UNIVERSITÀ DEGLI STUDI DI ROMA

“TOR VERGATA”

MACROAREA DI LETTERE E FILOSOFIA

CORSO DI LAUREA IN
LINGUE NELLA SOCIETÀ DELL’INFORMAZIONE

TESI DI LAUREA IN
METALINGUAGGI DI MARCATURA

TITOLO

Evoluzione dell'arte digitale attraverso la tokenizzazione: caso studio sui token non fungibili (NFTs)

Relatore

Prof.

Giorgio Piccardo

Laureanda

Aurora Possenti

Anno Accademico

2022/2023

Indice

Introduzione

Negli ultimi anni è emersa un'innovazione che risulta essere rivoluzionaria nel mondo delle risorse digitali: *Non-Fungible token (NFT).*

Questa tesi si concentra sull'importanza degli *NFTs* nell'intersezione di tre ambiti cruciali: arte, tecnologia e finanza. Questa convergenza ha generato un crescente interesse sull'argomento e ha sollevato domande riguardo al futuro della proprietà, dell'autenticità e del valore in questa nuova era digitale.

La domanda centrale di questa tesi è: "In che modo gli NFT stanno influenzando l'arte, l'economia e la cultura digitale?"

Al fine di ottenere una comprensione approfondita di questo nuovo mondo, questa tesi si impegna a esaminare tutti gli aspetti dei token non fungibili attraverso quattro diverse sezioni, partendo dal tipo di tecnologia di cui essi fanno uso fino all'applicazione pratica delle conoscenze acquisite.

La prima sezione definisce gli *NFTs* e spiega le relative tecnologie utilizzate quali *Blockchain* ed *Ethereum*, nonché i vari algoritmi, i *DAO*, i *Smart Contracts* e i protocolli da essi utilizzati.

La seconda sezione approfondisce la storia dell'arte digitale, tracciando un percorso evolutivo nel tempo evidenziando i primi casi d'uso degli *NFTs*. Viene illustrato il processo di creazione e vendita degli *NFTs*, includendo vantaggi e svantaggi nel contesto artistico.

La terza sezione si concentra sugli aspetti legali, esaminando diverse problematiche relative al diritto di autore, alla proprietà e alle frodi, sia dal punto di vista europeo che italiano.

Nell'ultima sezione viene fornita una dimostrazione pratica di quanto precedentemente illustrato riguardo i token non fungibili, attraverso un esempio di creazione e vendita di un *NFT*.

In conclusione, questa mia tesi auspica a fornire un quadro completo degli *NFTs*, esplorando le loro implicazioni tecnologiche, artistiche, legali e pratiche. Contribuendo a una maggiore consapevolezza e comprensione del potenziale degli *NFTs* nel breve e nel lungo termine.

1. Cos’è un NFT

Un *NFT* “*Non-fungible token*” è una tipologia di criptovaluta costituita da metadati univoci e codici di identificazione, rappresentante un’unità non intercambiabile di un’opera digitale, quale immagine, video o suono.

Gli *NFTs* vengono creati utilizzando una tecnologia *blockchain*, che consente di registrare e tracciare la proprietà e la trasferibilità di un’opera digitale in maniera sicura. Questo significa che un *NFT* può essere utilizzato per verificare l’autenticità e la proprietà di un’opera digitale, rendendola unica e di valore.

1.1 Storia degli NFTs

La storia degli *NFT* inizia con la nascita della tecnologia chiamata *blockchain*, rilasciata nel 2009 per la creazione di *Bitcoin.*

Nel 2011, cominciarono ad essere veicolati nella *blockchain* di *bitcoin* vari elementi testuali privi di utilità, che possono essere visti come un esperimento o primi tentativi di creazione di qualcosa di unico successivamente definito non-fungibile, all’interno del registro decentralizzato.

Nel 2014 avvenne una cosiddetta *fork*[1], la quale porta alla nascita di una *blockchain* parallela, la *Counterparty*[2], che permette la realizzazione di *criptoasset*[3] unici. Da questo momento in poi cominciano a svilupparsi quelli i primi NFT, composti da meme. In questo stesso anno viene rilasciata un’opera d’arte digitale intitolata “*Quantum*” dagli artisti Jennifer e Kevin McCoy, si tratta di un breve video che rappresenta l’inizio di questa nuova forma d’arte.

Due anni dopo, su *Counterparty* viene lanciato il primo *collectables* di NFT, chiamato *Force of Will*, rappresenta una serie di carte digitali che possono essere collezionate.

[1] Fork: in programmazione consiste nella modalità attraverso cui un processo crea in memoria una copia di se stesso, questa prenderà il nome di processo figlio, mentre il processo originale sarà chiamato processo padre.
[2] Counterparty: o controparte, tradizionalmente si tratta dell’altra parte di una transazione finanziaria, ma in questo caso si intende il protocollo di tipo metacoin, costruito sulla rete Bitcoin per consentire agli utenti di coniare, acquistare e vendere asset digitali unici.
[3] Cryptoasset: risorsa digitale che viene creata e funziona per mezzo di tecnologie crittografiche, e rappresenta una risorsa di valore.

Nel 2013, lo sviluppatore Vitalik Buterin promulga una nuova *blockchain*, diversa da quella del *bitcoin* e la denomina *Ethereum*.

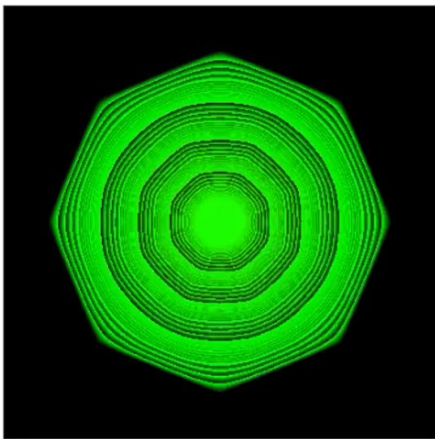

Figura 1: Opera *"Quantum"* di *McCoy.*

Su questa nuova blockchain si può programmare tramite codici chiamati *smart contract*, una raccolta di codici (con le loro funzioni) e dati (il loro stato), che si trovano ad un indirizzo specifico sulla *blockchain* di *Ethereum*. Questi definiscono delle regole e le applicano in maniera automatica tramite il codice, vengono distribuiti in rete ed eseguiti senza il controllo da parte di un utente, quest'ultimo può esclusivamente usarli, ovvero interagire inviando transazioni che eseguono una funzione. Queste azioni sono irreversibili, infatti queste raccolte di codici di *default*[4] non possono essere eliminate o modificate.

Il funzionamento dei codici è logico, seguendo una struttura *if this then that* digitalizzano i termini di un contratto o accordo in codici di tipo informatico, così che tutte le condizioni vengano rispettate.

