeFi, ovvero la *finanza decentralizzata*. È un mercato dalle grandi potenzialità, che è in continua espansione; basti pensare che agli inizi del 2020, il totale delle risorse depositate nei protocolli DeFi erano pari a un miliardo di euro, mentre oggi quegli assets hanno un valore che supera i 230 miliardi di dollari[2]. Altrettanto esponenziale è stata la crescita degli utenti della DeFi: sono passati da meno di 100000 a circa 4,5 milioni, nello stesso arco temporale[3].

Questo fenomeno consente di effettuare delle transazioni senza aver bisogno di intermediari finanziari. Ciò è possibile grazie all'utilizzo della blockchain, ovvero un database condiviso ed immutabile, a ritroso, in cui gli utenti stessi possono tener traccia delle transazioni, senza che ci sia bisogno di un'entità centrale che le controlli. Gli strumenti finanziari in questo caso sono gestiti da protocolli informatici pubblici: gli *smart contract* che si basano sulle *blockchain*.

Gli *smart contract* sono dei programmi, eseguiti in codice, che vengono eseguiti in automatico dai software della rete e che quindi in teoria non sono controllate e controllabili da nessuno.

In realtà, all'interno di questi protocolli possono essere inseriti degli input esterni che possono essere quindi controllate da persone e perciò possono rendere la catena centralizzata. Gli *smart contract* fatti meglio sono perciò o quelli che non possono ricevere input esterni o che si servono di oracoli decentralizzati e quindi strumenti che servono a inviare uno *smart contract* dei dati provenienti dall'esterno. Gli strumenti Defi non sempre sono fatti bene, ma quando questi lo sono, risulta impossibile

I vantaggi della DeFi rispetto alla finanza tradizionale sono molti, tra cui spiccano:

- l'anonimato;
- numero ridotto di barriere all'ingresso;
- costi di transazione ridotti;
- molte applicazioni tra cui poter scegliere;
- maggiore rapidità nell'eseguire i contratti;

[2] fonte: DdefiLlama
[3] fonte: Dune analytics

- minor rischio di perdita dei dati.

La finanza decentralizzata, proprio come la finanza tradizionale, è stata l'evoluzione della moneta: prima si sono sviluppate le cripto valute, e poi i sistemi di pagamento e di conseguenza tutti i servizi finanziari correlati.

Le prime applicazioni dei sistemi decentralizzati consistevano nel poter prestare le *stablecoin* in cambio di interessi e di titoli a garanzia. Col tempo sono state scambiate nei sistemi decentralizzati, tante altre valute. Queste operazioni finanziarie vedono al loro centro i "tokens", che sono un insieme di informazioni che definiscono il proprietario di un bene, all'interno della *blockchain*.

Le operazioni nei sistemi finanziari hanno dato vita a operazioni via via più complesse: si può fare trading di *crypto*, stipulare contratti assicurativi, di asset management, derivati ecc.

Esistono inoltre molti modi per mettere a reddito in modo passivo i propri *tokens*, tra cui quelli di cederli per un arco di tempo a delle piattaforme che hanno lo scopo di *minare liquidità* e sono dette "*liquidity mining*". Così facendo chi *presta i token*, si ritrova in cambio un con un surplus di liquidità. Queste piattaforme guadagnano prestando a loro volta i token ad altri utenti o consentendo agli altri di scambiarsi coppie di cripto-assets a un tasso di cambio che è determinato da dei *market-makers automatici*.

3.1. Blockchain

Considerate le varie innovazioni emerse nel settore della Fintech, probabilmente tra le più popolari risalta la *blockchain*. Questa risale al 1991 e fu ideata da due ricercatori americani. Nasce con lo scopo di vidimare i documenti digitali per far sì che questi non potessero essere retrodatati o modificati. Questa tecnologia rimase inutilizzata fino al 2008, ovvero quando Satoshi Nakamoto ideò il Bitcoin.

La blockchain ha attirato molto l'attenzione della stampa e degli analisti grazie al proprio potenziale. Può essere applicata a vari ambiti, che spaziano dalla programmazione alla registrazione di voti. La prima applicazione di questa tecnologia risale alle cripto-valute: queste hanno poi dato vita a una serie di nuove tecnologie, attività, lavori, per non parlare della rivoluzione nell'ambito dei sistemi di pagamento inerenti ad esse.

C'è chi dice che queste detengano il potenziale per rivoluzionare il sistema finanziario; prima di valutare quest'affermazione è però necessario capire che tecnologia c'è dietro queste risorse.

Gli elementi principali di un sistema blockchain sono:

- Nodi di rete, ovvero coloro che partecipano e interagiscono con la rete

- La crittografia delle transazioni e gli strumenti che certificano gli scambi. Ogni nuova voce dati è detta *hashing*: L'*hash*, dopo aver acquisito dei dati, calcola un'impronta digitale che non può essere modificata. L'output dell'*hash* è invece il *digest*.
- La fiducia tra i nodi
- I nodi possono svolgere due ruoli all'interno della rete *blockchain*:
    - *Wallet node* e quindi gestire un insieme di indirizzi che identificano il nodo all'interno della rete
    - *Miner node* e quindi si occupa delle esecuzioni e delle verifiche e conferme delle transazioni effettuate dagli utenti. Con il termine *miner*, si indica quindi, in questo caso, la partecipazione alla stesura del registro. Ad esempio, nel caso dei Bitcoin, è come se i *miner* li estraessero grazie a dei calcoli; come fa un *miner* di oro attraverso il lavoro di estrazione mineraria.

La *blockchain* potrebbe essere vista come un archivio decentralizzato e digitale condiviso che può essere consultato da chiunque faccia parte della rete. Letteralmente per blockchain si intende una catena di blocchi contenenti informazioni. Ognuno di questi blocchi contiene 3 tipi di informazioni:

- I dati che vengono memorizzati in quel blocco (ad esempio il mittente, il destinatario e la quantità di Bitcoin che viene scambiata).
- L'*hash*, ovvero una stringa di numeri e lettere che serve per identificare sia il blocco, che il suo contenuto. Questa è sempre unica ed infatti ogni blocco ha un *hash* che è unico e specifico per quel blocco. Nel caso in cui un dato all'interno del blocco dovesse cambiare, anche l'hash cambierebbe.
- L'*hash* del blocco precedente ed è questo a rendere il sistema blockchain così sicuro. Ad esempio, nel caso in cui ci fosse una catena di tre blocchi, ogni blocco conterrebbe il suo hash e quello precedente. In questo caso il terzo blocco conterrebbe anche l'hash del secondo ed il secondo quello del primo. Il primo invece è detto *genesis block* e non contiene altri hash a parte il proprio. Se per esempio qualcuno dovesse manomettere il secondo blocco, allora l'hash di quel blocco sarebbe immediatamente modificato e di conseguenza il blocco tre non sarebbe più valido visto che non conterrebbe più l'hash valido del blocco precedente: così facendo quindi si invaliderebbero anche tutti i blocchi successivi.
- Al giorno d'oggi, data la rapidità degli elaboratori, si potrebbe manomettere un blocco e ricalcolare velocemente tutti gli hash successivi, col fine di rendere valida la blockchain, per questo motivo la blockchain ha bisogno anche di un protocollo criptografico chiamato *proof of work* (PoW). Questa è una richiesta di calcoli aggiuntivi necessari per realizzare la creazione di nuovi blocchi e rendere molto più complesse le operazioni di attacchi da parte degli hacker. Oltre

che il calcolo degli hash, infatti, si dovrebbe ricalcolare la *proof of work* per ognuno di essi e per far ciò si impiegherebbe troppo tempo.

Altra caratteristica che contribuisce alla sicurezza della tecnologia è la decentralizzazione. Le blockchain utilizzano una rete *p2p* (per *p2p* si intende *peer to peer* e quindi da pari a pari: è una rete costituita da computer tutti uguali tra di loro in cui non c'è un centro di controllo) a cui può accedere chiunque. Chi si unisce alla *blockchain* diventa un nodo e subisce una copia di essa. Quando nella blockchain viene creato un nuovo blocco, questo arriva a tutti i nodi della rete. Ogni nodo, quindi, analizza il nuovo blocco e, solo se risulta uguale a quello aggiunto agli altri blocchi, viene aggiunto alla catena. Nel caso in cui una catena aggiunga un blocco manomesso, questo verrebbe respinto dagli altri. Quindi in questo caso per compromettere la rete, bisognerebbe manomettere il 50% più uno dei nodi di essa.

Tutte queste precauzioni fanno sì che attaccare la catena risulti poco conveniente, sia per motivi di tempo, che per motivi energetici.

La *blockchain* è stata sviluppata per la prima volta con i Bitcoin, ed è anche alla base di molti altri assets che sfruttano tale struttura tramite processi di replica e variazione. È infatti vero che molte cripto valute sono cloni di Bitcoin, o presentano solamente parametri differenti (come potrebbero essere i tempi di blocco e l'offerta di valuta).

Le applicazioni della *blockchain* vanno oltre quelli del mondo cripto e infatti ora li andremo a citare:

- tracciare gli alimenti in modo rapido da parte delle catene della grande distribuzione. Serve ad esempio a tener traccia dei percorsi che il cibo effettua prima di essere venduto nei supermercati. In Italia, già a partire dal 2015, è stata sviluppata un'applicazione, detta "Foodchain", che tracciava i percorsi effettuati dagli alimenti a partire dalle origini, fino ad arrivare al consumo finale.
- Seguire i percorsi delle merci in giro per il mondo e, in particolare, questa tecnologia viene utilizzata per il tracciamento dei container. Il punto di forza di tale tecnologia è quello che permette a vari utenti di interagire tra di loro.
- Validare le certificazioni, che con queste tecnologie diventerebbero impossibili da falsificare.
- Proteggere l'identità online, senza bisogno che ci sia una terza parte (come, ad esempio, lo stato) che oltre a fornire il servizio potrebbero esercitare potere discrezionale sulle regole alla base del sistema.
- Irrobustire la contabilità, dato il fatto che offre la possibilità di archiviare le informazioni in modo trasparente, ma con la possibilità di criptarle e renderle accessibili sono a chi ha le chiavi private. Inoltre, queste rimarrebbero immutate per sempre.

- Potrebbe inoltre essere vista come modo per aiutare nel lavoro i notai, in particolare aiutandoli in compiti come quelli di gestione delle imposte sulla casa, delle bollette, spese dell'immobile ecc.
- Nel gaming: in questo caso vengono utilizzate nell'ambito delle *skin* e perciò le caratteristiche come il colore dei giocatori, i gadget, eventuali armi speciali ecc. Questi oggetti possono essere registrati nella blockchain e la loro proprietà può essere gestita tramite transazioni tra gli utenti, creando così un vero e proprio mercato di scambio.
- In Estonia, addirittura, il certificato di matrimonio, non necessita del notaio, ma viene salvato tramite la *blockchain*.

La blockchain presenta, tuttavia, dei limiti. Tutto ciò che è all'interno del sistema ha una sicurezza garantita dalla crittografia, la tracciabilità delle informazioni, l'inalterabilità e l'immutabilità del registro. Per quanto riguarda, invece, il momento in cui le informazioni vengono inserite all'interno della catena, può accadere che il voler inserire determinati argomenti all'interno della blockchain possa risultare pericoloso. Nel caso di voto elettronico, ad esempio si tenderebbe a sottovalutare il mezzo con cui avviene la votazione. Non si ha la sicurezza che il voto entri all'interno della *blockchain*, esattamente per come è stato espresso. Inoltre, non è neanche così garantito che il voto risulti effettivamente anonimo. Ad esempio, nel caso in cui il voto avvenga tramite computer, questo potrebbe essere compromesso, proprio come potrebbe essere compromessa la rete.

Per quanto riguarda il tracciamento alimentare, il problema è nel fatto che non si ha la garanzia che i dati immessi siano corretti: soprattutto nel caso in cui a fornirli siano i produttori stessi, in cui è evidente il conflitto di interessi.

In conclusione, quindi possiamo affermare che il problema della catena è tutto ciò che è intorno ad essa.

Si hanno inoltre dei problemi a livello di regolamentazione ed in particolare non riescono a rispettare la protezione dei dati personali e in particolare si hanno difficoltà con il diritto all'oblio (siccome la *blockchain* si basa sul fatto che i dati siano perpetui), con il principio di necessità (secondo il quale può accedere ai dati solo chi è legittimamente interessato) e la minimizzazione del dato.

All'interno della *blockchain* è possibile revocare i dati, ma per far ciò bisogna creare un nuovo blocco di informazioni: queste non cancellano le precedenti, ma le sostituiscono.

La maggior parte delle aziende, inoltre, non sono in grado di fare sistema visto che si sta parlando di una tecnologia che risulta immatura e in cui è difficile raggiungere a delle soluzioni che siano economicamente sostenibili.

Molte persone inoltre parlano di *blockchain* più per moda che perché abbiano compreso le reali potenzialità di tale tecnologia. Non è infatti semplice individuare, tramite questa tecnologia, risposte a tutte le esigenze del mercato.

La diffusione *blockchain* è stata trainata dal settore Fintech, che gli permette di essere applicata a vari ambiti. Le iniziative sul mondo *blockchain* da parte delle istituzioni finanziarie avvengono tramite 4 modalità principali:

- Sviluppo di gruppi di lavoro e laboratori di ricerca per sperimentare le varie soluzioni blockchain
- Investimento in startup che si occupano di questo tipo di tecnologie sia tramite operazioni *venture capitalist*, che direttamente.
- Partnership con le maggiori aziende del settore blockchain, per avere un'accelerazione sul know-how
- Entrare a far parte di *cross-industry* o consorzi di operatori finanziari, con il fine di definire degli standard omogenei con gli altri membri del settore.

3.2. Mining

Mining è un termine inglese, che significa "estrarre". Siccome nel mondo delle blockchain non esiste un ente centrale che stampa la moneta, ci si chiede come questa possa essere coniata.

Ci sono dei *miner* che, si occupano di creare, o meglio "minare", nuova moneta, in cambio di una remunerazione.

Un blocco è un contenitore che raccoglie tutte le transazioni; quando questo è pieno, si unisce alla catena dei blocchi precedenti. Coloro che permettono di convalidare i blocchi sono i *miner*, che attraverso dei calcoli matematici complessi, arrivano a calcolare il *Codice Hash*. Se il codice hash da loro trovato è lo stesso richiesto dall'algoritmo, il *miner* riceverà il compenso in nuove cripto valute.

L'insieme dei calcoli matematici per la risoluzione del problema è detto *proof of work* ed ha tra gli obiettivi quello di evitare il fenomeno della doppia spesa, che consiste nello spostare, in modo simultaneo, i Bitcoin verso due portafogli, attraverso la stessa transazione.

Il *mining*, quindi, può essere definito come un processo che serve per aggiungere nuovi blocchi alla *blockchain*.

I vari nodi della rete competono tra di loro con il fine di risolvere per primi la *proof of work*.

Nel caso dei Bitcoin, il sistema produce un nuovo blocco ogni 10 minuti e con il tempo, il numero di Bitcoin creati andrà a diminuire, fino all'esaurimento dell'asset, che verrà raggiunto a 21 milioni di unità. Il meccanismo è stato pensato per mantenere la tempistica di 10 minuti, quindi, nel caso in cui,

come sta effettivamente accadendo, il numero di *miner* dovesse aumentare, la difficoltà nel trovare la situazione tenderebbe ad aumentare e quindi ci sarà bisogno di avere una potenza di calcolo proporzionale al numero di minatori.

Ogni 4 anni, inoltre, si ha un processo di "*halving*", che consiste nel dimezzamento della ricompensa per la creazione di un nuovo blocco.

Queste sono caratteristiche che servono a proteggere il Bitcoin dall'inflazione.

Nel caso in cui si dovesse produrre un blocco contraffatto, questo per essere approvato, dovrebbe detenere la maggioranza della potenza di calcolo dell'intera rete. Al giorno d'oggi, il rischio di monopolio del Bitcoin è quasi nullo, nonostante si sia in grado di accentrare una potenza di calcolo elevata.

Inizialmente per essere dei *miner* bastavano dei computer domestici, mentre al giorno d'oggi l'estrazione tramite essi è antieconomica. La prima soluzione fu quella di progettare un hardware che serviva per potenziare il mining dei Bitcoin.