L'esplosione di questa nuova tecnologia, NFT, avvenne nel 2021. Il valore delle transazioni è aumentato nel 2020 da $ 82.492.916 a $ 17.694.851.721 del 2021.

[4] Default: in informatica consiste nella scelta operativa elaborata da un sistema in assenza di istruzioni da parte dell'utente.

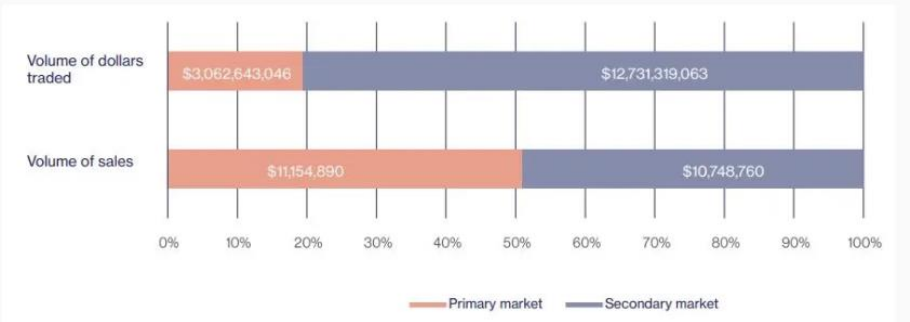

Figura 2: Volume delle vendite e dollari scambiati del mercato primario e secondario.

1.2 Tecnologia Blockchain

La tecnologia *Blockchain* si tratta di un registro digitale, un sistema immutabile, trasparente, distribuito e decentralizzato che fa uso di una catena di blocchi di dati e nodi.

I nodi possono essere qualsiasi cosa, un router, un computer o un cellulare e ce ne sono due tipologie: pieno e parziale. Il nodo pieno consiste in un computer che possiede l'intera catena di blocchi e ogni blocco che viene aggiunto successivamente, il suo compito è la verifica della catena di blocchi e ha bisogno di una grande quantità di spazio.

Questa tipologia di nodo può essere anche un *miner*[5], in questo caso servirà un'enorme potenza di calcolo, quindi un intero centro con pile di *CPU* e un'enorme quantità di *GPU*, ogni volta che un blocco subisce il mining, si è ricompensati con una commissione di transazione e in più nel caso dei Bitcoin, si avrà un bitcoin per ogni blocco minato.

Un nodo parziale può essere un telefono, su cui dopo aver scaricato un software, si può scaricare una parte della catena di blocchi e può essere usato anche come portafoglio.

Ognuno di questi blocchi composto da un insieme di dati, ovvero tutte le transazioni registrate e trasmesse agli altri nodi, quindi il volume dei dati è estremamente alto. Un blocco possiede un *header* ovvero un'intestazione, la marca temporale indicante la sua creazione, le varie versioni o i vari protocolli

[5] Miner: o minatore è colui che attraverso il processo di mining utilizzato da Bitcoin per utilizzare nuove monete e convalidare transazioni collegandole a quelle già esistenti.

utilizzati, un *merkle tree*[6], un obiettivo di difficoltà, un *nonce*[7] e infine un hash di riferimento.

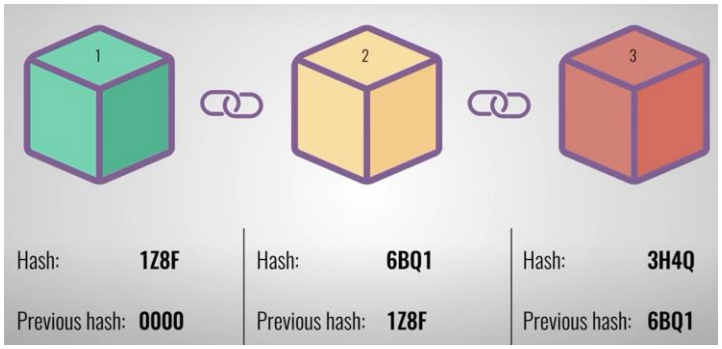

Figura 3: Struttura catena di blocchi a partire dal Genesis Block.

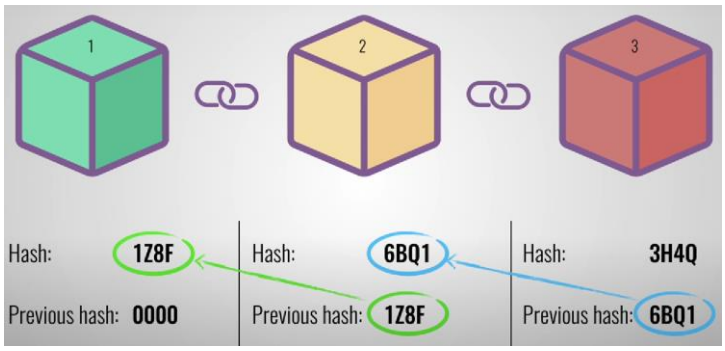

Figura 4: Gli hash di riferimento ai blocchi precedenti.

Il blocco che dà inizio alla catena viene chiamato *Genesis Block*, al quale viene assegnato un *hash*[8], però essendo il blocco iniziale, non possiede l'hash di riferimento al blocco precedente per questo gli viene affidato come chiave 0000, mentre il secondo blocco avrà un *hash* diverso, poiché possederà la chiave di riferimento del blocco precedente e la stessa cosa accade a quelli successivi. Se uno di questi valori di riferimento viene cambiato, i successivi non avranno più un *hash* di riferimento al blocco precedente, questo comporta che tutti i blocchi successivi non saranno più validi.

[6] Merkle Tree: una struttura dati con l'obiettivo di facilitare la verifica dell'integrità di grandi quantità di dati.
[7] Nonce: o number only used once, un numero che un miner deve scoprire prima di risolvere un blocco nella blockchain, utilizzato una sola volta.
[8] Hash: termine inglese per "sminuzzare", si tratta di una funzione cui dati vengono "sminuzzati" per essere portati ad una lunghezza uniforme, indipendentemente il valore di partenza.

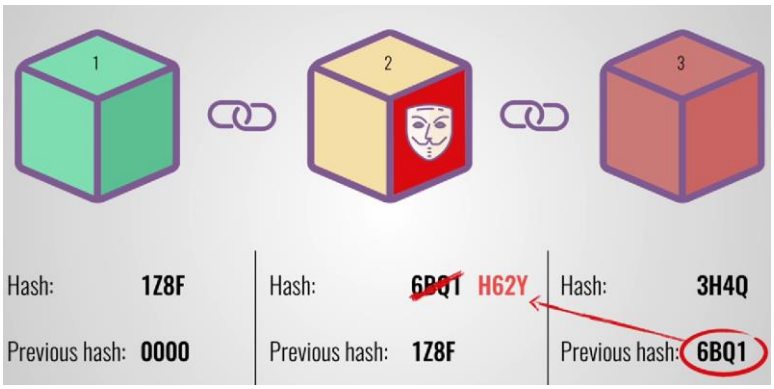

Figura 5: Secondo blocco manomesso e conseguente mancanza del riferimento.