Col tempo si sono sviluppati dei raggruppamenti di *miner*, che uniscono la propria potenza di calcolo con il fine di massimizzare le possibilità di aggiudicarsi i nuovi Bitcoin. Questa pratica, diffusa specialmente in aree fredde e in cui il costo dell'energia è basso, sono chiamate *Pool Mining*.

A causa di questi concorrenti, l'estrazione di Bitcoin domestica risulta ormai obsoleta, a causa degli elevati costi, rispetto ai guadagni.

4. Bitcoin

Partendo da Bitcoin, criptovaluta a maggior capitalizzazione, andremo poi a vedere le altre maggiori cripto.

4.1. Storia dei bitcoin

La nascita di Bitcoin deriva da un movimento, detto Cypherpunk; questo ritiene che l'uso intensivo della crittografia informatica debba essere la via da seguire per ottenere un cambiamento politico e sociale. Gli appartenenti al movimento ritenevano di non potersi aspettare dai governi e dalle grandi società la privacy e quindi iniziarono loro stessi a creare dei software per difenderla. Questo gruppo, già agli inizi degli anni 90', comunicava attraverso delle mailing list crittografate, scrivendo codici software crittografati che consentivano di scambiare informazioni e denaro in modo riservato. Questi codici venivano poi da loro distribuiti gratuitamente, con lo scopo di diffonderli il più possibile.

Nel 1997, Adam Back, membro dei Cypherpunk, realizzò un token, detto Hashcash, con lo scopo di costringere gli spammer a pagare prezzi elevati per inviare le e-mail. Questo sistema diventò in seguito una parte fondamentale per garantire il processo di mining, ma presentava alcuni rischi, tra cui quello della doppia spesa[4] .

Nel 1998, l'ingegnere informatico Wei Dai introdusse l'idea di cripto valuta, in cui proponeva un sistema di cassa anonimo e distribuito.

Nel 2005 l'inventore degli **Smart contract**[5], Szabo, inventò la *bit Gold*, ovvero una valuta digitale che si basava sulla *proof of work*, in questo modo si riuscivano a evitare i problemi della doppia spesa, ma i processi di validazione e protezione del "double spending" avvenivano ancora su un server centrale.

[4] la doppia spesa è una truffa che consente di spendere più volte lo stesso titolo valutario.

[5] gli smart contract saranno trattati più approfonditamente nel prossimo capitolo. Si tratta di protocolli informatici utilizzati per effettuare negoziazioni o esecuzione dei contratti digitali. Il tutto può avvenire senza necessità di interventi da parte di intermediari, grazie ai codici informatici che validano, in automatico, il contratto al verificarsi di determinate condizioni. Il loro campo d'azione spazia dai rimborsi assicurativi alle transazioni finanziarie, fino ad arrivare alla tracciabilità delle merci e alle operazioni societarie. Il concetto di smart contract risale agli anni 90, ma ha trovato il proprio approdo ideale nella blockchain.

Di seguito si illustra un possibile utilizzo degli smart contract: i contraenti scrivono il contratto che vogliono stipulare e lo registrano nella blockchain. I nodi della catena verificano che il contratto sia eseguito in modo corretto e quindi lo smart contract entra a far parte del blocco. Questo, se supera la proof of work, viene aggiunto alla blockchain. A questo punto un soggetto terzo (ad esempio un'applicazione) deve dare conferma alla blockchain che una o più condizioni siano verificate, in modo tale che quest'ultima autorizzi in automatico l'esecuzione del contratto.

Queste idee e innovazioni vennero messe insieme e da “Satoshi Nakamoto“ (dall’identità ancora da svelare), il quale, attraverso la tecnologia blockchain, riuscì a superare molti dei problemi che non erano stati risolti in precedenza.

4.2. Funzionamento Bitcoin rispetto al sistema tradizionale

Nel sistema tradizionale, quando si paga con la carta di credito o con un bonifico, si passa da uno o più intermediari finanziari. L’intermediario procederà con la transazione dopo aver verificato che il soggetto abbia effettivamente il denaro che vuole utilizzare, che la transazione avvenga in modo corretto e che l’intermediario del beneficiario li possa ricevere. A questo punto si perfezionerà la transazione e gli intermediari annoteranno all’interno dei propri server, il fatto che ci sia stato un trasferimento di denaro tra le due parti, ossia un addebito nel conto dell’ordinante e un accredito nel conto del beneficiario.

Nel caso in cui il pagamento avvenga tramite Bitcoin, il processo di pagamento avverrà in modo diverso. Come abbiamo già accennato parlando della blockchain, infatti, le informazioni non sono più in possesso di un intermediario, che in questo caso è del tutto assente. Tutti i dati del le transazioni sono distribuiti tra gli operatori del mercato, visto che è tutto pubblico. Inoltre, non è più sufficiente che un singolo soggetto approvi la transazione, ma è necessario che la maggior parte dei soggetti la approvino, rendendo il tutto molto sicuro.

Quando avviene un pagamento, in questo caso, ci saranno dei *miner* che sono dei soggetti che andranno a controllare i vari blocchi della catena, per verificare se il soggetto pagante abbia effettivamente il denaro che vuole trasferire.

Se l’ordinante non dispone della necessaria provvista, la transazione sarà negata. Altrimenti il pagamento sarà accettato: a questo punto la transazione sarà unita a molte altre, creando così un nuovo blocco all’interno della catena. Il *miner*, per consentire che il blocco venga aggiunto alla catena, dovrà svolgere dei calcoli molto complessi e lunghi attraverso degli elaboratori. Questi calcoli richiedono tempo ed energia, che verrà ricompensata attraverso dei nuovi Bitcoin.

Il fatto che i blocchi siano distribuiti e che tutti ne abbiano una “copia”, rende molto difficile per un hacker manomettere il sistema. Questo dovrebbe infatti avere più del 50% della potenza di calcolo dell’intera rete Bitcoin ed è il motivo per cui risulterebbe molto difficile anche cambiare il funzionamento sostanziale della rete Bitcoin.

4.3. Caratteristiche di Bitcoin

Una delle caratteristiche principali di Bitcoin è la sua scarsità, visto che Satoshi Nakamoto, ha creato questo sistema in modo tale che non possano essere minati mai più di 21 milioni di Bitcoin. Questa è una caratteristica distintiva rispetto agli altri assets finanziari che sono tutti potenzialmente illimitati, a partire dalle valute come dollari ed euro, fino ad arrivare ad azioni e obbligazioni. Questa caratteristica preserva i possessori di Bitcoin da rischi che invece corrono i possessori di altri assets. Nel corso della storia abbiamo infatti visto che nel momento in cui a gestire una valuta sia un essere umano, questa è sempre, anche se in modo più o meno limitato esposta a rischi di inflazione o iperinflazione. Nel caso delle *valute fiat*, infatti, le banche centrali o altre autorità statali possono stampare moneta nel modo che ritengono opportuno. Questo strumento, molto utilizzato dagli stati, espone però i possessori di valuta ad un rischio continuo di un aumento di inflazione (basti pensare alla Francia nell'epoca della Rivoluzione francese o alla Germania nel post Prima guerra mondiale, ma senza dover ricorrere a catastrofi, basti anche pensare all'inflazione che abbiamo vissuto in Italia negli anni 70' dovuta all'aumento dei prezzi petroliferi).

A protezione dall'inflazione c'è un ulteriore accorgimento: la *blockchain* è progettata per aggiungere un nuovo blocco all'incirca ogni dieci minuti. Ci si potrebbe immaginare che con l'aumento di *miner*, o con l'aumento della potenza di calcolo, si riuscirebbero ad ottenere i blocchi in minor tempo. Proprio per far fronte a questo, la difficoltà dei calcoli necessari per minare nuovi Bitcoin, variano in maniera proporzionale al numero di *miner* e alla potenza di calcolo.

Inoltre, ogni volta che un determinato numero di blocchi viene minato, si avrà una ricompensa per singolo blocco minore. Questi processi sono detti *halving*. Ogni circa quattro anni, infatti, la quantità di Bitcoin da dare ai minatori viene dimezzata. Nel momento del lancio di Bitcoin, nel 2009, il sistema permetteva di minare 50 Bitcoin ogni 10 minuti, nel 15 novembre 2012 si ebbe il primo *halving*, che vedeva la ricompensa passare a 25. Al giorno d'oggi la quantità è di 6,25 unità ogni 10 minuti ed il processo continuerà fino a quando saranno state minate 21 milioni di monete.

A questo punto, che si stima essere intorno al 2040, una volta che tutti i Bitcoin saranno creati, i minatori non avranno più la ricompensa finale, ma saranno comunque ricompensati attraverso le commissioni di transazione che sono incluse in ogni nuovo blocco.

Questi processi sono fondamentali perché contribuiscono all'aumento del valore dell'asset a condizione di una stabilità di moneta.

Tutte queste caratteristiche insieme rendono i Bitcoin paragonabili all'oro o ad altri metalli preziosi. Ciò che li accomuna è infatti la scarsità. Rispetto all'oro ha però delle qualità in più:

- mentre non si sa quanto oro ci sia ancora sottoterra, si sa esattamente quale sia il numero di Bitcoin ancora da minare;

- i Bitcoin possono circolare, a livello mondiale, con una semplicità elevata, molto maggiore rispetto a quella dei metalli preziosi.

Fondamentalmente i vantaggi di Bitcoin, dal punto di vista dei promotori sono:

- il sottrarsi dall'azione degli incentivi delle banche e dei governi sovrani, che possono risultare controproducenti;
- maggiore velocità ed efficienza nei pagamenti e nelle rimesse estere (lo afferma la Consob nell'articolo in bibliografia, ma vedremo che non è sempre così approfondendo il funzionamento delle transazioni);
- promozione dell'inclusione finanziaria;
- gli utenti Bitcoin riescono a controllare le proprie transazioni a pieno: non si può intervenire in maniera occulta su esse;
- i pagamenti in Bitcoin possono avvenire senza alcuna informazione personale connessa alla transazione e quindi si è protetti per quanto riguarda il furto di identità;
- tutte le informazioni sui Bitcoin sono sempre disponibili sulla Blockchain e possono essere consultate, in qualsiasi momento da chi lo desideri. C'è quindi un elevata trasparenza, e le informazioni sono fornite in modo neutrale.

4.4. Commissioni su Bitcoin

Le commissioni su Bitcoin, non vengono pagate in base all'importo inviato, ma in base alla quantità di spazio che occupa sul blocco che il *miner* dovrà minare. Quindi la commissione non si calcola in base al valore della transazione, ma in base alla dimensione a livello informatico. La commissione inoltre non è né fissa né imposta, ma viene stabilita dall'utente. I *miner*, infatti, possono scegliere se includere una transazione o meno all'interno del proprio blocco e probabilmente includeranno le transazioni che gli garantiranno profitti maggiori. Il metodo di pagamento delle commissioni può quindi essere paragonato ad un'azienda di trasporti, in cui non si paga in base al valore del bene, ma alla dimensione della scatola.

Dal punto di vista di chi vuole effettuare la transazione in Bitcoin, questo dovrà espettare che l'operazione venga convalidata. Si verrà così a creare una lista d'attesa per la convalida. Per accelerare la velocità della transazione sarà sufficiente pagare delle commissioni più alte ed avere una priorità maggiore. Non si avrà mai la certezza sul tempo esatto che sarà necessario per il processo di accettazione.

4.5. Rischi e caratteristiche dei Bitcoin

I **rischi** dal punto di vista del consumatore sono altresì molteplici:

- abbiamo detto che le "regole" nell'ambito Bitcoin siano molto complesse da cambiare, proprio grazie alla propria struttura. È tuttavia possibile che una grande potenza di calcolo riesca ad assumere il 51% della potenza di calcolo. Così facendo, molte delle sicurezze e delle certezze che si hanno su questa cripto valuta vacillerebbero e verrebbero messe in discussione: sarebbe addirittura possibile distruggere Bitcoin. Nel corso della storia è accaduto che la società Gash.Io arrivasse a controllare oltre il 50% della rete, ma al giorno d'oggi questa società non è più operativa ed il potere hash è più distribuito;
- non essendoci un quadro giuridico preciso, risulta complicato, attuare una tutela legale e contrattuale nei confronti degli utenti, che si potrebbero trovare pressoché disarmati nel caso in cui le piattaforme che custodiscono gli e-wallets (portafogli digitali personali), dovessero fallire o comportarsi in modo fraudolento;
- le piattaforme on-line di scambio sono esposte a rischi operativi e di sicurezza (frodi e cybercrimes) più elevati rispetto agli intermediari riconosciuti visto che non sono tenute a dare alcuna garanzia di qualità e non devono rispettare alcun requisito patrimoniale;
- il Bitcoin è ancora poco diffuso e pertanto vi è un elevata volatilità: bastano piccoli scambi, eventi o attività speculative per causare variazioni di prezzo elevate. Questo problema potrà essere risolto solamente con una maggior conoscenza o con un maggior utilizzo dell'asset; solo allora il prezzo sarà stabile;
- il Bitcoin, essendo una cripto valuta, è visto come moneta digitale e decentralizzata. Ricordiamo che le monete devono avere 3 funzioni principali: unità di conto (metro comune per misurare il valore); mezzo di scambio (consente di accettare un oggetto in cambio di un altro, con l'aspettativa di poter utilizzare lo stesso anche per scambi futuri); riserva di valore (capacità di mantenere il proprio valore nel tempo, senza che questo si deteriori). Dopo aver definito le caratteristiche che deve avere una moneta, il professore Ferdinando Ametrano, docente di Blockchain technologies all'università Bicocca di Milano, afferma che secondo lui "la criptovaluta non può considerarsi unità di conto perché è come un metro che con il passare del tempo si allunga o si accorcia". Personalmente ritengo tale considerazione condivisibile visto che presenta evidente carenze nell'ambito di unità di conto.

Se si volesse paragonare ad una moneta, questa probabilmente potrebbe essere una moneta merce, in quanto fondamentalmente quello che si va a scambiare è un bene virtuale la cui quantità è limitata: un paragone storico potrebbe essere fatto con lo scambio di metalli preziosi del passato.

Proprio come l'oro, inoltre, il prezzo è dato dall'incontro della domanda e dell'offerta. Si è cercato a lungo di trovare una correlazione con delle variabili (ad esempio con il consumo di energia); ma la verità che se domani ci fosse una richiesta smisurata di Bitcoin il prezzo di questo schizzerebbe alle stelle, viceversa il contrario (a prescindere dal consumo di energia o dal prezzo di questa).

Tuttavia, i prezzi sono talmente variabili che a mio avviso non potrebbe essere neanche definita moneta merce. Fa riflettere il fatto che con un Bitcoin a Settembre del 2020 si potesse comprare a malapena un'utilitaria (quotazioni intorno ai 9000 euro) e a novembre 2021 un suv di fascia medio-alta (quotazioni che superano i 50 mila euro), per poi riscendere fino agli attuali 35000 euro (quotazioni degli inizi di marzo '22). Anche i metalli preziosi hanno visto le loro valutazioni fluttuare, ma in modo molto più contenuto e in modo proporzionale alle crisi: In un biennio in cui stiamo vivendo una pandemia e ora lo scoppio della guerra in Ucraina il valore dell'oro è cresciuto in modo pressoché costante, il che non si può dire per il Bitcoin.

Andamento della quotazione del Bitcoin 2017-2022 al 22 marzo 2022 - Fonte: Google Finanza

Queste considerazioni, basate soprattutto sulle quotazioni finanziarie degli asset evidenziano come al momento i due strumenti si comportino in modo molto differente. È però, secondo me, fondamentale considerare il fatto che l'oro abbia uno storico che va avanti da migliaia di anni, mentre i Bitcoin, devono compiere ancora il 15esimo compleanno. Altra differenza è data dal fatto che i Bitcoin si basino su dei processi molto complessi da capire ed approfondire e che quindi molte persone non investono in essi per motivi legati alla mancanza di conoscenza in materia piuttosto che ad una scelta consapevole e studiata.

Non escludo perciò il fatto che le fluttuazioni dei Bitcoin dipendano da elementi come scarsità di informazione e da uno storico troppo giovane. Ritengo che queste in un futuro potrebbero essere considerate “come un oro del futuro”.

Per avvalorare la tesi ricordo che anche l’oro, nonostante possa essere usato per scopi industriali o per la realizzazione di gioielli, non vede il proprio prezzo giustificato dalla funzionalità o dalle caratteristiche fisiche, bensì dal mercato.

Sul tema Bitcoin si sentono pareri discordanti, anche tra i maggiori investitori: c’è chi crede molto nel progetto e chi invece lo considera fallimentare e da evitare in ogni modo.

Basti pensare al fatto che Charlie Munger, socio storico di Warren Buffet ne abbia parlato così, durante la riunione annuale di Berkshire del 1 maggio 2021: “Certo che odio il successo dei Bitcoin. Non accolgo favorevolmente una valuta che possa essere così utile per i delinquenti, e non mi piace trasferire miliardi di dollari a qualcuno che ha appena inventato dal nulla un nuovo prodotto finanziario. Penso di dover dire, con modestia, che l'intero dannato sviluppo è disgustoso e contrario agli interessi della civiltà”.

Anche lo stesso Warren Buffet si era riferito al mondo delle cripto valute definendole come “deludenti” e come “veleno per topi”.

Dall’altra parte ci sono invece tutta una serie di miliardari che invece sono diventati miliardari proprio grazie alle cripto valute:

- Brian Amstrong, ad esempio può vantare di un patrimonio di oltre 7 miliardi di dollari grazie alla fondazione della piattaforma Coinbase;
- Bankman-Fried, che grazie alla creazione dell’Exchange di cripto valute Ftz, si è riuscito a guadagnare il primato di under 30 più ricco del mondo.

Secondo Forbes, nel 2021, grazie al boom dei Bitcoin, il settore ha visto emergere 11 nuovi miliardari.

Il fatto che ci siano molti pareri discordanti è una delle cose che mi ha maggiormente incuriosito, e come nella maggior parte dei casi credo che in queste situazioni la verità sia nel mezzo. Secondo me i Bitcoin hanno le potenzialità per crescere e diventare un asset sempre più valido: sono paragonabili all’oro data la loro scarsità e nonostante non possano avere alcune funzioni tipiche dell’oro (ad esempio essere utilizzate come conduttori, gioielli ecc.) ne hanno altre che, a mio avviso, hanno un’importanza ancora maggiore: in particolare il fatto di essere così facilmente scambiabile, le fornisce caratteristiche che, nel tempo (siccome per ora è decisamente prematuro dati i ragionamenti fatti in precedenza affermare una cosa simile) potranno renderla simile a quella delle valute fisiche.

D’altro canto, è anche vero che il valore di beni simili è dato dall’incontro tra la domanda e l’offerta. Non è detto che Bitcoin continui ad avere tutto questo successo e c’è addirittura la possibilità, anche se secondo me remota, che questa perda tutto il proprio valore in pochi giorni.

Al giorno d’oggi penso che Bitcoin debba essere visto ancora come un asset speculativo, in cui investire solamente dopo aver capito effettivamente le potenzialità di esso. Anche se è uno degli strumenti che ha registrato performance migliori degli ultimi anni, bisogna essere consapevoli del fatto che il futuro non replicherà necessariamente il passato.

Personalmente credo che, sulla carta, Bitcoin abbia tutte le caratteristiche per continuare a crescere nel tempo. Vorrei però concludere il ragionamento con tre domande:

- “Bitcoin è stato inventato da Satashi Nakamoto, il quale ha stabilito che il numero massimo di Bitcoin fosse di 21 milioni, perché noi siamo così sicuri che nessuno riuscirà a cambiare questo numero?”.
- “Nel corso della storia, è accaduto che una società riuscisse a possedere oltre il 50% della potenza di calcolo, ma che comunque non avrebbe effettuato un attacco alla catena perché questo non sarebbe stato effettivamente conveniente. Nel momento in cui i *miner* guadagneranno solo sulle commissioni (perché raggiunti i 21 milioni di Bitcoin minati), e nel caso in cui le quotazioni salissero, potremmo avere ancora la certezza del fatto che non ci sia un “attacco al 51%”?
- “Bitcoin presenta grandi problemi soprattutto dal punto di vista della criminalità: favorisce le transazioni di attività illecite, favorisce il riciclaggio di denaro, la corruzione ecc. Può essere visto come la “valigetta piena di contanti” o il “sacchetto di diamanti” 2.0; a questo punto quindi mi chiedo: anche nel caso in cui l’attacco al 51% non fosse in alcun modo conveniente, è possibile che siano gli stessi stati ad effettuarlo con lo scopo di combattere l’illegalità e di non vedere le proprie politiche monetarie minacciate in alcun modo?

Alla luce delle considerazioni fatte ritengo che nel caso in cui si dia per certo il fatto che il funzionamento dei Bitcoin rimanga invariato, senza subire alcun tipo di attacco, questo possa essere un ottimo assets che nel futuro potrebbe continuare a sorprendere. La quasi totalità delle persone ritiene che sia molto sicuro e che sia pressoché impossibile riuscire ad effettuare comportamenti fraudolenti nei confronti della blockchain (le truffe si possono verificare eventualmente sulle piattaforme di trading di valute o comunque su intermediari esterni alla catena). Per di approfondire maggiormente questo argomento, ora tratterò alcune minacce che potrebbero spaventare i possessori di Bitcoin, vedendo se queste siano effettivamente così remote.

Inizieremo il discorso approfondendo il rischio dell’ “attacco al 51%”: in cui la maggior parte degli hash della rete sono controllate dallo stesso soggetto, il quale può effettuare operazioni ai danni degli altri utenti. Se il 51% del network è sotto il controllo dello stesso gruppo di minatori, questi

riusciranno a diffondere e validare blocchi falsi nella rete. Verrebbe perciò a mancare la centralità, che è ciò su cui si basa l'intero universo Bitcoin.

Nel caso in cui ciò dovesse accadere, colui che detenesse la maggioranza dei nodi della catena, riuscirebbe a controllarla in modo totale. Ciò gli consentirebbe di avere molteplici poteri:

- può approvare operazioni di doppia spesa e quindi spendere la stessa moneta più volte;
- può aggiungere dei nuovi blocchi;
- può negare l'approvazione di transazioni che altrimenti risulterebbero valide;
- potrebbe impedire il mining degli altri miner, ottenendo così il monopolio di mining.

Nell'agosto del 2016 la mining pool Gash.io riuscì ad ottenere circa il 55% della rete e ridusse volontariamente la propria quota al 40%. Rispetto ad allora il network è cresciuto molto ed è proprio il fatto che ci sia un'elevatissima quantità di nodi che dà sicurezza agli utenti.

Bisogna inoltre considerare che si può modificare un determinato blocco solo a condizione che vengano eliminati tutti quelli successivi e quindi, all'aumentare dei blocchi, risulta sempre più complesso eliminare la catena di blocchi a seguire.

In altre cripto valute, anche se a capitalizzazione minore, è stato sferrato un attacco di questo tipo (Krypton, Shift, Verge ecc.)

La cosa positiva è che la parte che attacca in questo modo la rete Bitcoin non può modificare le informazioni dei blocchi già esistenti e non può neanche generare delle nuove monete. Non è neanche possibile rubare monete mai appartenute all'attaccante.

Il fatto che il network di Bitcoin sia così vasto la rende la più sicura tra le cripto valute che si basano sulla *proof of work*.

Dopo esserci fatti un'idea di quanto, effettivamente, sia improbabile un attacco alla rete Bitcoin, vediamo che invece gli attacchi dovuti al modo in cui queste cripto valute sono detenute sono molteplici. Vedremo ora le minacce che possono verificarsi a monte o a valle della catena:

- Phishing: ci sono molti siti web che imitano gli Exchange con il fine di rubare i dati le credenziali di accesso ai portafogli digitali. È perciò necessario prestare attenzione che l'indirizzo del sito web sia esatto ed è inoltre necessario proteggerli tramite un certificato HTTPS. Bisogna assicurarsi inoltre che la rete WiFi a cui ci si collega utilizzi protocolli avanzati.
- Altri rischi derivano inoltre dalla stabilità degli Exchange stessi. Mi ha colpito particolarmente l'attacco hacker avvenuto nel 2014 ai danni del maggior portale per scambio di cripto valute di quei tempi: "Mt.Gox". In quell'occasione furono rubati 850.000 Bitcoin, per un valore, alle quotazioni di allora, di 473 milioni di dollari. Il che fa ancora più impressione se si pensa al fatto che in base alle valutazioni di oggi, quel furto varrebbe oltre trenta miliardi di dollari (riferimento

alle quotazioni dell'8 marzo 2022). Fortunatamente ci sono dei modi per tutelarsi e limitare l'esposizione al rischio exchange.

I portafogli digitali possono infatti essere divisi in due macro-categorie: caldi e freddi.

- gli *hot wallets*, possono essere consultati sempre e sono connessi ad internet (portafogli su dispositivi mobili, portafogli cloud online, exchange ecc.
- I *cold wallets* consentono invece di memorizzare i propri fondi offline, senza quindi aver bisogno di essere connessi ad internet (portafogli hardware, dispositivi di archiviazione offline, chiavette usb ecc.)

Il consiglio è perciò quello di separare i propri fondi: i *wallet* caldi sono indicati per effettuare transazioni o trading, mentre quelli freddi sono più funzionali per chi vuole detenere i Bitcoin a lungo termine.

Ci sono inoltre altri rischi, meno frequenti, che possono coinvolgere i possessori del cripto-asset. Basti pensare al fatto che ci sono dei programmi che possono modificare l'indirizzo di transazione errato ad ogni invio di una transazione: in questo caso bisogna verificare attentamente e più volte gli indirizzi cripto, per evitare di inviare di inviare i nostri Bitcoin a dei male intenzionati. Ci sono inoltre tutta una serie di misure di prevenzione, tra cui l'autenticazione a due fattori e l'utilizzo di un indirizzo IP statico.

Altro rischio che si corre è inoltre quello di eccedere con l'utilizzo delle misure di sicurezza e quindi non riuscire più ad accedere ai propri fondi. Bisogna perciò trovare delle misure di sicurezza commisurate alle proprie conoscenze, non rischiando così di perdere l'accesso al proprio account. A tal proposito, cito una storia che mi ha particolarmente colpito: quella di un programmatore tedesco, il quale non riusciva più ad accedere alla propria Ironkey, all'interno della quale c'erano oltre 7.000 Bitcoin. Questa chiave fornisce agli utenti 10 tentativi prima di bloccarsi e siccome Bitcoin non offre un servizio per il ripristino della password, il fatto che il programmatore non se la ricordasse lo ha messo in grave difficoltà.

Di storie così se ne sentono molte, altro fatto eclatante è stato quello della morte prematura di Gerald Cotten, fondatore della piattaforma QuadrigaCX: in questo caso la piattaforma è diventata inaccessibile, bloccando quindi non solo il proprio patrimonio, ma anche il denaro di molti altri investitori, che operavano tramite l'Exchange. In quell'occasione sono andati persi 26.500 Bitcoin, oltre che un'altra serie di cripto valute (tra cui 430.000 Ethereum).

Si stima che in tutto siano andati persi quattro milioni di Bitcoin e il che ci fa capire quanto questo possa rappresentare un problema tanto importante quanto sottovalutato (anche se col crescere del valore dell'asset credo che questi episodi tenderanno a diminuire!).

5. Ethereum

Ethereum è una piattaforma blockchain, decentralizzata di seconda generazione, che nacque nel 2013 grazie allo sviluppatore russo Vitalik Buterin, con lo scopo di riuscire a svolgere operazioni più complesse rispetto a Bitcoin. Anche alla base del funzionamento di Ethereum ci sta una blockchain che viene gestita dagli utenti stessi. Il sistema è tra l'altro open source e quindi qualsiasi operatore può apporre delle migliorie, le quali devono però essere prima controllate dalla Ethereum Foundation (azienda no profit Svizzera).

5.1. Cenni storici Ethereum

Nel 2014 Buterin riuscì a raccogliere i fondi necessari per il progetto tramite un'operazione di *crowdfunding* e a luglio dell'anno successivo il sistema venne reso pubblico e tutti ne potettero usufruire. Attualmente è la seconda cripto valuta per capitalizzazione, seconda solo a Bitcoin. Ad oggi, martedì 8 marzo, può infatti vantare di una capitalizzazione di mercato di oltre 283 miliardi di euro. Sta assumendo un'importanza sempre maggiore e quinti ritengo necessario parlarne, basti pensare che è la valuta alla base anche dei meccanismi più moderni che si stanno sviluppando recentemente, come ad esempio, il Metaverso e gli NFT.

5.2. Funzionamento Ethereum

Vediamo ora come funziona la rete Ethereum, ma anche la correlazione che si ha con il token ETH.

Partiamo dalla definizione di Ethereum presa da Wikipedia per poi spiegarla: "Ethereum è una piattaforma decentralizzata Web 3.0 per la creazione e pubblicazione peer-to-peer di contratti intelligenti (smart contracts) creati in un linguaggio di programmazione Turing-completo. La cripto valuta a esso legata è Ether".

Ci sono varie definizioni di web 3.0, tuttavia la più coerente con l'ambito che stiamo considerando è che sia l'evoluzione del modo di utilizzare il web e l'interazione tra i molteplici percorsi di evoluzione diversi. Gli obiettivi posti sono molteplici e riguardano aree differenti: dal voler trasformare il web in un database, col fine, di garantire anche ad altre applicazioni che non siano browser, un accesso facilitato ai contenuti, allo sfruttamento delle tecnologie che sfruttano l'intelligenza artificiale al web semantico ecc.

Lo stesso Ethereum rappresenta un'innovazione tipica del Web 3.0 visto che è la maggior rete peer-to-peer di smart contracts. Ciò significa che si basa su una rete decentralizzata e senza gerarchie, all'interno della quale i clienti possono stipulare smart contracts in totale libertà digitale.

Le transazioni sono garantite dalla scrittura su una blockchain pubblica e quindi gli utenti non hanno bisogno di ricorrere a intermediari.

La scrittura della blockchain Ethereum utilizza linguaggi di programmazione Turing completi.

Per linguaggio di programmazione Turing completo si intende un linguaggio che ha una potenza espressiva almeno pari a quella necessaria per programmare ogni tipo di macchina di Turing[6].

Grazie a queste tecnologie non è necessario un terzo soggetto che regolamenti e medi la transazione, visto che la transazione è istantanea e sarà inoltre validata dallo stesso linguaggio di scrittura.

Gli smart contract, citati sopra, sono dei codici che vengono eseguiti sempre allo stesso modo dalla blockchain; così facendo si ottiene un sistema deterministico, grazie al quale, attraverso gli stessi input, si otterranno sempre i medesimi risultati. Il punto di forza di questi contratti, quindi, è fatto che all'effettuarsi di un determinato pagamento, il pagante può essere sicuro di ricevere lo stesso servizio.

Nonostante si chiamino contratti, non vanno confusi con i contratti legali, in quanto non devono essere compilati. Questi eseguono delle porzioni di codice interessate durante una transazione e effettuano un controllo diretto sul proprio conto di valuta Ether, con lo scopo di conservare la traccia delle variabili, garantendo sia trasparenza che tracciabilità. All'interno di ogni transazione sono presenti informazioni inerenti a:

- Firma del mittente e nome del destinatario
- Quantità di Ether che sono coinvolti nella transazione
- Il numero massimo di passaggi che si possono eseguire nella transazione
- La commissione che il mittente paga per lo step computazionale e quindi la cifra da pagare al network per poter effettuare le transazioni e far circolare gli smart contracts.

Questo tipo di contratto è detto intelligente perché risponde agli input con degli output conseguenziali. Consente quindi di vincolare, in modo inderogabile, i contraenti alle regole da loro condivise al momento dell'accordo.

Nel caso di Ethereum questi programmi possono essere utilizzati sia per facilitare lo scambio di denaro, che per arricchire l'ecosistema Ethereum. La novità rispetto all'avere un programma normale

[6] La macchina di Turing è un sistema che, programmato correttamente, è in grado di eseguire ogni tipo di operazione, è un modello di agente di calcolo che è in grado di simulare la logica di ogni tipo di algoritmo computazionale.

che gira su un dispositivo, come il nostro computer, consiste nel fatto che mentre sviluppo un programma, sono io che lo scrivo, nel momento in cui però lo consegno ad Ethereum, ne perdo il controllo e quindi tutti possono vedere come è fatto. Tutti gli utenti possono perciò esprimere un'opinione riguardo l'ottenimento di un determinato output, a partire da un certo input.