L'*hashing*[9] consiste in una funzione crittografica in grado di convertire una stringa di caratteri con una lunghezza qualsiasi in un *hash* che avrà una lunghezza prestabilita, quindi indipendentemente dalla combinazione di simboli in *input*, come *output* ci sarà sempre una stringa di cifre e caratteri unici. Una funzione *hashing* può essere considerata buona se: l'*output* è dato dai dati all'inizio del processo, vengono utilizzati completamente non ci saranno dati inutili e sono distribuiti in maniera uniforme sull'insieme dei valori *hash*, per stringhe simili vengono generati valori diversi di *hash*. Questo processo non è essenziale solo all'estrazione di blocchi, ma per tutti i processi riguardanti transazioni e alla generazione di chiavi private.

Bitcoin	Contanti Bitcoin	Ethereum	Bitcoin	Ondulazione
SHA-256	SHA-256	keccak256	scrypt	SHA-512

Figura 6: Esempi di hash.

Le principali proprietà dell'*hashing*:

- Output di lunghezza fissa: indipendentemente dalla tipologia dell'input inserito, il risultato finale è generato unicamente, con la stessa lunghezza, ovvero 64 caratteri, 256 *bit*[10].
- È deterministico: lo stesso input produrrà sempre lo stesso output.
- Funzione unidirezionale: partendo dall'output non sarà possibile risalire al suo input, l'unico modo è utilizzando il metodo di forza bruta, ovvero

[9] Hashing: algoritmo matematico utilizzato per calcolare l'hash, ovvero un output univoco.
[10] Bit: la cifra binaria consiste nell'unità di misura elementare dell'informazione, rappresentata alternativamente con 0 e 1.

provare stringhe casuali fino a che non si troverà la stringa giusta, ma per faro ciò ci vorrebbero moltissimi anni e una grande potenza computazionale.

- Resistenza alle collisioni: anche se la probabilità è bassa, la collisione consiste nel verificarsi di uno stesso output in due diversi input dati, questo può accadere perché si ha un infinito numero di input, ma un finito numero di hash univoci.

Il processo dell'*hashing* è la base su cui poi si costruirà la blockchain. Inizialmente c'era l'MD, *message digest*[11] con le sue diverse versioni, MD2[12], MD3…MD6, invece tutt'ora ci si sta spostando verso SHA, *secure hash algorithm* costruito dall'NSA, *national security agency*, anche di questo algoritmo ci sono varie versioni: SHA0, SHA1, SHA2, SHA3. Nella blockchain viene usata la famiglia dei SHA2, 256 o 512 bit.

Le caratteristiche della *Blockchain* sono:

- Immutabilità del registro: dopo che i dati sono stati registrati non possono essere modificati e/o cancellati senza il consenso della rete, per garantire l'autenticità e la tracciabilità di tutte le transazioni.
- Decentralizzazione: avendo le informazioni registrate su più nodi e quindi mancando un'entità centrale, il sistema è più resistente ad attacchi e risulta difficile falsificare o modificare i dati.
- Sicurezza: la crittografia e i meccanismi di consenso garantiscono la protezione delle transazioni per eventuali frodi e da attacchi informatici.
- Trasparenza e verificabilità: le informazioni contenute sul registro sono accessibili a tutti e possono essere facilmente verificate.

La blockchain funziona su una rete *peer-to-peer*[13], ovvero un'architettura di calcolo in cui non si ha bisogno di un server centralizzato, ma ci sono multipli nodi e possono scambiarsi informazioni tra loro in maniera diretta. È definita "da pari a

[11] Message digest: una funzione hash crittografica contenente una stringa di cifre creata da una formula di hashing unidirezionale, serve per proteggere l'integrità di un dato o supporto per la rilevazione di alterazioni a qualsiasi parte di un messaggio.
[12] MD2: o message digest algorithm 2 è un algoritmo crittografico di hashing ottimizzato per computer da 8 bit.
[13] Rete peer-to-peer: consiste in una rete informatica nella quale i computer degli utenti connessi fungono nello stesso tempo da client e server.

pari” poiché i nodi non hanno una struttura gerarchizzata, ma riescono a svolgere sia il ruolo di *client*[14] che di *server*[15].

1.2.1 Crittografia asimmetrica

La crittografia consiste in una tecnica secondo la quale si vuole inviare un messaggio da X a Y, di cui solo Y può leggerne il contenuto e può farlo solo decriptando il file, quest’ultima fase avviene se sia X che Y possiedono le due chiavi.

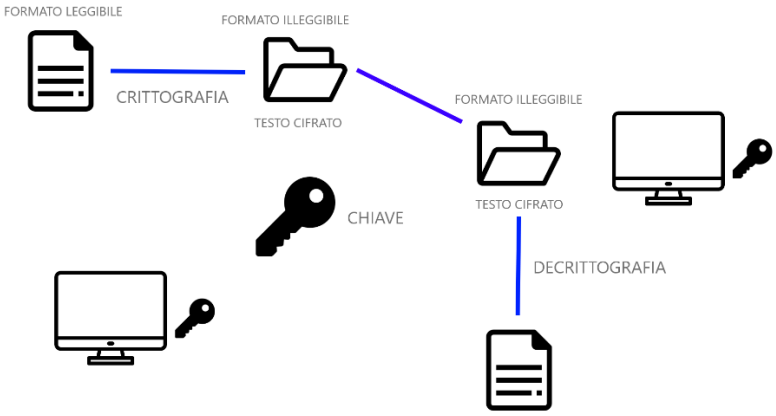

Figura 7: Crittografia.

Ci sono due tipologie: Crittografia simmetrica e asimmetrica.

Per permettere le transazioni, quindi lo scambio di beni tra una persona e un’altra, la blockchain fa uso della crittografia asimmetrica, grazie alla quale solo il proprietario riesce a decriptare una determinata transazione.

La crittografia asimmetrica fa uso di due tipologie di chiavi: privata e pubblica, unite tra loro tramite una funzione che rende possibile il deciframento di una delle due grazie l’altra.

[14] Client: programma o una parte di esso che permette lo scambio di dati con un server.
[15] Server: un computer di elevate prestazioni che in una rete fornisce un servizio agli altri elaborati collegati con il server, definiti client.

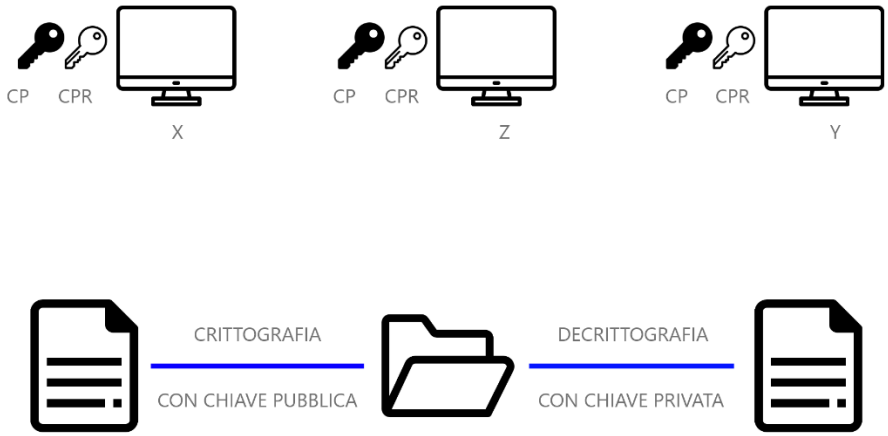

Figura 8: Funzionamento della crittografia asimmetrica.

Se invece si utilizza inizialmente la chiave privata, poi si dovrà usare quella pubblica, nota anche come *address*, per decriptarlo, si devono utilizzare entrambe contemporaneamente, non è possibile utilizzare solo una chiave per entrambi i processi.

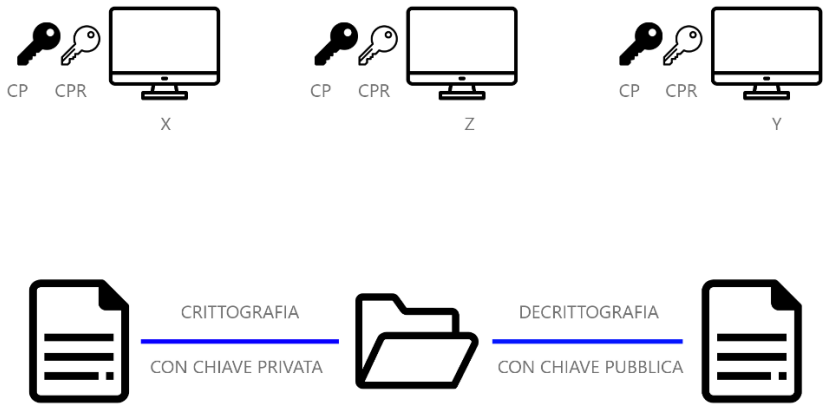

Figura 9: Utilizzo della chiave privata inizialmente.

Figura 10: Impossibilità nell'utilizzare una sola chiave.

Il vantaggio di questa tipologia di crittografia è di poter passare il messaggio attraverso un canale non sicuro senza che nessuno ne possa leggere il contenuto, garantendo la sicurezza delle transazioni. Questo processo è utilizzato anche per l'implementazione della firma digitale. Viene utilizzata la chiave privata per firmare o *signing* un testo chiamato *signature* o firma.

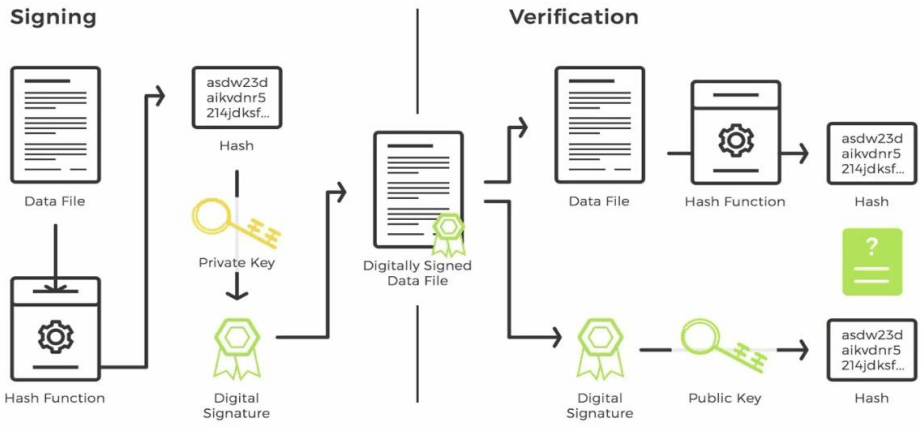

Figura 11: Processo di firma e successiva autenticazione.

Il file viene crittografato con la funzione hash, firmato digitalmente per poi passare alla fase di autenticazione per avere la certezza su chi lo abbia mandato e usando la chiave pubblica è decriptato dal ricevente.

Merkle tree

All'interno di un qualsiasi blocco posizionato sulla blockchain, si ha una struttura chiamata *Merkle tree*, questa è una struttura dati suddivisa in vari livelli che associa ad essi una sola e unica radice, che risulterà nel valore hash dell'intero

blocco. Colui che inventò questo fu Ralph Merkle, nel 1979, ciò di cui si necessitava era un modo per velocizzare la verifica di grandi quantità di dati. Un albero di Merkle è una struttura formata da valori di hash:

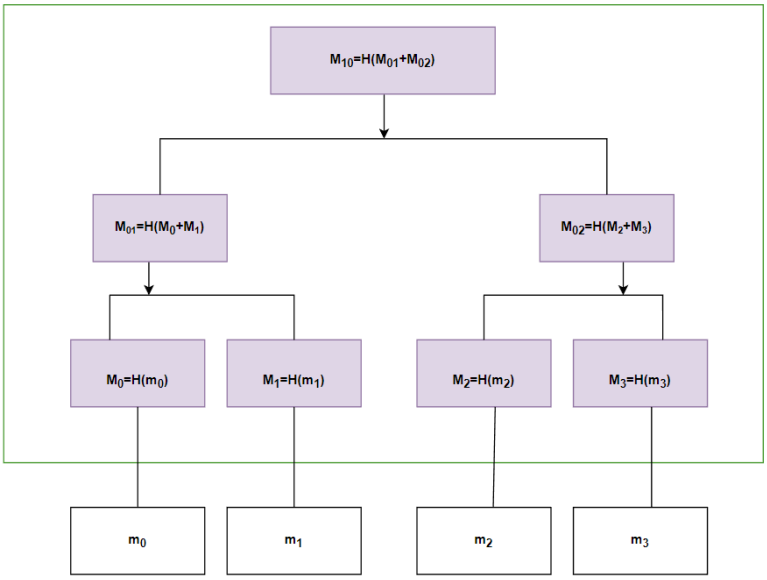

Figura 12: Merkle Tree.

Nell'immagine precedente si può notare che soltanto i valori hash (M) sono considerati una parte dell'albero di *Merkle*, mentre i valori (m) non sono compresi.

Ogni blocco ha il suo valore hash associato a ogni nodo e all'interno un numero n di transazioni. I nodi iniziali vengono definiti foglie e vengono associati a un ramo, ovvero un ramo superiore.