Per verificare se la transazione è andata a buon fine bisognerà raggiungere una maggioranza. Il tutto è quindi fatto in modo estremamente trasparente.

Un esempio pratico del vantaggio della Blockchain, riferito al gioco d'azzardo online, può essere quello di avere delle garanzie su un corretto funzionamento della roulette: su blockchain posso infatti vedere il codice su cui si basano le estrazioni della roulette e si può quindi controllare se effettivamente l'estrazione sia effettuata in modo casuale, senza alcuna interferenza nella comunicazione del numero uscito. Questo è possibile grazie al meccanismo del codice *open source* e trasparente, che permette di poter effettivamente controllare la regolarità dello strumento utilizzato.

Per effettuare le transazioni in Ethereum, come in Bitcoin, bisogna pagare delle commissioni ai *miner*, per far sì che questi aggiungano le proprie transazioni ai blocchi, che poi verranno aggiunte alla blockchain. Ed anche in questo caso ci sono dei tempi di attesa dovuti al fatto che la rete deve comunicare e i vari nodi devono sincronizzarsi per raggiungere un consenso sul risultato finale dell'operazione.

Gli utenti di Ethereum utilizzano una rete *peer-to-peer* e quindi sviluppano i contratti Ethereum servendosi delle risorse computazionali della rete. Queste risorse hanno un costo che viene remunerato tramite gli Ether. Queste sono monete virtuali che hanno duplice funzione:

- Quella di *token* transazionale che serve ad autorizzare le operazioni su Ethereum, fungendo quindi da carburante per la blockchain
- Quella di valuta virtuale (seconda solamente a Bitcoin per capitalizzazione)

Ethereum quindi si basa su degli *smart contract* che permettono di gestire i contratti in modo pubblico e allo stesso tempo sicuro, attraverso una remunerazione in Ether. Vengono così regolate attività come il *crowdfunding*, gestione del diritto d'autore, registrazione di domini ecc.

Una delle maggiori applicazioni di Ethereum, riguarda proprio la finanza decentralizzata; pertanto, si è cercato di fornire i servizi tipici della finanza tradizionale, creando però anche delle novità:

- Ethereum dà la possibilità di creare nuove monete e quindi ci sono compagnie che hanno provato a creare delle "*stable coin*"[7] ;
- Ethereum consente di chiedere un prestito utilizzando le cripto valute come garanzia;

[7] cripto valute che vogliono limitare la volatilità tramite un sottostante che può essere una valuta fisica, beni materiali o altre cripto valute.

- è disponibile una funzione di deposito, che sono remunerati tramite la corresponsione di interessi;
- È possibile fruire di "prestiti flash", che consistono nel prendere a prestito delle cripto valute, potendo effettuare delle operazioni con esse, a patto che si sia in grado di restituire la somma nella stessa transazione.

Il funzionamento di Ethereum si basa sulla *Ethereum virtual machine* (EVM), che è l'ambiente attraverso cui vengono sviluppati e gestiti gli *smart contract* del sistema. Questo meccanismo consente a tutti i partecipanti di eseguire algoritmi su una rete globale che si basa sui nodi della rete (questi vengono poi ricompensati tramite Ether).

Le attività di ricerca, sviluppo e supporto della piattaforma Ethereum sono gestite dall'organizzazione "Ethereum Foundation". Questa inizialmente aveva la forma di un'impresa e successivamente fu trasformata in fondazione *no-profit*. Questa società, con sede in Svizzera, si finanziò inizialmente nel 2014 tramite il *crowdfunding*; promettendo ai finanziatori di acquistare Ether tramite Bitcoin. Il suo scopo principale è quello di dare sostegno (sia finanziario che non) ai progetti che riguardano la comunità Ethereum per rendere la crescita dell'ecosistema il più rapida possibile. Quest'organizzazione vuole massimizzare l'espressione di Ethereum a livello globale ed ha quindi il ruolo di prendere decisioni inerenti alla piattaforma. Il potere che ha questa fondazione potrebbe preoccupare gli utenti visto il rischio di centralizzazione. Proprio a tutela degli utenti Ethereum, per favorire il mantenimento del decentramento, si è mantenuta la filosofia di libera espressione delle idee all'interno del progetto, organizzandolo tramite il modello di sviluppo *Bazaar* (come, ad esempio, quello di Linux) e non *Cathedral* (come la maggior parte dei software proprietari). Grazie a questo sistema gli utenti sono in grado di migliorare il progetto in autonomia e presentare le proprie migliorie, che verranno applicate nel caso in cui risultino effettivamente utili per la collettività.

Nel 2015 è stato inoltre creato il programma DEVgrants, con il quale si vuole premiare e incentivare il lavoro degli sviluppatori che lavorano sulla piattaforma.

Nello stesso periodo è stato inoltre lanciato il programma "Ethereum Bug Bounty", questo programma, ancora in corso, consiste in una gara tra gli utenti a chi riesce a trovare più bug o vulnerabilità possibili nel sistema. Chi ne trova riceve delle ricompense e chi ne trova di più, sale anche nella classifica del sito web.

Questi, come gli altri metodi per garantire la sicurezza, vanno però a incidere negativamente sul numero di transazioni al secondo che possono essere effettuate dalla piattaforma (circa 20). Questo è infatti uno dei prezzi da pagare, oltre quello energetico, per avere una rete così ampia e sviluppata. Al momento Ethereum è ancora una nicchia, ma sicuramente a lungo andare questo potrebbe rappresentare un problema.

Altro problema che cresce in modo proporzionale alla crescita della blockchain è il peso che ha il mantenere traccia di tutta la lista di transazioni, da quando è nata, della piattaforma. Al momento è di quasi 6 TB e la soluzione non può essere quella di eliminare le transazioni più vecchie visto che così facendo si andrebbe a perdere il concetto di blockchain.

Inoltre, con l'aumento degli utenti, aumenterà anche il costo delle transazioni e questo potrebbe causare l'esclusione dall'utilizzo di Ethereum di tutti coloro che non muovono grandi capitali e che quindi non riterranno accettabile il pagamento di commissioni troppo alte rispetto alle transazioni che vogliono effettuare. Anche in questo caso, come in Bitcoin, pagando delle commissioni maggiori, si ridurrà il tempo di attesa della transazione, visto che il *miner* sarà più propenso a includerla nel proprio blocco.

5.3. Ethereum 2.0 e Proof of Stake (PoS)

Da quando è nata, la piattaforma Ethereum ha vissuto un continuo sviluppo, ricevendo continue migliorie, in ogni ambito. Ora però si sente parlare di un cambiamento molto più grande e che andrebbe a cambiare proprio la sua struttura sostanziale. Con Ethereum 2.0, infatti, si vuole cambiare il meccanismo di consenso: da *Proof of Work* (PoW) a *Proof of Stake* (PoS). In questo modo si potranno risolvere alcuni dei problemi citati prima tra cui quello del numero limitato di transazioni e quello di avere una piattaforma più sostenibile a livello energetico. Ricordiamo infatti la vision riportata sul sito ufficiale di Ethereum "portare Ethereum nella rete principale e servire l'umanità, dobbiamo rendere Ethereum più scalabile, sicura e sostenibile".

La PoS è un algoritmo di consenso che fu proposto per la prima volta nel 2011 come soluzione ai problemi connessi all'ingente consumo richiesto dal sistema di PoW di Bitcoin. Questo sistema consente di sostituire il processo di mining, con un sistema in cui il consenso si basa sul principio secondo cui ogni utente ha potere in base al numero di cripto valuta che possiede. In questo sistema, i *miner* sarebbero sostituiti da dei *Validator* che avranno il compito di garantire che le operazioni effettuate siano valide, tramite l'impiego di una quota delle proprie cripto valute a garanzia. Le probabilità di essere selezionati come *validator* variano in funzione della quantità e della longevità delle cripto valute depositate. C'è anche una componente casuale, che serve a limitare il rischio di far arricchire ulteriormente i più ricchi della rete. Per capire come funziona questo sistema di scelta, paragoniamolo a un'estrazione tra i vari *validator*: chi ha più cripto longeve, avrà più bigliettini, e quindi più possibilità di essere estratto, ma questo non significa che chi ha meno bigliettini non possa esserlo.

Per evitare che i nodi che posseggono ingenti qualità di assets, dominino le reti, c'è un processo che impedisce, per un determinato periodo, all'utente che è appena stato nominato *validator*, di essere

selezionato nuovamente come tale. Il compenso dei *validator*, consisterà in una percentuale sulla commissione della transazione che andranno a validare e non più quindi tramite la creazione di nuova moneta. Se il *network* vede che si verifica una transazione fraudolenta, il nodo perde sia il proprio deposito, che la possibilità di essere selezionato in futuro come *validator*. L'unico modo per aggirare la rete sarebbe quindi quello di possedere il 51% delle cripto valute in circolazione. Viene così ridotto il rischio di attacchi al sistema e inoltre si incentivano gli utenti a detenere sempre un ingente somma di Ethereum, per poter essere selezionati a *validator* (per cui sono stimati rendimenti tra il 5 e il 10% sullo *stake*).

Per quanto riguarda il fattore del risparmio energetico, avviene perché l'algoritmo selezionerà in pochi secondi il *validator* e questo impiegherà pochissimo tempo per validare la transazione (nel momento della convalida si espone economicamente con il deposito dato a garanzia). Si risparmia così dal punto di vista energetico e temporale visto che non si dovranno risolvere problemi matematici complessi.

Abbiamo visto quindi che cambiando il meccanismo di consenso, Ethereum riuscirebbe a risolvere alcuni dei suoi problemi maggiori. Questo è proprio il motivo per cui nella community ci si sta concentrando sullo sviluppo di "Casper" ovvero su un aggiornamento che consentirà alla Blockchain di basarsi sulla *Proof of Stake.* Così facendo riuscirebbe anche ad essere più apprezzata anche al di fuori degli utenti, visto che rispetterebbe maggiormente l'ambiente.

Probabilmente questo aggiornamento avverrà tra il 2022 e il 2023.

Il discorso inerente alla difficoltà derivante del numero di transazioni, nello specifico, viene risolto tramite un processo detto "*shard*": quando si pensa alla blockchain si pensa ad un'unica catena in cui i vari blocchi vengono aggiunti. Con lo *sharding*, sarà possibile dividere la catena in più sotto catene. È come se ci fosse una catena centrale, alla quale si aggiungono catene minori ed il vantaggio sta proprio nel fatto che lavorare su questi frammenti di catena richiede costi nettamente inferiori: i nodi saranno così più veloci e gli algoritmi da utilizzare saranno più efficienti. Tramite questo meccanismo innovativo, la fondazione mira a voler riuscire a raggiungere le 100.000 transazioni al secondo.

Gli sviluppatori Ethereum stanno lavorando e continueranno a lavorare con il fine di potenziare e migliorare la piattaforma senza però andare a gravare sulla decentralizzazione.

Rispetto a Bitcoin, Ethereum risulta essere una realtà molto più complessa ed innovativa, basti pensare al fatto che mentre la prima nasce e si sviluppa con lo scopo di essere esclusivamente un mezzo di scambio, la seconda, nasce come una piattaforma, che ha tra le sue funzioni quella di essere una valuta, basti pensare ad Ether, ma ne ha anche molte altre funzioni:

- Dà innanzitutto la possibilità di creare cripto valute diverse; in particolare, può essere un mezzo per la creazione di *stablecoin*, ovvero delle cripto valute che hanno molte

caratteristiche in comune con gli Ether, ma la cui volatilità è limitata da un collaterale. Ci sono moltissimi tipi di *stablecoin* diversi e questi possono essere scambiati per Ether tramite la piattaforma Ethereum. Nella scelta dello *stablecoin* da acquistare è necessario informarsi prima correttamente: bisogna innanzitutto considerare il fatto che i token vengono realizzati da enti centralizzati e quindi bisogna assicurarsi che questi abbiano riserve sufficienti.

- Consente di realizzare un Exchange decentralizzato; il vantaggio è che in uno centralizzato si ha un'autorità centrale di cui bisogna fidarsi e, come visto nel caso delle piattaforme QuadrigaCX o Mr.Gox, questa fiducia rappresenta un rischio. Il fatto di poter avere un Exchange decentralizzato ci permette di arginare il "rischio Exchange". All'atto pratico, per creare queste piattaforme bisogna programmare delle applicazioni, costruite come degli *smart contract*, che permettono agli utenti di scambiare i propri assets con gli altri players del mercato, mantenendo però il controllo dei propri fondi.
- Altro argomento interessante, esploso negli ultimi mesi è quello dei token non fungibili (NFT: Non Fungible Token) e quindi dei token che sono unici e questa unicità può essere dimostrata. Lo esamineremo in modo più approfondito successivamente.
- Nell'ambito delle assicurazioni consentirebbe di stipulare delle polizze che risarcirebbero in automatico al verificarsi dell'evento assicurato. Ciò consentirebbe una gestione decentralizzata delle polizze assicurative.
- Gli *smart contract* potrebbero essere utilizzati per il miglioramento della tracciabilità dei prodotti, consentendo così di perfezionare anche il settore della logistica.
- Gli *smart contract* possono essere inoltre applicati ad altri ambiti; tra cui quello del crowdfunding, della tutela della proprietà intellettuale e la compra-vendita, anche rateale dei beni.

Per quanto Ethereum stia lavorando per velocizzare i propri processi di transazione, questa piattaforma è comunque, anche al momento, più efficiente di Bitcoin: circa 15 transazioni al secondo contro 5/6 dati presi dal sito:

https://www.italian.tech/2021/07/05/news/bitcoin_e_il_trilemma_blockchain-307521114/

Anche dal punto di vista dei consumi, Bitcoin richiede oltre 700 kWh ora di elettricità, mentre Ethereum non ne richiede nemmeno 100. Bisogna considerare inoltre il fatto che mentre i consumi di Bitcoin rimarranno molto alti, Ethereum sta lavorando per ridurli ulteriormente tramite il passaggio alla *proof of stake*. In questo modo i consumi si ridurrebbero, secondo stime di circa 10.000 volte.

Personalmente, ritengo che Ethereum rappresenti il futuro delle cripto valute e, soprattutto se il progetto Ethereum 2.0 andrà a termine, riuscirà ad assumere sempre più importanza sia a livello

finanziario che in ogni sua altra forma di applicazione. La varietà di cripto valute che si basano su questa piattaforma e la varietà di operazioni che consente di effettuare, rappresentano sicuramente un valido motivo per cui gli utenti dovrebbero preferirla ad una piattaforma meno varia e meno efficiente sia dal punto di vista energetico, che quello temporale. Credo quindi che a lungo andare Bitcoin tenderà ad essere considerata sempre di più come riserva di valore (data la sua scarsità) e sempre meno come moneta o strumento da utilizzare per le transazioni o le operazioni finanziarie più comuni.

I rendimenti dell'ultimo lustro mostrano che le performance di Ether siano state molto maggiori rispetto a quelle di Bitcoin il che ha portato il gap tra i due assets a ridursi. Vedo che online molte persone confrontano i due rendimenti, autoconvincendosi che, dato lo storico e le diversità tra le due piattaforme, probabilmente Ethereum riuscirà a sovrastare, nel tempo Bitcoin.

Personalmente, ritengo che il concetto su cui bisogna soffermarsi sia proprio quello della diversità: a mio avviso, i due assets non dovrebbero essere rivali, bensì complementari.

L'oro è sicuramente meno efficiente, come strumento di pagamento, rispetto alle valute come Dollaro e Euro: è più scomodo da portare, soprattutto se si considerano tutti gli sviluppi finanziari (carte di credito, bonifici ecc.) con cui è possibile effettuare transazioni da casa, senza la necessità di incontrare la controparte. Nonostante questo però le persone continuano e continueranno sempre a comprare oro per vari motivi, come quello di diversificare il proprio portafoglio, proteggersi da crisi finanziarie, inflazione, ecc. Ritengo che per gli stessi motivi per cui la rivoluzione Fintech non ha impedito alle persone di continuare ad acquistare l'oro, lo sviluppo della tecnologia Ethereum, non impedirà a Bitcoin di continuare ad essere uno strumento interessante.