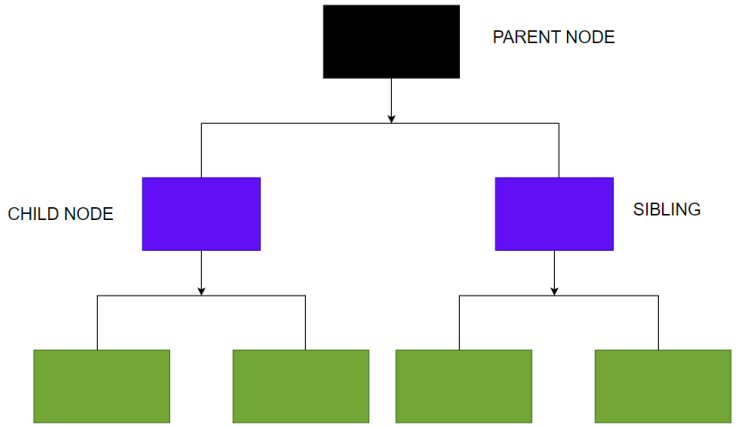

Figura 13: Struttura dei blocchi nel Merkle Tree.

Se ogni nodo ha due foglie sottostanti, si parla di un albero hash binario.

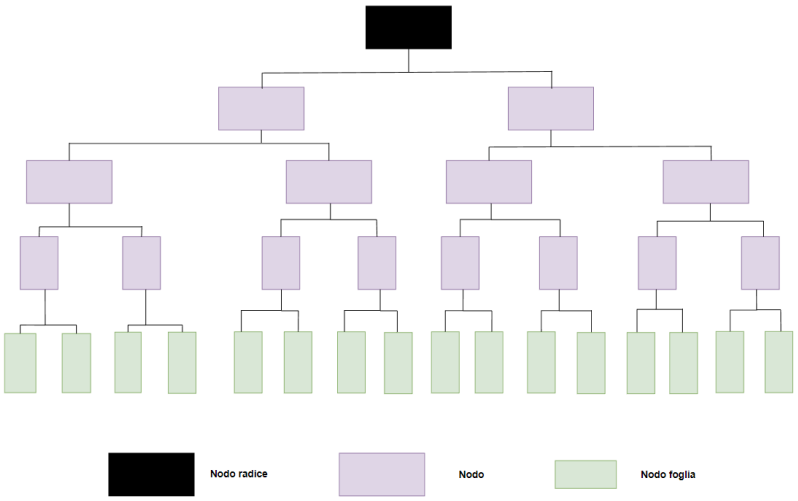

Figura 14: Struttura albero hash binario.

Prendendo un singolo blocco, si suppone che al suo interno ci siano un numero di transazioni pari a dieci e ognuna possiede un codice hash.

Figura 15: Contenuto dei singoli blocchi.

Questi hash dei rami vengono raggruppate a due a due e si calcola il loro numero di hash.

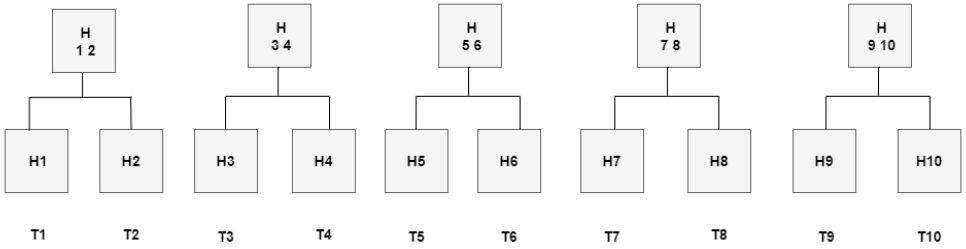

Figura 16: Calcolo di coppie di hash.

Gli hash risultanti si combinano di nuovo e si calcola un altro hash.

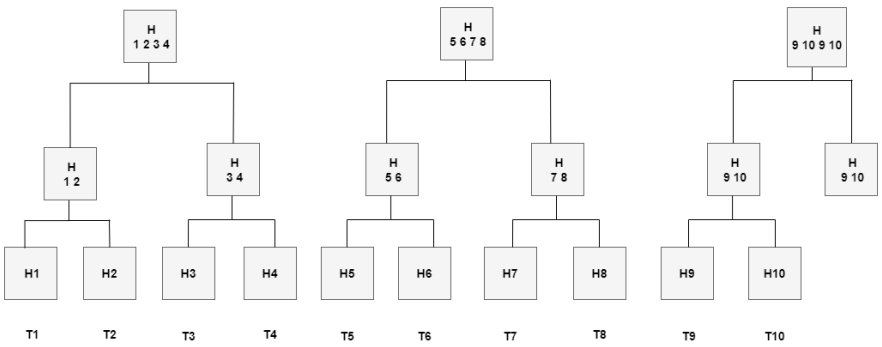

Figura 17: Calcolo unendo gli hash già calcolati a coppie.

Si effettuerà lo stesso procedimento fino ad avere una struttura ad albero, con in cima la radice dell'albero Merkle.

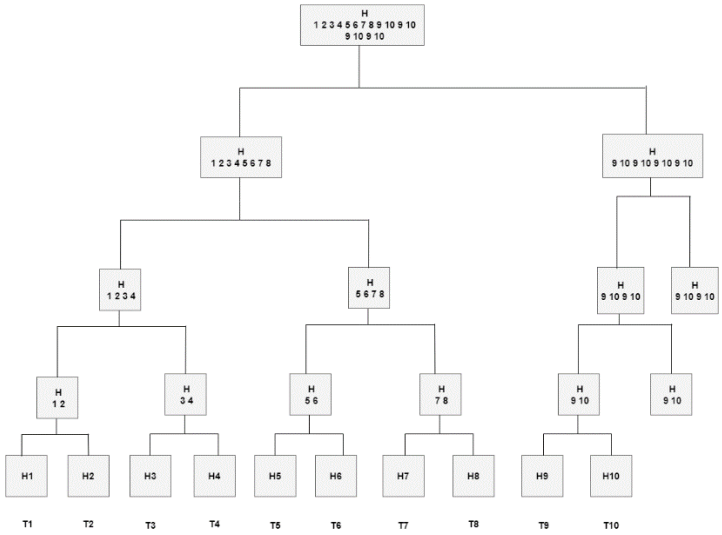

Figura 18: Calcolo degli hash fino al nodo radice.

Questo procedimento viene effettuato per calcolare l'hash di un singolo blocco, questo hash principale contiene tutti i dati contenuti nelle singole transazioni che lo compongono.

La *merkle root* possiede una proprietà chiamata *Simplified Payment Verification*[16] o SOV, verrà richiesta una *merkle proof*, ovvero una prova data dal *full node o nodo pieno,* per dimostrare la posizione di una determinata transazione in un blocco.

1.2.2 Algoritmi di consenso

[16] Simplified payment verification: è un client leggero utilizzato per verificare le transazioni crittografiche sulla blockchain. Gli utenti eseguono transazioni P2P mentre i nodi formano il regolamento.

Un algoritmo di consenso è un meccanismo usato nel sistema delle blockchain per raggiungere l'accordo su un singolo valore di dati o stato della rete tra più sistemi, uno tra i quali può essere la criptovaluta, la quale utilizza il *proof of work*. Questo permette di acquisire fiducia tra sconosciuti in un ambiente decentralizzato.

Viene garantito che il blocco aggiunto alla catena sia l'unica versione accordata da tutti i nodi formanti quella determinata blockchain.

1.2.2.1 Algoritmo Proof of Elapsed Time (PoET)

Il *proof of elapsed time* è un algoritmo di consenso utilizzato sulla blockchain, il quale genera casualmente un tempo di attesa per ogni nodo, per poter decidere i diritti di mining e con il suo sistema di lotteria blocca i vincitori sulla rete come se fossero in *stand-by*, il nodo con il tempo di attesa più breve, si "sveglierà" per primo vincendo il blocco e avendo la possibilità di impegnare un nuovo blocco nella blockchain, grazie alla trasparenza gli utenti possono verificare i risultati della lotteria. L'algoritmo fu sviluppato da *Intel Corporation*[17] nel 2016 e utilizzato principalmente in *Hyperledger Sawtooth*[18], un registro distribuito per la catena di approvvigionamento e la logistica di aziende.

Questo tipo di algoritmo utilizza meno potenza di calcolo rispetto ad altre tipologie e ha bisogno di un certificato a chiunque voglia far parte della rete, per questo motivo non fa uso di un sistema decentralizzato.

1.2.2.2 Algoritmo Proof of Capacity (PoC)

Il *proof of capacity* o prova di capacità è un meccanismo che consente ai dispositivi di mining nella rete di utilizzare lo spazio sul disco rigido per decidere i diritti di *mining* e convalidare le transazioni, l'algoritmo stila una lista di possibili soluzioni già prima di iniziare il processo di mining, invece di ripetere i numeri hash o dell'intestazione del blocco. Per questo motivo, più grande è il disco rigido, più valori si possono memorizzare e più solo alte le possibilità che i *miners* vincano

[17] Intel Corporation: società elettronica statunitense produttrice di semiconduttori e microprocessori, fondata nel 1968 da R. Noyce e G. Moore, che inizialmente si dedicò alla produzione di dispositivi di memoria, ma successivamente all'invenzione dei microprocessori nel 1970, l'azienda si specializzò in questo ramo.

[18] Hyperledger Sawtooth: piattaforma blockchain aziendale per la creazione di reti e applicazioni di contabilità distribuita. Lo sviluppo di queste è semplificato grazie alla separazione tra sistema principale e dominio dell'app.

una ricompensa. In questo algoritmo ci sono due passi da seguire: *plotting* e *mining*.

- *Plotting*: il disco rigido viene tracciato, si crea la lista di tutti i valori possibili del *nonce* tramite l'hashing ripetuto dei dati, includendo l'account del *miner*. Ognuno di questi *nonce* contiene 8192 hashes, numerati da 0 a 8191, e accoppiati in scoop ovvero adiacentemente in una coppia di due.
- *Mining*: in questo secondo passo, un *miner* calcola la scadenza di una coppia di scoop. Dopo averla calcolata per tutti i *nonce*, viene selezionato quello con la scadenza minima. La scadenza consiste nella durata del tempo in secondi dal momento della creazione dell'ultimo blocco prima che ne venga creato un altro.

Questo algoritmo possiede vari vantaggi: la possibilità di utilizzare qualsiasi disco rigido, dal punto di vista energetico la sua efficienza supera il mining di Bitcoin basato su *ASIC*[19], non si ha bisogno di un hardware specifico e i dati mining posso essere cancellati e riusare il disco. Però utilizzando il *PoC* è possibile che i malware influiscano sull'attività di mining, per questo non è un sistema diffuso tra gli sviluppatori.

1.2.2.3 Algoritmo Proof of Work (PoW)

Il meccanismo di consenso utilizzato da parte di alcune blockchain è il *Proof of work* (*PoW*), il quale conferma le transazioni e crea nuovi blocchi, questo viene svolto attraverso un processo conosciuto come *mining*. Ai nodi della rete, chiamati *miners* (minatori) viene presentato un problema matematico complesso da risolvere ma facile nel momento della verifica della validità delle transazioni contenute nel blocco.

Gli obiettivi di questo processo sono:

- L'iniziale convalida delle transazioni e la successiva aggiunta del blocco alla catena di blocchi;
- L'aggiunta del blocco alla catena con l'altezza del blocco più lunga;

[19] ASIC: sigla di Application Specific Integrated Circuit, che in elettronica in particolare tipo di circuito integrato. Nella maggioranza dei casi sono dispositivi digitali, dotati di memoria, capacità elaborativa ed elementi di calcolo specifici, utili nel campo dell'elaborazione numerica dei segnali.

- I *miners* lavorano per risolvere un problema matematico complesso per aggiungere il blocco alla rete;
- La continua crescita di complessità del problema.

Ogni macchina possederà una copia di essa nella rete della blockchain.

La sicurezza è garantita anche da una serie di meccanismi di crittografia *peer-to-peer* e di consenso tra tutti i partecipanti alla rete, definiti nodi. Quindi non c'è un utente possessore del sistema, ma la rete dei partecipanti conferma e registra tutte le transazioni avvenute.

1.2.2.4 Algoritmo Proof of Stake

Il *proof of stake* è un algoritmo di consenso utilizzato nella blockchain. Al suo interno ci sono i *validators*, ovvero i partecipanti alla rete sono coinvolti nella verifica delle transazioni e nella creazione di blocchi successivi proporzionati alla rete di ogni utente e per fare ciò si deve fare uno *stake*[20] di una somma di criptovalute. In cambio dello *stacking* della criptovaluta si guadagna una maggiore quantità di essa. I creatori dei blocchi vengono scelti in base a vari criteri, come il saldo effettivo. Se vengono validati dati fraudolenti, il *validator* può perdere tutti o una parte del suo *stake*.

Alcune delle criptovalute che utilizzano questo meccanismo sono Solana, SOL ed Ethereum, ETH. Ogni blockchain richiede un set di regole per i validatori, di tenere almeno 32 ETH.

1.2.3 Tipologie di Blockchain

La *blockchain* può essere suddivisa in quattro tipologie: pubblica, privata, ibrida e *consortium*.

[20] Stake: consiste nell'impegnare una somma delle proprie criptovalute per poter garantire la validità delle operazioni effettuate.