Si deve considerare che Ethereum non prevede un protocollo per il controllo della quantità di token prodotti. Viene perciò a mancare la caratteristica della scarsità tipica di Bitcoin. Potenzialmente la catena potrebbe, quindi, produrre un numero infinito di Ether, facendo sorgere delle preoccupazioni inflattive che, in realtà, sono attenuate dal fatto che il numero di Ether nel sistema devono essere proporzionali alla capacità della rete. Gli Ether sono lo strumento necessario sia per effettuare le transazioni, che per ripagare chi permette il funzionamento della rete (un po' come se fossero il carburante di questa). Quindi il numero di Ether può crescere solamente al crescere della capacità della blockchain e dei progetti che si realizzano sulla piattaforma.

Questo sistema fa sì che non ci siano né fenomeni di inflazione, né di iperinflazione, ma limita anche la crescita del valore delle singole cripto valute: col fatto che all'aumentare degli utenti, aumentino anche le valute in circolazione, viene limitato quel fenomeno di scarsità tipico di Bitcoin; in cui invece, al crescere degli utenti, la quota cresce in modo sempre minore, fino a fermarsi raggiunti i 21 milioni di Bitcoin totali.

Questo tipo di sistema, basato su una crescita della quantità di valuta, proporzionale rispetto al volume di iniziative e utenti che operano sulla piattaforma limita di molto i vantaggi di speculazioni legate al valore dei singoli Ether, consentendo quindi di avere dei valori più stabili. Anche se, secondo me, al momento l'Ether è ancora troppo volatile per definirla tale, ritengo che col tempo Ether potrebbe essere considerata una vera e propria moneta, grazie a questi meccanismi studiati per riuscire a far stabilizzare nel tempo l'asset, assumendo un andamento del valore simile a quello delle valute tradizionali.

Come acquistare e conservare Ether:

Anche con Ether, come per Bitcoin, è possibile acquistarli tramite Exchange in tre passaggi:

- registrazione alla piattaforma di scambio e apertura del proprio conto;
- deposito del denaro all'interno della piattaforma (euro, dollari, etc.);
- acquisto della valuta.

Anche per gli Ether vale un discorso analogo a quello fatto per Bitcoin sui modi per detenere la valuta:

- Strumenti a freddo più sicuri (perché meno soggetti ad attacchi hacker) e quindi indicati per le posizioni a lungo termine.
- Strumenti a caldo meno sicuri ma più pratici e quindi indicati per chi intende effettuare transazioni, o qualsiasi altro tipo di transazione nel breve termine.

Anche in questo caso è fortemente consigliata una diversificazione nel mantenimento degli Ether in base ai due criteri precedenti.

Andiamo ora ad approfondire il concetto di *wallet Ethereum*: sono delle applicazioni tramite cui si riesce a interagire con il proprio account Ethereum. È come se fosse un'applicazione bancaria (ci si può collegare ad applicazioni, si può controllare il saldo e si possono effettuare transazioni) senza la presenza di una banca.

Questo portafoglio è però solamente lo strumento per gestire Ethereum, ma non si ha alcun ausilio alla custodia dei fondi, che spetta all'utente: è come se fosse una finestra sull'account Ethereum. Il fornitore del portafoglio potrà essere cambiato in qualsiasi momento e senza limiti. È quindi lo strumento necessario a dimostrare la proprietà dell'asset.

Il portafoglio, ci consente inoltre di connetterci alle applicazioni decentralizzate utilizzando il proprio account Ethereum: un po' come se fosse il login valido per l'utilizzo delle varie app.

I portafogli cripto non vanno confusi con gli Exchange visto che non consentono di effettuare trading di cripto valute, ma semplicemente di effettuare transazioni. Ulteriore differenza sta nel fatto che mentre in questo caso le nostre valute stanno nel nostro portafoglio, nell'altro caso, stanno all'interno

di un portafoglio che è dell'*exchange* (un po'come se qualcun altro stesse tenendo il denaro per noi). I *wallet* sono definiti da due stringhe alfa numeriche che hanno funzioni diverse. Queste sono dette:

- Chiave pubblica: Ovvero l'indirizzo a cui vogliamo ricevere o inviare gli assets finanziari. Se lo volessimo paragonare ad una banca, sarebbe il nostro iban. Per effettuare pagamenti basterà ricevere la chiave pubblica del destinatario, mentre per riceverli basterà fornire la propria. È fondamentale però essere consapevoli che qualsiasi transazione effettuata sia irreversibile e quindi bisogna prestare particolare attenzione alla correttezza del destinatario.
- Chiave privata: è la password necessaria per accedere ai nostri fondi. Potrebbe essere quindi paragonata alla password che utilizziamo per l'accesso al nostro home banking. È come se fosse la chiave necessaria per aprire la parte di blockchain sui cui è registrato il fatto che noi abbiamo quei determinati fondi.

Nel caso in cui si dovesse perdere la Chiave privata, è comunque possibile ripristinarla attraverso il Feed che è un insieme di parole chiave che conviene scrivere e mantenere in un posto sicuro ed offline. È come se fosse una seconda chance per recuperare l'account, nel caso in cui qualcuno dovesse smarrire la password.

C'è una vasta gamma di portafogli cripto tra cui scegliere: alcuni che permettono di operare su alcune cripto valute, ad esempio, *Electrum* che permette di operare solamente con i Bitcoin, altri che permettono di gestirne altre.

Andremo ora a parlare dei maggiori portafogli che permettono di mantenere Ether, visto che ci serviranno in seguito per il nostro progetto sugli NFT:

- Exodus: è un portafoglio software gratuito risalente al 2016 che ha un Exchange integrato al proprio interno. È quindi un portafoglio multi-valuta che supporta entrambe le cripto da noi trattate, ma anche altre. È un *wallet* che può essere considerato sicuro, in cui ci si può registrare senza documenti (non bisogna dare alcun nostro dato) e le cui le chiavi sono criptate. Essendo però su computer o cellulare, è soggetto ai rischi *hacker* legati ad essi e quindi occorre prendere le giuste precauzioni. Il vantaggio di questo portafoglio consiste nel poter gestire transazioni, in diverse criptovalute, senza la necessità di aprire molteplici portafogli specializzati. È anche semplice da utilizzare, ma tutto ciò a prezzo di elevate commissioni. Dà anche la possibilità, in modo semplice, di fare *staking* di cripto valute, ovvero generare interessi passivi tramite il congelamento degli assets. Naturalmente, bisogna prestare particolare attenzione a questo tipo di attività in quanto, congelando degli asset variabili, ci si espone al rischio di svalutazione della moneta.
- Metamask: è un'estensione di Chrome che può essere utilizzato come *wallet* compatibile con tutte le cripto valute che si bassano sulla piattaforma Ethereum. Quindi non è compatibile

con Cardano, Solana o altre cripto, anche se ad alta capitalizzazione. Per effettuare da computer l'accesso a Metamask bisogna connettersi al sito https://metamask.io e registrarsi (importante prestare attenzione all'indirizzo per evitare problemi di phishing). Al momento della registrazione, sarà necessario memorizzare una *seed frase*, che è una stringa composta di 12 o 24 parole che viene utilizzata dai *wallet* per generare una serie di chiavi private. Quindi ricordandosi il *seed* si potranno avere automaticamente una serie di chiavi private e la chiave pubblica, quindi l'indirizzo.

- Metamask consente di essere utilizzato sia come *hot wallet*, che come *cold wallet*. È quindi funzionale sia all'inizio, quando si muovono piccole cifre, che nel futuro, in cui è sempre consigliato diversificare la ricchezza, detenendola anche in strumenti *hardware*, come ad esempio i Trezor o i Ledger. Nel caso in cui si deciderà di configurare l'account con un ulteriore *hot wallet*, si creeranno nuovi account: ognuno di questi avrà una chiave privata propria, ma sarà possibile accedere a tutti semplicemente ricordandosi la *seed frase* iniziale.
- Coinbase: è un Exchange di criptovalute che permette di acquistare entrambe le criptovalute approfondite nella tesi, ma anche molte altre. Fondato nel 2012, è al momento uno dei maggiori al mondo .Oltre alla funzione di acquisto e vendita di criptovalute consente anche di negoziare gli *stablecoin* e dispone di un *wallet* che permette di detenere le proprie criptovalute. Permette, inoltre, di accettare dei pagamenti in criptovaluta e può essere anche utilizzato come strumento per finanziare le proprie start up. Per effettuare l'accesso a *coinbase* è necessario fornire nome, cognome, email e password, questi dati rispettano però il regolamento di protezione dei dati dell'Unione Europea. Oltre all'Exchange, per acquistare cripto con *coinbase* occorre avere un wallet digitale. Si può decidere di utilizzare il portafoglio fornito gratuitamente dalla piattaforma stessa: senza ne costi di apertura, che di mantenimento, che di transazione. Le commissioni riguardano quindi la compravendita di criptovaluta, alla quale è applicato uno spread che si aggira intorno allo 0,5%. Oltre a questi costi ci sono quelli legati alle commissioni fisse (che variano in base all'importo della transazione) o variabili (variano in base a se i pagamenti effettuati sono standard, istantanei o bancari).

Dopo aver menzionato alcuni dei principali *wallet* ed Exchange, si andrà ad affrontare l'argomento NFT in modo teorico, per poi procedere con la scelta e l'apertura di un wallet che permetta di operare sulla piattaforma Ethereum.

6. NFT (non-fungible token)

Wikipedia definisce gli NFT come:

"Gli NFT (non-fungible token) è un tipo speciale di token che rappresentano l'atto di proprietà ed il certificato di autenticità, scritto su catena di blocchi, di un bene unico (digitale o fisico); i gettoni non fungibili sono quindi reciprocamente intercambiabili; ciò è in contrasto con le cripto valute, come Bitcoin, e molti gettoni di rete o di utilità, che sono per loro stessa natura fungibili."

La nascita degli NFT risale al 2014, quando in occasione della quinta conferenza del Seven on Seven (evento in cui si riuniscono i massimi esponenti dell'arte, con i massimi esponenti dell'informatica) si incontrano l'imprenditore informatico Anil Dash e l'artista Kevin McCoy. I due vengono abbinati per un progetto, che iniziano con l'obiettivo di risolvere insieme alcune delle criticità dovute al fatto che, a causa della non fisicità, l'arte digitale sia spesso considerata senza valore, rendendo così molto complicata la monetizzazione di essa. I due capiscono che tramite la tecnologia blockchain, sarebbe stato possibile riuscire a certificare l'unicità, la limitatezza e la proprietà delle opere d'arte, consentendo così agli artisti di attribuire un valore alle proprie opere. Quindi si dà la possibilità al proprietario di un immagine di dimostrarne la proprietà e la scarsità, tramite hash depositati sulla blockchain. L'artista, inoltre, è in grado di autenticare la propria opera d'arte. L'insieme di queste caratteristiche rende quindi possibile la creazione di un mercato sull'arte digitale in cui le opere hanno finalmente un valore che può essere provato. In quell'occasione venne sviluppata una demo in grado di mettere in pratica quanto detto sopra: fu creata una gif animata, che fu venduta per quattro dollari. È così che nacque il primo NFT. Nascono quindi in stretta correlazione con il mondo dell'arte e rimangono confinati a quel mondo per diversi anni, fino a quando, nel 2020, questa tecnologia è uscita dalla ristretta cerchia dei collezionisti di criptovalute. Si è così passati alla creazione di carte digitali e gattini animati a collaborazioni con marchi importanti tra cui la Marvel o l'NBA. Ci sono molti luoghi comuni legati a questo mondo. Ad esempio c'è chi ritiene che sia una truffa, ignorando tutti i possibili utilizzi alternativi all'arte e asserendo che non abbia senso acquistare per cifre astronomiche (alcuni NFT sono venduti per decine di milioni) semplici immagini che si potrebbe avere copiando l'immagine da internet. Sicuramente è un mercato in bolla, in cui la maggior parte degli utenti non sono degli appassionati di arte. Infatti, è innegabile che sia un mercato ad altissima speculazione ed in cui è molto semplice gonfiare le quotazioni delle opere d'arte.

È noto che nell'arte, come in molti altri settori dell'economia, il prezzo sia dato dall'incontro tra domanda e offerta. Nel caso degli NFT, è possibile che un artista riesca a creare una bolla, in modo autonomo, attorno alle proprie opere d'arte. Per far ciò è sufficiente che l'artista compri le proprie opere d'arte a prezzi elevati: dopo diversi acquisti, i potenziali clienti potrebbero credere che quello sia il vero valore degli NFT e saranno disposti a comprare l'opera digitale a prezzi elevati, credendo di star facendo un

affare. Questa tecnica è molto diffusa e ha coinvolto anche personaggi molto noti. Melania Trump, ad esempio, aveva creato la sua prima propria opera d'arte digitale, ed era riuscita a venderla per 185 mila dollari, partendo da un prezzo di partenza di 175 mila. Sfortunatamente per lei però, nel mondo degli NFT, ogni transazione è registrata in un registro pubblico, che ha permesso di scoprire che l'acquirente del suo primo NFT fosse lei stessa. È stato possibile capirlo visto che il profilo di Melania, ha trasferito del denaro ad un conto, che a sua volta lo ha trasferito al conto che ha effettuato l'acquisto. Di comportamenti simili ce ne sono moltissimi e non è sempre facile smascherarli: se ad esempio Melania avesse inviato i fondi al conto che ha effettuato l'offerta, partendo da un portafoglio diverso da quello con cui ha messo in vendita l'NFT, sarebbe stato molto più complesso capire il trucco. Comportamenti simili sono molto diffusi anche con l'arte tradizionale, in cui soci acquistano i quadri dell'artista per alzare le quotazioni, ma è importante essere consapevoli che questo avvenga anche negli NFT; inoltre pensare al fatto che addirittura l'ex first lady sia coinvolta in tali operazioni, rende un idea di quanto effettivamente questo mercato sia in bolla.

Bisogna quindi essere molto cauti quando si acquistano NFT, ma questo non vuol dire che non ci siano anche artisti digitali validi, che stiano lì per passione e che vendano opere di qualità e che effettivamente possano trasmettere emozioni a chi le acquista, in grado di giustificare anche prezzi elevati. Tornando al discorso di chi dice che le opere d'arte digitale non abbiano senso, "siccome alla fine l'immagine la posso avere gratis scaricandola da internet ed è uguale", gli si può dare ragione solamente nel caso in cui ritengono inutile anche comprare quadri originali visto che "che senso ha comprare un quadro di Vincent van Gogh originale quando si può acquistare, per molto meno una copia di un altro artista. Il motivo per cui si decide di comprare un quadro originale, virtuale o materiale che sia, non è solamente quello di poterlo ammirare, ma è soprattutto quello di avere la soddisfazione di detenere l'originale o per motivi di investimento. E dire che acquistare NFT non ha senso visto che si può "acquistare una schermata", è un'affermazione che può essere tranquillamente paragonata al dire "non acquisto quadri originali visto che posso avere le copie". Naturalmente c'è chi non acquista nessuno dei due tipi di quadri perché preferisce utilizzare denaro per altro o perché non è interessato all'arte, e sicuramente questa è una visione più coerente rispetto all'altra.

Il mercato è in bolla ed è possibile osservare come molte quotazioni si stiano già ridimensionando, tuttavia, quando questa bolla sarà esplosa, emergeranno gli artisti che veramente hanno talento, e le opere che potrebbero effettivamente suscitare interesse. Molti sono rimasti impressionati dal fatto che Jack Dorsey, il fondatore di Twitter, abbia venduto, per 2,5 milioni di dollari, il primo Tweet, da lui fatto, di sempre. Sicuramente sono cifre alte, e i benefici risultano difficili da notare, però sicuramente il poter dire di possedere qualcosa di così unico e raro potrebbe essere motivo di orgoglio dei super ricchi, che sia hanno piacere di ostentare, che di possedere un qualcosa di così unico, che magari semplicemente di diversificare i propri investimenti.