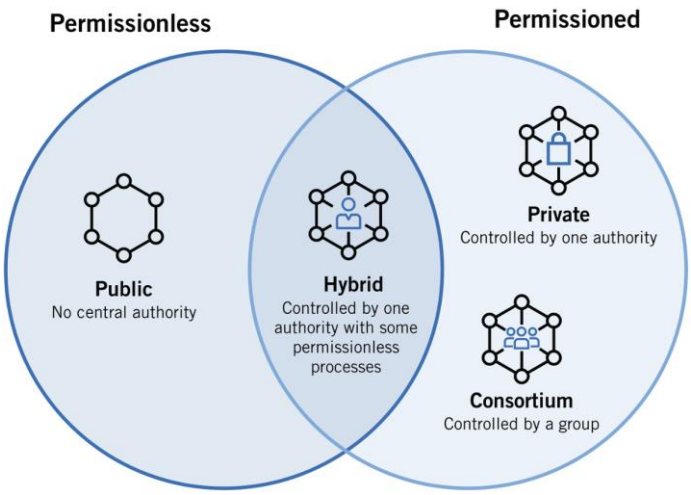

Figura 19: Tipologie di blockchain.

Il modello suggerito da *Satoshi Nakamoto* nel 2009 fu di una blockchain pubblica o anche definita *permissionless*, aperta e chiunque può accedervi, è decentralizzata, non possiede un'autorità principale, i nodi connessi alla rete hanno uguali diritti di accesso, creazione di nuovi blocchi e la loro conseguente validazione, eseguita attraverso il meccanismo di *proof of work*. Su questo tipo di blockchain i nodi si scambiano principalmente criptovalute e alcuni esempi possono essere *Bitcoin*, *Ethereum* e *Litecoin*. I nodi risolvendo equazioni crittografiche, coniano la criptovaluta creando nuovi blocchi per set di dati, in cambio di questo ricevono una *fee*, ovvero una minima quantità di criptovaluta. Lo svantaggio di questa tipologia è il lungo tempo di validazione per i nuovi dati. Altre caratteristiche sono:

- Libero accesso ai nodi di lettura e scrittura sul registro;
- Potenziamento dell'utente, con il libero download e aggiunta di nodi al sistema;
- Anonimità, nessuno può tracciare le transazioni;
- Trasparenza;
- Immutabilità, nessuno può manomettere il sistema o rubare i soldi.

Opposta alla tipologia precedente si ha la blockchain privata o anche *permissioned*, controllata da una singola organizzazione, quale può essere un'impresa, di conseguenza si ha un'autorità centrale che può non garantire ai nodi eguali diritti. Alcuni esempi di blockchain private possono essere *Ripple* e *Hyperledger*. Lo svantaggio di questo tipo è la sua estrema vulnerabilità a frodi.

Consortium blockchain sono *permissioned* con a capo un gruppo di organizzazioni, quindi hanno un sistema decentralizzato che gli conferisce sicurezza. La sfida principale di questa tipologia è la difficoltà di creazione, in quanto a rischi antitrust, di logistica e di cooperazione. Un esempio di questa tipologia è il *Global Shipping Business Network Consortium* creato da *CargoSmart* con lo scopo di digitalizzare il settore dei trasporti marittimi.

L'ultima tipologia è la blockchain ibrida, controllata da una singola organizzazione con la supervisione della blockchain pubblica per poter eseguire le convalide delle transazioni. Un esempio è *l'IBM Food Trust*, per poter migliorare l'efficienza sulla catena alimentare.

1.3 Ethereum

Ethereum è una piattaforma decentralizzata, *open-source*[21] per la creazione di app e organizzazioni, per effettuare transazioni, lanciata nel 2015 sull'innovazione di Bitcoin, ma si distacca da quest'ultimo per la sua programmabilità, tramite il linguaggio *Turing-complete*[22], nella *EVM*, *Ethereum virtual machine*[23], il codice si compone di *smart contracts* memorizzati in strutture dati.

Lo scopo della EVM è di aggiornare lo stato globale dopo che vengono eseguite le transazioni, ogni nodo della macchina esegue una copia locale della EVM, quest'ultima è una *stack machine*, ovvero le operazioni svolte sono eseguite su un'area dati virtuale, formata da 1024 parole di 256 bit, per una breve durata di tempo e verso uno stack push down.

La blockchain di Ethereum ebbe molti fondatori, Gavin Wood, Charles Hoskinson, Amir Chetrit, Anthony di Iorio, Jeffrey Wilcke, Joseph Lubin e Mihai Alisie, ma colui che pubblicò un foglio in cui veniva spiegato il concetto e il funzionamento della

[21] Open-source: software di cui l'utente finale, che può liberamente accedere al file sorgente, è in grado di modificare a suo piacimento il funzionamento, correggere errori, ridistribuire a sua volta la versione da lui elaborata.
[22] Turing-complete: un linguaggio di programmazione di cui la sua semantica permette di implementare una qualsiasi macchina di Turing, usato per risolvere qualsiasi problema che ammetta soluzione. Quasi tutti i linguaggi di programmazione sono di questa tipologia.
[23] Ethereum virtual machine: consente l'esecuzione di programmi o contratti intelligenti al fine di implementare una serie di funzionalità aggiuntive sulla blockchain.

catena di blocchi fu Vitalik Buterin nel 2013 con un *white paper*[24], successivamente fu formalizzata da Gavin Wood nel 2014. Lo sviluppo iniziò nel 2013, le prime versioni furono programmate in linguaggio *Go* e *C++* invece successivamente vennero sviluppati tre linguaggi: *serpent*, *LLL*, *Mutan*. La prima iterazione della blockchain di ethereum che la fece funzionare tramite smart contracts e il proof of work mining fu denominata *Frontier*, con il tempo ci furono molti aggiornamenti, tra questi ci fu *Byzantium*, *Constantinople* e la *Beacon Chain*, tra l'uno e l'altro sono stati alterati alcuni aspetti della blockchain, ad esempio nel beacon chain, venne cambiato l'algoritmo di consenso, da un *proof of work* a un *proof of stake*, che inizialmente avevano un funzionamento parallelo, nel 2022 questo passaggio avvenne definitivamente unendo la rete principale Ethereum con il meccanismo PoS, riducendo così il consumo energetico del processo di mining del 99,95%, quest'ultimo processo non è più usato per la produzione di blocchi, poiché questo compito venne affidato ai validatori o stakers, che per portare a termine il loro compito devono investire un capitale di ETH, il quale ha la funzione di garanzia. La tempistica per la creazione di nuovi blocchi con il PoS è predeterminata, suddivisa in slot, ovvero 12 secondi. Dopo il *merge*[25] la cronologia delle transizioni della rete principale venne fusa con la *Beacon Chain*.

Anche i primi due aggiornamenti apportarono varie modifiche, come una riduzione dei costi di mining da cinque a tre ETH.

In Ethereum esistono due tipologie di account: EOA e i *contract account*.

[24] White paper: documento informativo, emesso da un'azienda o da un'organizzazione no-profit, per promuovere o evidenziare le caratteristiche di una soluzione, prodotto o servizio.
[25] The merge: si riferisce al passaggio dell'algoritmo, che la blockchain utilizza per garantire la validità di ogni transazione e di ogni nuovo blocco aggiunto alla rete, e che i sviluppatori di Ethereum portarono a termine.