Per quanto riguarda gli investimenti e le speculazioni, è inoltre importante sapere che è possibile vendere l'NFT mantenendo una quota di proprietà su esso. Questo può consentire a degli artisti di continuare a ricevere delle percentuali (variabili a seconda della quota che si vuole detenere e del valore delle transazioni future inerenti al token) anche dopo aver venduto l'NFT. In questo modo si potrà continuare a guadagnare nel tempo con la stessa opera d'arte.

Tramite gli NFT è inoltre possibile collezionare oggetti prima impossibili da collezionare; basti pensare al fatto che si possono acquistare NFT di canzoni: questi non danno però alcun diritto (ad esempio sfruttamenti commerciali o copyright) e quindi possono essere paragonati a dei cd autografati (solo che in questo caso sia la canzone che il cd sono autografati in modo digitale).

Al giorno d'oggi gli NFT possono essere utilizzati per molti scopi, anche esterni all'arte: possono perciò essere visti come dei contratti che garantiscono a chi possiede dei diritti, dovuti al fatto che possono dimostrare di essere gli unici possessore di un determinato NFT e di tutti i contratti ad esso collegati.

Facciamo un esempio di NFT esterno al mondo dell'arte: quando si acquista un abbonamento annuale in palestra, questo è nominale. Fin quando vorremo andare in palestra quindi sarà possibile per noi farlo, ma nel caso in cui ci dovessimo stancare, a metà anno di andarci, avremmo sprecato tutti i nostri soldi per la parte in cui non lo utilizziamo. Tramite NFT sarebbe possibile effettuare un contratto non nominale, e quindi la persona che decide di interrompere il proprio percorso in palestra, potrebbe vendere il proprio NFT che gli attribuisce il dritto di entrarci. Questo diritto sarà venduto probabilmente al di sotto del prezzo dell'anno intero, visto che il tempo residuo rimasto sarà minore rispetto a quando il contratto è stato stipulato, ma non è detto; potrebbe infatti addirittura essere venduto a un prezzo uguale o maggiore rispetto a quello di acquisto nel caso in cui, ad esempio, la palestra fosse stata ammodernata e i prezzi si siano alzati.

Un altro esempio di utilizzo potrebbe essere quello di un cantante che, invece di far acquistare i biglietti per il proprio concerto, dice che sta organizzando un concerto gratuito solo per i propri fan. Potrebbe però chiedere ai fan, per partecipare, di esibire il proprio NFT creato dall'artista. In questo modo si riuscirebbe a sostituire il biglietto tradizionale con un NFT. In vantaggio al momento più evidente, sarebbe sicuramente quello fiscale, essendo la regolamentazione a riguardo ancora acerba.

Gli NFT hanno trovato un applicazione anche nei videogiochi, ad esempio sotto la forma degli NFT videoludici, ovvero di oggetti digitali che si possono acquistare all'interno del videogioco: basti pensare a dei cappellini, dei vestiti, delle armi speciali o addirittura case e terreni. In questo caso si potrebbe creare un mercato, all'interno dei videogiochi, in cui gli utenti possono acquistare e vendere questi assets di gioco. Grazie alla scarsità, infatti, si può addirittura riuscire a creare dei modelli di gioco in cui le persone, giocando, collezionando e scambiando questi oggetti virtuali, riescano a creare ricchezza. Il mercato interno al mondo dei videogiochi c'è sempre stato, visto che anche senza la tecnologia

Blockchain è possibile mettere in vendita degli oggetti speciali all'interno del gioco. La differenza risiede però nel fatto che, utilizzando la tecnologia blockchain, sarebbe possibile, per i giocatori, vendere i propri assets direttamente all'interno della piattaforma Ethereum, rendendo così molto semplice la conversione in valuta legale. In questo modo si renderebbe più fattibile lo sviluppo di giochi in cui più si gioca e più si guadagna; ad esempio nel caso in cui si allena un determinato giocatore lo si rende forte, sarà poi possibile venderlo direttamente su piattaforma Ethereum: è quindi la facilitazione dell'incontro tra domanda e offerta di asset del gioco, unita alla facile conversione in valuta corrente che potrebbe portare i giocatori a non giocare più perché spinti solamente dalla competizione e voglia di divertirsi, ma anche da un potenziale guadagno.

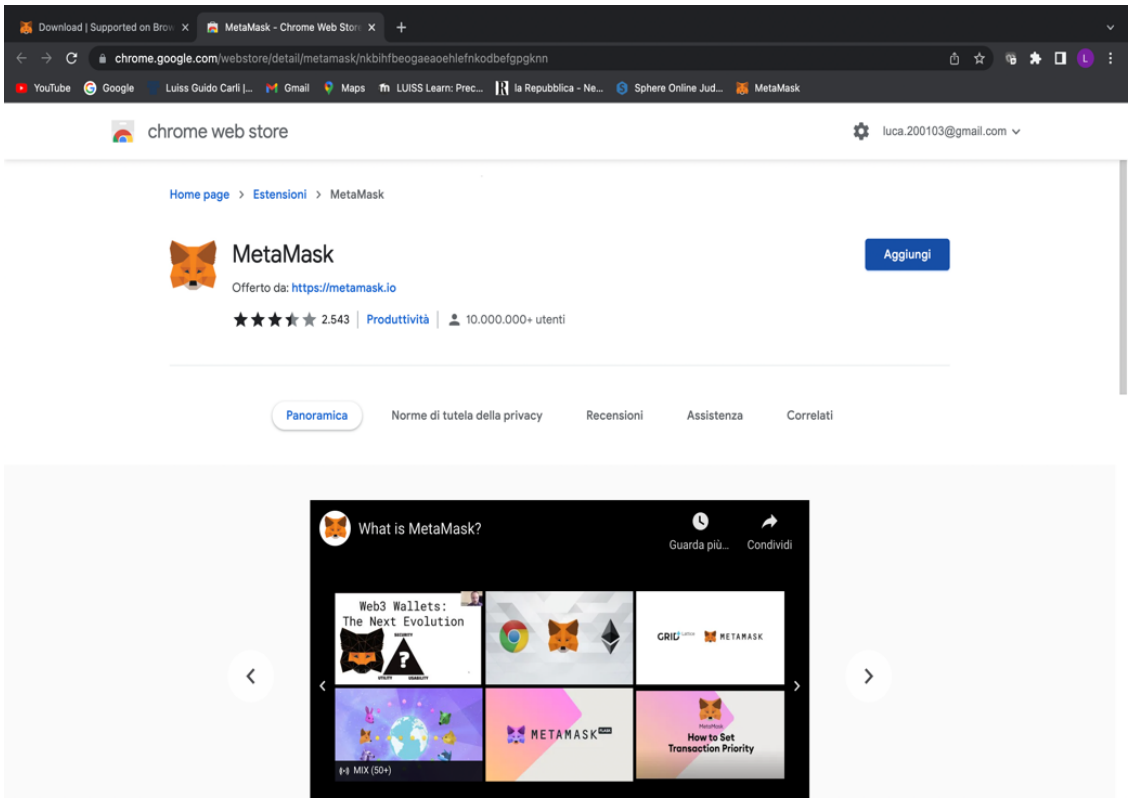
7. Un caso pratico: creazione e vendita di un NFT.

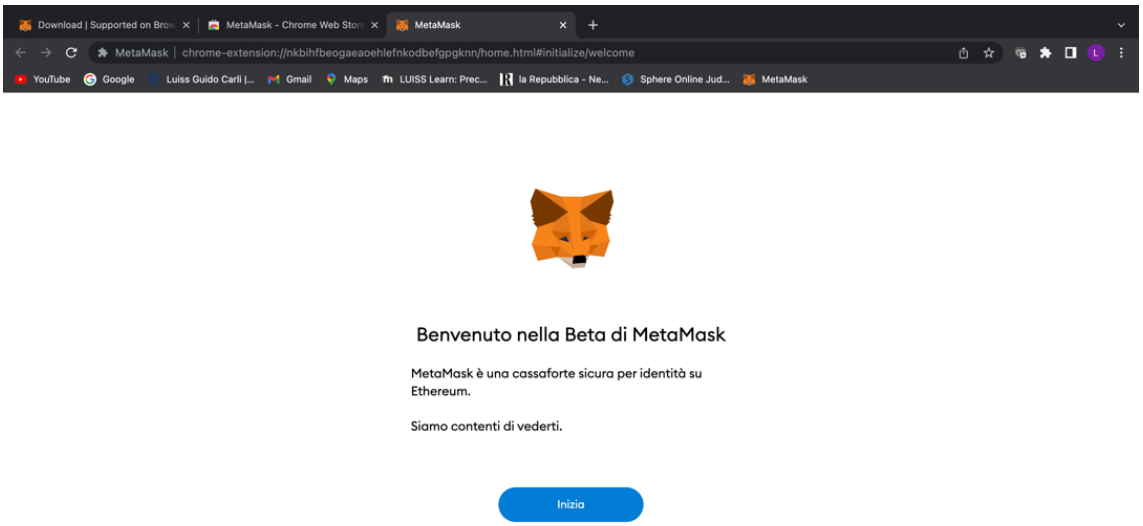
Dopo aver visto nel dettaglio la tecnologia Blockchain, abbiamo spiegato la tecnologia su cui si basa la piattaforma Bitcoin e quella di Ethereum. Abbiamo visto come tutelarsi dai possibili problemi legati all'operare con queste tecnologie. Dopo aver visto nella teoria il funzionamento di queste tecnologie, ora passeremo alla pratica, aprendo un Wallet Ethereum che ci servirà per la creazione e la vendita di un NFT.

Dovendo movimentare piccole cifre di Ether, utilizzeremo Metamask: questo consente sia di detenere il denaro su hot wallet che su cold wallet. In un primo momento, caricheremo piccole somme di Ether sul portafoglio e quindi sarà sufficiente utilizzare il portafoglio in modalità online, se poi le cifre da noi detenute sul wallet, andranno ad aumentare, sarà opportuno, per la nostra sicurezza, diversificare il denaro aprendo anche un cold wallet, tramite strumenti come Trezor o Ladger.

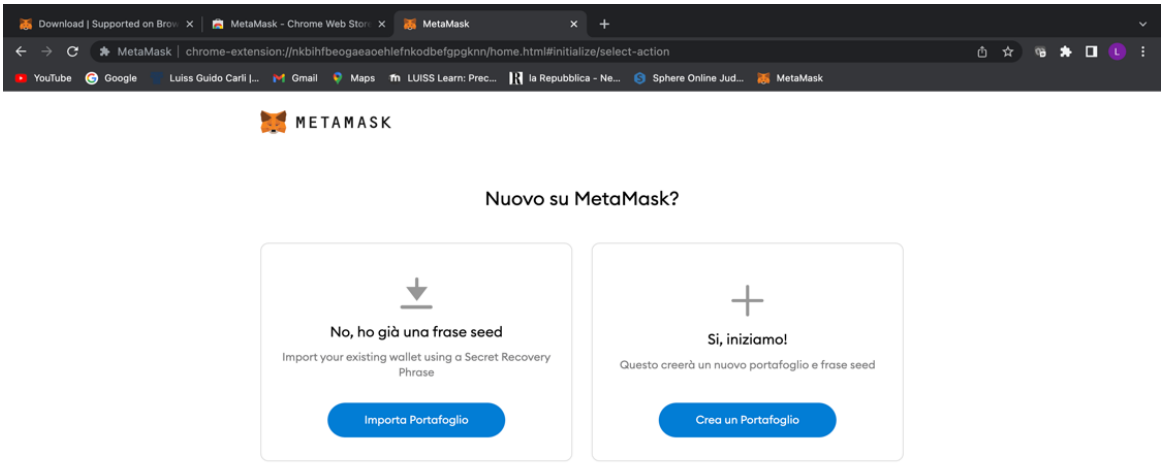
Il dispositivo su cui operiamo è un Mac book e quindi la prima cosa da fare sarà quella di installare il Google Crome, necessario per utilizzare Metamask.

Si dovrà installare anche l'estensione del browser Chrome di Metamask, tramite il sito Metamask.io (occorre prestare molta attenzione che sia il sito corretto, per evitare di incappare in truffe).

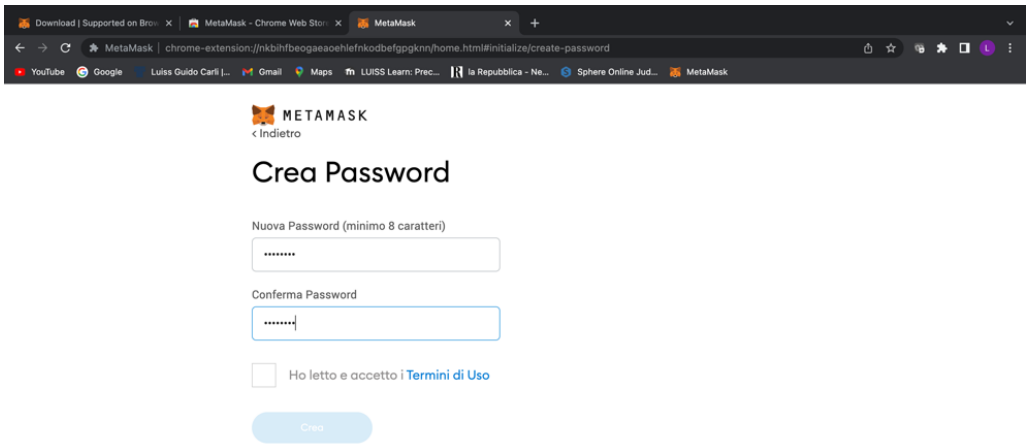




Una volta scaricata l'estensione, sarà necessario registrarsi; procederemo quindi con l'opzione di destra.



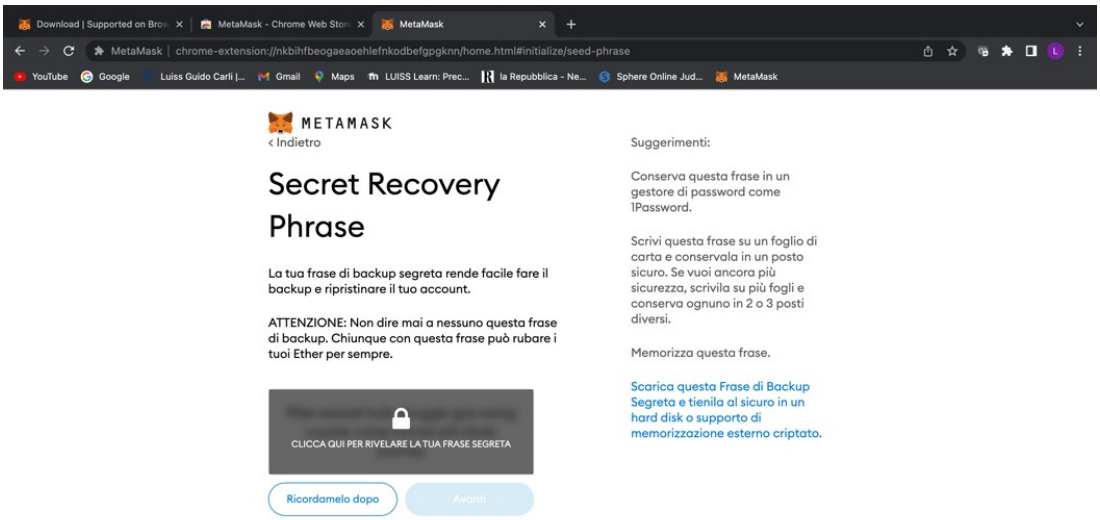
A questo punto dovremo stabilire una password, di almeno 8 caratteri, per il nostro wallet; dopo aver letto i termini d'uso, li confermeremo.



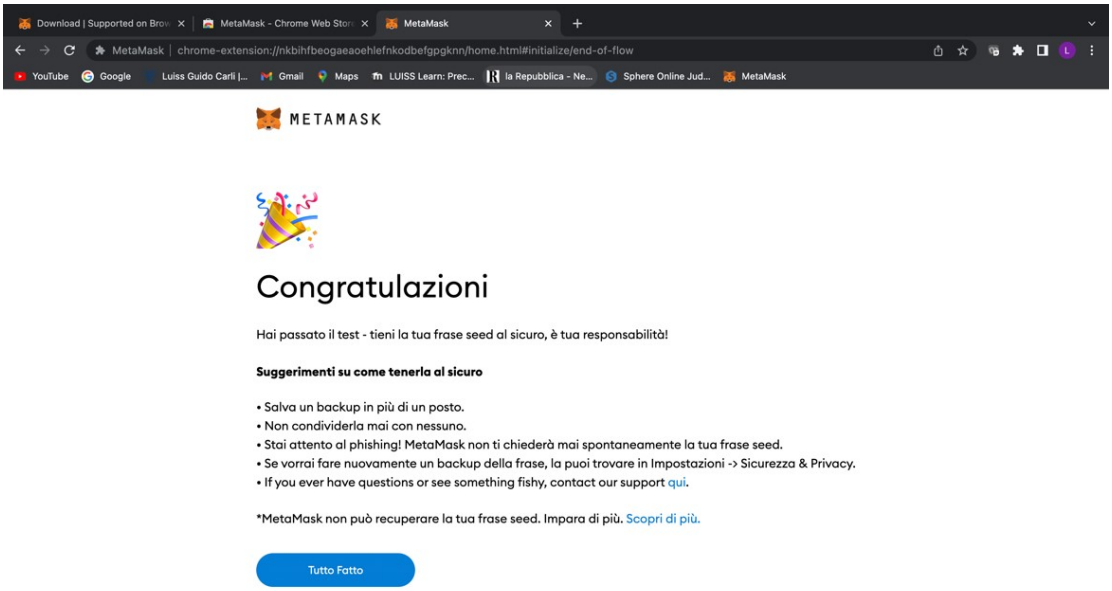
A questo punto vedremo un video di durata di poco più di un minuto e trenta in cui viene spiegata cosa è la *seed frase*; avendola già trattata in precedenza, sappiamo già molto a riguardo. Dopo aver visto il video, ci verrà fornita la nostra *seed frase* (composta di 12 parole), potremmo vederla cliccando nell'apposita area. Una volta vista la *seed frase*, sarà necessario memorizzarla e appuntarsela da qualche parte. A tal proposito ci sono moltissimi modi diversi per farlo: il classico pezzetto di carta in cassaforte (anche se potrebbe presentare problemi come lo sbiadimento o di furto); registrarlo sul proprio computer (anche se anche questo potrebbe rompersi ed è comunque esposto al rischio di essere hackerato); acquistare delle tavolette di alluminio su cui incidere i dati da ricordare, evitando che possano deteriorarsi come un foglio di carta, da detenere in casa o in banca (anche qui col rischio di furto) ecc.

È importante infatti ricordare che tramite il *seed* è possibile reimpostare la password e che quindi se dovesse andare nelle mani di un male intenzionato perderemmo tutto. È molto più importante il seed che la password visto che per accedere tramite la password è necessario connettersi dal proprio dispositivo, mentre con la *seed frase* è possibile accedere anche tramite altri dispositivi.

Le alternative sono molte e queste dipendono dalle preferenze della persona: ciò che conta realmente è il ricordarsi la frase e conservarla in un posto sicuro.

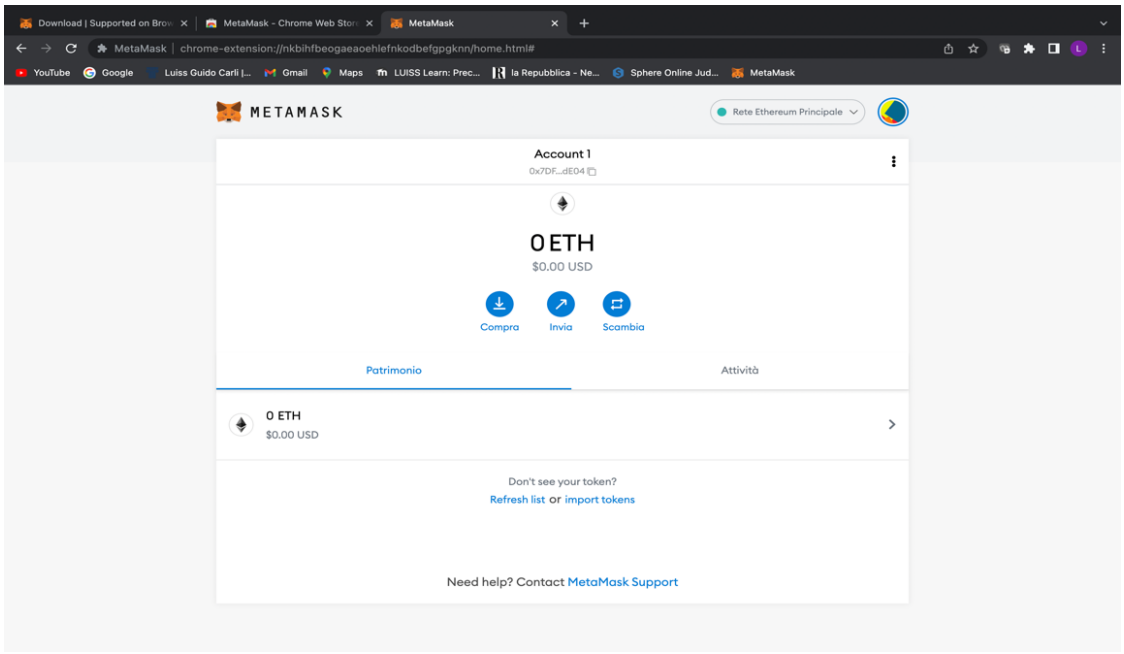


A questo punto verrà chiesta una conferma per vedere se effettivamente la *seed frase* è stata memorizzata correttamente e successivamente avremo questa schermata, in cui verranno fatte ulteriori raccomandazioni per un corretto funzionamento della piattaforma.

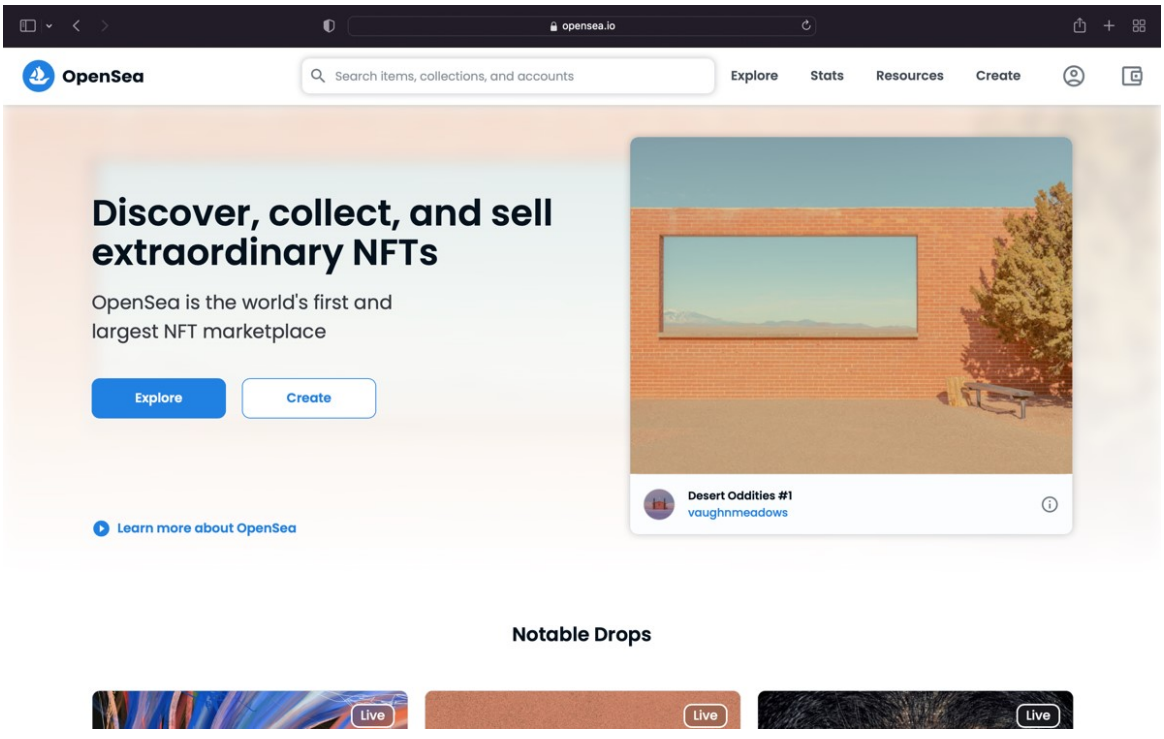


Successivamente, si entrerà finalmente all'interno dell'applicazione e saremo connessi sulla rete Ethereum principale. Inizialmente si avrà un solo account legato al *seed*, ma cliccando sul pallino in altro a destra, si potranno creare una moltitudine di account, che portano a indirizzi diversi. È anche possibile connettere degli Hardware Wallet ed il che è fondamentale da un punto di vista di sicurezza: la transazione per partire ha sia bisogno della conferma su Metamask, che sul Ledger. Al momento non

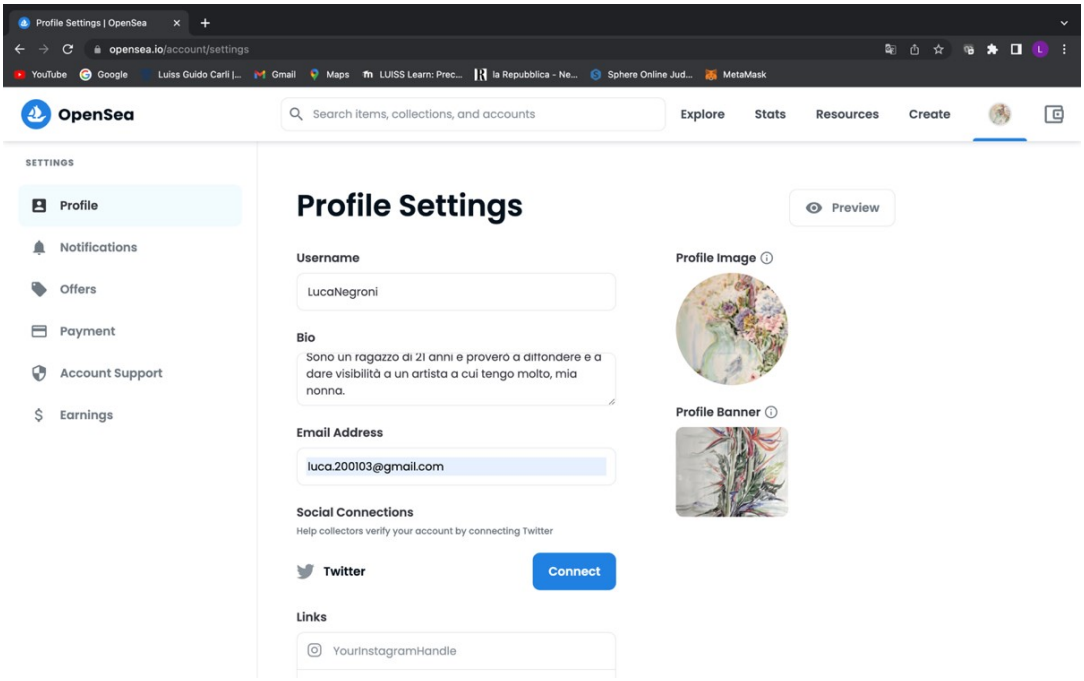
si ritiene necessario l'acquisto di un Ledger, date le moderate somme che andremo a movimentare inizialmente, ma nel caso in cui queste aumentino, sarà necessario acquistarlo e connetterlo al portafoglio.



Ora si tratterà di Open Sea: il *market place* di riferimento per gli NFT. Per accedere al sito bisogna accedere al sito https://opensea.io , tramite cui si potranno sia vedere gli NFT già esistenti, che crearne uno proprio. In particolare si tratterà della creazione di un NFT. Per fare ciò andremo inizialmente a collegare il wallet Metamask creato in precedenza.

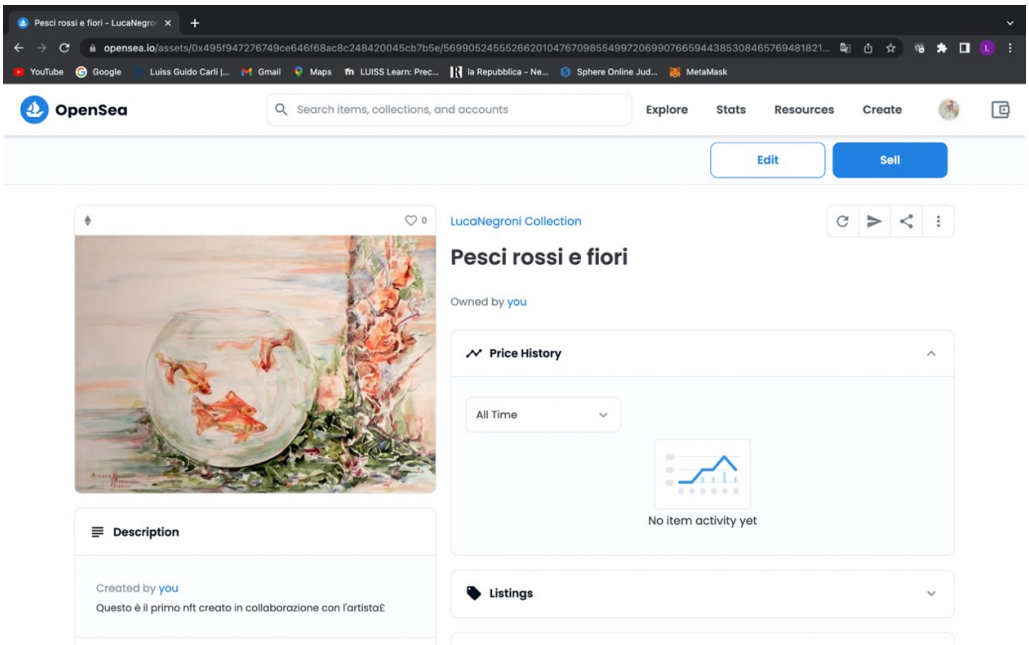


A questo punto, creato il profilo, si andrà a personalizzare tramite le impostazioni



Si procede con la creazione dell'NFT. Per fare ciò sarà necessario andare sulla sezione "create", bisognerà poi selezionare l'opera d'arte, dargli un titolo e aggiungere una descrizione. Nella sezione "Unlockable content", sarà inoltre possibile scegliere se dare un premio a chi sceglie di acquistare l'NFT: può essere utilizzato per dare un codice d'accesso (ad esempio a una lezione online) oppure per dare in link (ad esempio per poter avere una foto più qualitativa del nostro collezionabile).

Al termine di questo processo non bisognerà pagare nulla, visto che i costi della piattaforma andranno affrontati al momento della messa in vendita.

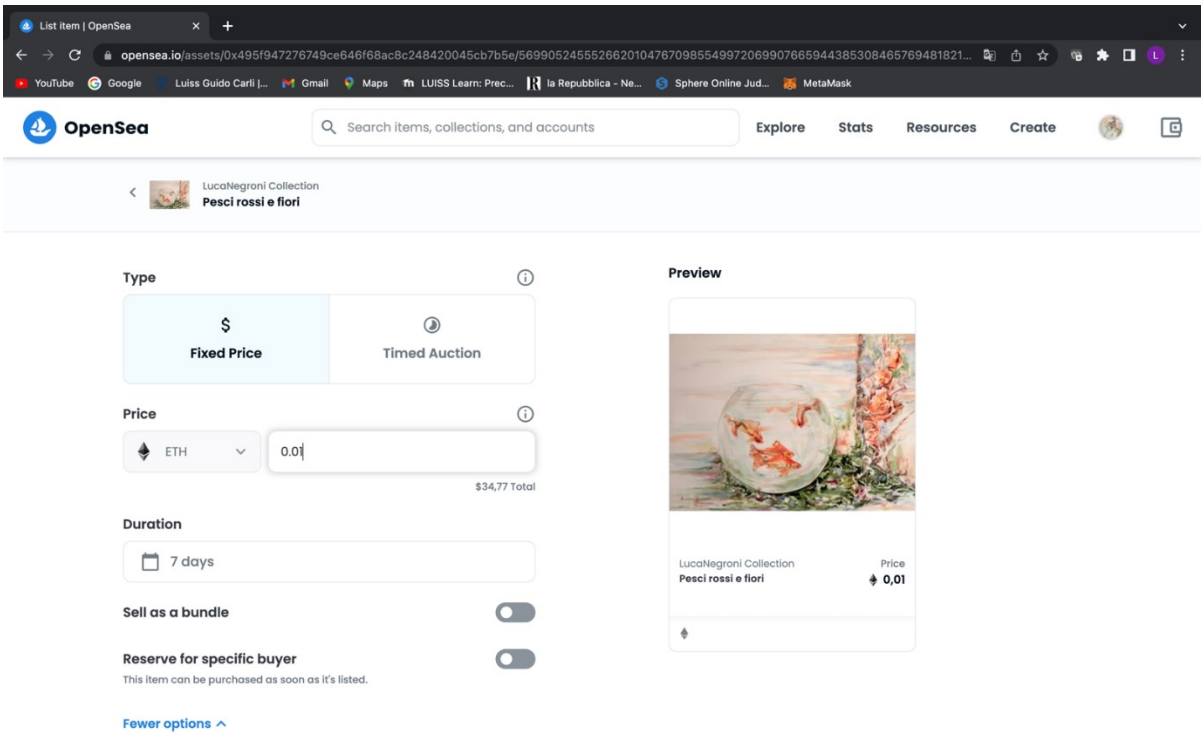


Bisognerà infine procedere con la vendita, fissando il prezzo (ed un eventuale prezzo minimo di riserva, e di rialzo) e la durata. Open Sea consente anche la vendita dell'NFT tramite asta, in cui si potrà scegliere il numero di domande che si potranno effettuare in un determinato periodo di tempo. C'è anche l'opzione "acquista subito", con cui si darà la possibilità ai compratori di saltare il processo di aste, comprando l'NFT subito al prezzo da noi indicato.

Terminato con il processo di vendita, bisognerà pagare le commissioni. Queste variano a seconda della velocità con cui si vuole mettere in vendita il token ed in base a quanto è utilizzata la rete Ethereum in quel momento. Conviene, nel caso in cui non ci sia fretta nel vendere il token, aspettare il momento in cui la rete sia meno congestionata, per poter risparmiare sulle commissioni.

Inoltre *OpenSea* consente di creare NFT senza alcuna commissione iniziale. Questa procedura è detta "Lazy Minting" e consente di trasferire l'NFT sulla catena solamente una volta che il trasferimento sia avvenuto. In questo modo sarà possibile scaricare il costo delle *fee* direttamente sul compratore.

Bisogna tuttavia tenere presente che su *OpenSea*, nel caso in cui si stia caricando il primo annuncio, non sarà possibile effettuare questa operazione, e bisognerà pagare necessariamente le tariffe delle commissioni associate all'inizializzazione dell'account.



8. Conclusioni

Partendo dalle innovazioni derivate dall'applicazione della tecnologia alla finanza, si è parlato di come queste abbiano influenzato il sistema bancario, creando un sistema altamente competitivo, che ha portato alla creazione di nuovi strumenti finanziari, ma soprattutto ha consentito agli utenti di accedere ai servizi già esistenti in modo più semplice, economico ed in maniera autonoma.

Sempre più persone preferiscono le "fintech" rispetto alla banca tradizionale che, in realtà, viene completamente disintermediata. Abbiamo, in particolare, approfondito il concetto di "crowdfunding", tramite cui è possibile raccogliere contributi finanziari erogati direttamente da persone, senza la necessità di intermediazione. Ciò è possibile attraverso innovazioni che hanno permesso, tramite la diffusione capillare del *web* e delle relative applicazioni, di raggiungere platee di persone in modo semplice ed efficace.

La tesi si è evoluta spiegando come questo desiderio di disintermediazione abbia portato al voler creare un sistema monetario decentralizzato: abbiamo quindi parlato della Blockchain e delle due criptovalute a più alta capitalizzazione, basate su questa tecnologia. Ci si è concentrati maggiormente sul funzionamento, piuttosto che sull'ambito prettamente speculativo di queste, per permettere al lettore di farsi un'idea personale sullo strumento che sta acquistando, senza doversi basare esclusivamente su opinioni o pareri esterni

Questo è stato infatti uno dei motivi per cui si è deciso di scrivere la tesi. Le criptovalute sono ormai da anni un argomento sulla bocca di tutti e chiunque, sia persone qualificate e competenti che non, hanno opinioni contrastanti tra loro. Nella tesi si è ad esempio trattato di figure di spicco come Warren Buffet, che dichiarano di voler questi strumenti sono nel caso in cui gli vengano regalati o Elon Musk che, invece, è un forte sostenitore di questi.

Nella parte finale della tesi si è inoltre descritto lo strumento degli *NFT*, anch'esso molto controverso e complesso; come in molte innovazioni, si ha una forte euforia iniziale, che può portare a delle bolle speculative, che, esplodendo, possono lasciare spiazzati gli investitori. A tal proposito, si sono illustrate le varie funzioni di questi, spiegandone sia i punti favorevoli che le criticità. Si è anche voluto approfondire, come, nell'applicazione artistica di questi, ci siano moltissime manipolazioni del mercato, anche da parte di personaggi di rilievo. Si sono fatti degli esempi concreti al riguardo, spiegando come sia possibile e semplice gonfiare i prezzi delle opere d'arte.

Lo scopo di tutta la tesi, che si è conclusa con la creazione di un profilo su Opensea, è quello di far ragionare il lettore sul fatto che il mondo Blockchain è molto complesso, e che dietro questa complessità si celano sia grandi opportunità, che grandi rischi. Prima di investirci, pertanto, è opportuno comprendere il funzionamento della Blockchain, delle criptovalute e degli strumenti che si

basano su di essa. È proprio la conoscenza approfondita degli strumenti che si stanno acquistando, che distingue un investitore da uno scommettitore.

9. Bibliografia e sitografia

Bibliografia

- Davide Bulgarelli, Enrico Malverti, Gabriele Villa, *Fintech. La finanza digitale. Strategia di investimento con i roboadvisor,* Hopeli, 2018
- Raffaele Bianchi, Gianluca Chiap, Jacopo Ranalli, *Blockchain, Tecnologia e applicazioni per il business,* Hopeli, 2019
- Davide Capoti, Alessandro De Lorenzo, Matteo Maggioni, *Tutto su Bitcoin, Guida pratica per investire in criptovalute,* Hopeli, 2018

Sitografia

Fintech

- Patrizia Licata - "Fintech, le banche italiane mettono sul piatto 530 milioni per il biennio 2021-2022" - Marzo 2021 - https://www.corrierecomunicazioni.it/finance/fintech-le-banche-italiane-mettono-sul-piatto-530-milioni-per-il-biennio-2021-2022/amp/

- Wikipedia - accesso 31 Maggio - "Tecnofinanza" - https://it.m.wikipedia.org/wiki/Tecnofinanza

- Eleonora Truzzi, "Fintech: cos'è e quali vantaggi riserva" - Settembre 2021 - https://www.obiettivoprofitto.it/fintech-vantaggi/

Pagamenti digitali fintech

- Ivano Asaro - "Pagamenti digitali, cosa sono e quali sono" - Ottobre 2021 - https://blog.osservatori.net/it_it/pagamenti-digitali-guida#definizione

Fintech e sistemi di raccolta dei capitali

- Banca d'Italia - "Indagine Fintech nel sistema finanziario italiano" - Novembre 2021 - https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2021/2021-FINTECH-INDAGINE.pdf
- Morya Longo - "Capitali e strumenti alternativi: finanza e fintech per le Pmi" - Aprile 2020 - https://amp24.ilsole24ore.com/pagina/ADdWCCK

- Giulia Serafin - “Fintech: tra piattaforme di crowdfunding, valute virtuali e contrasto del riciclaggio” - Giugno 2019 - https://edizionicafoscari.unive.it/media/pdf/article/ricerche-giuridiche/2019/1/art-10.14277-Rg-2281-6100-2019-01-006_aZgU8uw.pdf

Fintech e financial security

- Banca d’Italia - “Le iniziative regolamentari per il Fintech: a che punto siamo?” - Maggio 2021 - https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2021/PERRAZZELLI-4-maggio-2021.pdf
- Marcello Condemi - “ Nuove Tecnologie e attività finanziarie, spunti per un rinnovato approccio regolamentare” - Gennaio 2021 - https://www.dirittobancario.it/art/nuove-tecnologie-ed-attivita-finanziarie-spunti-un-rinnovato-approccio-regolamentare/

Machine learning

- Sas institute – “Machine Learning, cos’è e perché è importante” - Maggio 2022 - https://www.sas.com/it_it/insights/analytics/machine-learning.html#machine-learning-importance
- Ferry - “ Cos’è il machine learning?” - Gennaio 2020 - https://youtu.be/WTt51-5K3L8

Defi

- Marcello Minenna - “DeFi: come funziona la finanza prêt-à-porter basata sulla blockchain” - Gennaio 2022 - https://amp24.ilsole24ore.com/pagina/AEJ3rj9

Blockchain

- Te lo spiego - “Che cos’è e come funziona una blockchain” - Aprile 2021 - https://youtu.be/sX25z_-zMgI
- Eugenio Spagnuolo - “7 applicazioni per la Blockchain oltre Bitcoin” - 15 Marzo 2019 - https://www.wired.it/economia/finanza/2019/03/15/blockchain-applicazioni/amp
- Davide Giribaldi - “Blockchain, a volte è solo moda: ecco i problemi applicativi” - Aprile 2019 - https://www.agendadigitale.eu/documenti/blockchain-a-volte-e-solo-moda-ecco-i-problemi-applicativi/

Mining

- Tiziano Tridico - “Cos’è il Mining?” - Luglio 2018 - https://youtu.be/GQ_9QKKTh8I

Bitcoin

- Riccardo Santili - “Il movimento Cyperpunk”: le origini delle criptovalute” - Luglio 2017 - https://www.iusinitinere.it/il-movimento-cypherpunk-le-origini-delle-criptovalute-23475/amp#
- Coinbase - “Che cos’è l’Halving dei bitcoin?” - Gennaio 2022 - https://www.coinbase.com/it/learn/crypto-basics/what-is-a-bitcoin-halving
- Bitcoin People - “Che cos’è l’Halving di bitcoin?” - Aprile 2021 - https://www.bitcoinpeople.it/halving-bitcoin/
- Bit 2 me Academy -“Come conoscere il valore di una transazione Bitcoin?” - Novembre 2021 - https://academy.bit2me.com/it/come-conoscere-la-commissione-di-una-transazione-bitcoin/
- Consob - “Le Criptovalute” – Maggio 2022 - https://www.consob.it/web/investor-education/criptovalute
- Vittorio Carlini - “Bitcoin, ecco perché non è una vera moneta. Il vero valore? La blockchain” - Gennaio 2018 - https://amp24.ilsole24ore.com/pagina/AEYilviD
- Forbes - “Chi sono gli 11 miliardari che hanno fatto la fortuna grazie al Boom dei Bitcoin” - Febbraio 2021 - https://forbes.it/2021/02/03/bitcoin-11-miliardari-fatto-fortuna-grazie-boom-2020/
- Emanuele Pagliari - “Cos’è un attacco al 51%e cosa causa l’hashrate di una blockchain” - Settembre 2019 - https://cryptonomist.ch/2019/09/14/attacco-51-hashrate-blockchain/?amp=1
- Pietrangelo Soldavini - “Blockchain, questa sconosciuta, a cosa serve?” - Luglio 2018 - https://amp24.ilsole24ore.com/pagina/AEYnTnEF
- Cryptotag - “Come conservare le criptovalute in modo sicuro nel 2020” - Novembre 2020 - https://it.cryptonews.com/guides/how-to-store-cryptocurrency-safely.htm

Ethereum

- Wikipedia - “Ethereum” - data di accesso: maggio 2022 - https://it.m.wikipedia.org/wiki/Ethereum
- Wikipedia – “Web 3.0” - Data di accesso: maggio 2022 - https://it.m.wikipedia.org/wiki/Web_3.0

- Mauro Cappelli - “macchina di Turing” - 2008 - Data di accesso: maggio 2022 https://www.treccani.it/enciclopedia/macchina-di-turing_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/
- QuiFinanza - “Cosa sono gli Ether e quanto valgono” - https://quifinanza.it/innovazione/ether-cosa-sono-come-funzionano/502181/amp/
- Mauro Bellini - “Ethereum, cos’è, come nasce, come funziona, ambiti applicativi, prezzi, grafici Eth aggiornati in tempo reale” - Maggio 2022 - https://www.blockchain4innovation.it/criptovalute/andamento/cose-quali-gli-ambiti-applicativi-ethereum/
- Ethereum Fondation - “Informazioni sulla Ethereum Foundation” - Maggio 2022 - https://ethereum.org/it/foundation/
- Giacomo Barbieri -“Il Trilemma Blockchain ci spiega perché Bitcoin ha un futuro assicurato” - Luglio 2021 - https://www.italian.tech/2021/07/05/news/bitcoin_e_il_trilemma_blockchain-307521114/
- Borsainside - “Ethereum supererà Bitcoin? 3 ragioni per cui performance ETH batte BTC” - Dicembre 2021 - https://www.borsainside.com/criptovalute/76307-prezzo-ethereum-superera-bitcoin-previsioni/
- Castero - “Ethereum limiti nel Mining e capitalizzazione massima” - Settembre 2021 - https://ethereum-news.it/ethereum-limiti-nel-mining-e-capitalizzazione/
- Autori vari - “La chiave per il tuo futuro digitale” - maggio 2022 - https://ethereum.org/it/wallets/
- Autori vari - ”Metamask wallet, cos’è, come funziona? Affidabile? Guida e opinioni” - Marzo 2022 - https://www.lecriptovalute.org/metamask-come-funziona-opinioni/
- The cripto gateway - “Metamask: tutorial definitivo” - Settembre 2022 - https://youtu.be/cscPvbK6C1U

Crowdfunding

- Wikipedia - “Crowdfunding - Accesso: 31 maggio 2022” - https://it.m.wikipedia.org/wiki/Crowdfunding
- Marco Montemagno - “Come raccogliere in Crowdfunding 1,2 mln” - Luglio 2018 - https://youtu.be/fDHECLdMTqQ
- Italiannonprofit - “Cos’è e come funziona il crowdfunding” - Data accesso: 31 maggio 2022 - https://italianonprofit.it/risorse/definizioni/crowdfunding/

NFT

- Riccardo Berti - “NFT: che cosa sono, come funzionano, come investire sui “Non Fungible Token” - febbraio 2022 - https://www.agendadigitale.eu/documenti/nft-che-cosa-sono-come-funzionano-come-investire-sui-non-fungible-token/amp/
- Autori vari – “Quando e come è stato acquistato il primo NFT: tutta la storia” Novembre 2021 - https://www.artribune.com/progettazione/new-media/2021/11/primo-acquisto-nft-new-york/
- Riccardo Staglianò - “L’opera da tre criptosoldi” - Dicembre 2021 - https://www.repubblica.it/venerdi/2021/12/17/news/nft_arte_digitale_criptovalute_bitcoin_collezionisti_reportage_stagliano_venerdi_repubblica-329930562/
- BitcoinEthereum - Dall'opera d'arte all'identità: l'evoluzione degli NFT - Ottobre 2021 - https://it.bitcoinethereumnews.com/technology/from-artwork-to-identity-the-evolution-of-nfts/
- Riccardo Luna - “La truffetta NFT di Melania Trump” - marzo 2022 - https://www.italian.tech/blog/stazione-futuro/2022/02/18/news/la_truffetta_nft_di_melania_trump-338231896/
- Gianni Rusconi - Dicembre 2021 - “Dagli Nft al Metaverso: Viaggio nelle tendenze tech del 2022 e oltre” - https://amp24.ilsole24ore.com/pagina/AE1E9a4
- Andrea Daniele Signorelli - “Perché nel mondo dell’arte, e non solo, sono tutti pazzi per gli NFT” - Marzo 2021 - https://www.wired.it/economia/finanza/2021/03/20/nft-arte-collezione-blockchain/amp/
- Luca Tremolada -“NFT e gaming: come la blockchain cambia le regole del gioco” - Gennaio 2022 - https://amp24.ilsole24ore.com/pagina/AE6JwM7