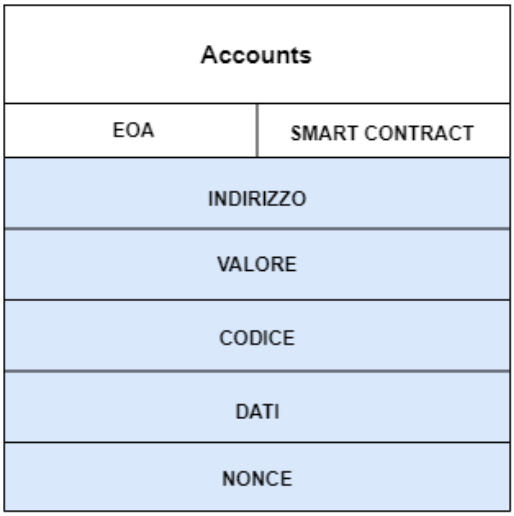

Figura 20: Struttura degli accounts.

- Agli *EOA* o *externally owned account*, viene associate una chiave privata capace di generare transazioni esterne.
- Ai *contract account* non viene associata nessuna chiave poiché non sono in grado di generare delle transazioni, si tratta di account controllati dagli *smart contracts*.

Le transazioni generate da questi account attivano le transazioni di stato, trasferendo valori monetari. Qualsiasi transazione esterna consiste in messaggi firmati digitalmente, che prendono origine dagli EOA e inclusi nei blocchi di Ethereum. Questi *message* sono tutte quelle transazioni da un EOA a un *contract account* contenente una chiamata parametrica a delle funzioni di uno *smart contract*. In ogni account della piattaforma si trova un valore scalare detto *nonce*, ovvero tutte le transazioni valide generate e questo risolve il problema del *double-spending,* il rischio di riuso della criptovaluta due o più volte.

Ethereum fa uso dei saldi correnti, definiti *stati* aggiungendovi lo *storage* degli *smart contracts*, le informazioni su queste transazioni di stato si trovano all'interno dell'albero di *merkle*. Per poter far girare contratti sulla rete peer-to-peer viene utilizzata un'unità di conto con la funzione sia di criptovaluta che di gas, l'*Ether* cui simbolo ETH o lettera greca *Ξ,* e deve essere indirizzata a un conto. Per rendere possibile quest'indirizzamento bisogna avere l'hash della chiave pubblica

ECDSA[26] che viene calcolato tramite l'algoritmo crittografico *Keccak-256*[27]. Gli indirizzi hanno 40 cifre esadecimali, cui prefisso 0x non si trova in memoria ma è inserito ogni volta, di seguito c'è la classifica di 10 indirizzi.

Rank	Address	Name Tag	Balance	Percentage	Txn Count
1	0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	Wrapped Ether	2,044,232.03368922 Ether	1.88687291%	469,801
2	0xbe0eb53f46cd790cd13851d5eff43d12404d33e8	Binance 7	1,985,015.10391695 Ether	1.83221433%	199
3	0x742d35cc6634c0532925a3b844bc454e4438f44e	Bitfinex 5	1,946,537.33355598 Ether	1.79669847%	5,398
4	0x53d284357ec70ce289d6d64134dfac8e511c8a3d	Kraken 6	1,378,754.14465437 Ether	1.27262160%	14,997
5	0xab7c74abc0c4d48d1bdad5dcb26153fc8780f83e		999,999.01470326 Ether	0.92302196%	465
6	0xdc76cd25977e0a5ae17155770273ad58648900d3	Huobi 6	850,860.64196888 Ether	0.78536383%	140
7	0x61edcdf5bb737adffe5043706e7c5bb1f1a56eea	Gemini 3	820,999.00123114 Ether	0.75780085%	162
8	0xe853c56864a2ebe4576a807d26fdc4a0ada51919	Kraken 3	801,052.79995972 Ether	0.73939005%	151
9	0xf4a2eff88a408ff4c4550148151c33c93442619e	Scam: Plus Token Ponzi	789,534.61080172 Ether	0.72875850%	1,007,669
10	0x267f70f9b856de226fea5fc1b0a8e319c72ceff5		697,220.00926344 Ether	0.64355001%	3

Figura 21: Top 10 indirizzi Ethereum.

Non è possibile identificare il beneficiario di questi conti, poiché non sono nominativi.

1.3.1 Smart contracts

Gli *smart contracts* sono dei programmi per computer memorizzati sulla blockchain di Ethereum che consentono di convertire i contratti tradizionali in digitali, consistono in una collezione di codici con le proprie funzioni e i propri valori localizzati in uno specifico indirizzo della Blockchain Ethereum.

La loro struttura è molto logica: *if this then that*. Il loro comportamento è programmato e non può essere cambiato.

Gli accordi digitalizzati vengono eseguiti in maniera automatica quando i termini degli stessi vengono rispettati.

Questi smart contracts vengono implementati tramite l'uso di un linguaggio di programmazione ad alto livello chiamato *Solidity*[28], che la blockchain di Ethereum

[26] ECDSA: si tratta di un algoritmo di firma digitale della curva ellittica, usato per firmare digitalmente per consentire la verifica da parte di terzi senza comprometterne la sicurezza.
[27] Keccak-256: algoritmo scelto dall'Istituto nazionale di standard e tecnologia per l'implementazione dello standard per la crittografia SHA-3.

non è in grado di capire, per questo motivo, prima che uno smart contract viene distribuito sulla catena è compilato sulla base di alcune istruzioni elementari che ethereum può capire, grazie anche all'utilizzo della EVM per eseguire i contratti intelligenti, la quale riesce a capire più di 100 istruzioni elementari, definite anche *EVM opcodes*.

Figura 22: Dal linguaggio ad alto livello alla Virtual Machine.

I contratti intelligenti possono essere paragonati alle classi dei linguaggi orientati agli oggetti, in Solidity. Ognuno di questi contratti può contenere dichiarazioni di variabili di stato, funzioni, modificatori di funzioni, errori, tipi Struct ed Enum, eventi e anche la proprietà di ereditare da altri contracts.

Le variabili di stato sono quei valori memorizzati in maniera permanente nel contratto:

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.0 <0.9.0;

contract SimpleStorage {
    uint storedData; // State variable
    // ...
}
```
[29]

Possono essere *constant*, ovvero il suo valore le viene assegnato in fase di compilazione o a livello di file, *immutable*, in fase di costruzione è ancora possibile assegnarle un valore. Queste due tipologie di variabili sono meno costose in quanto a gas rispetto alle variabili di stato normali. Per le variabili costanti non è consentita nessuna espressione di accesso allo storage, all'esecuzione dei dati, ai dati sulla blockchain o a chiamate a contratti esterni. Sono consentite le funzioni integrate *ecrecover*, *addmod*, *mulmod*, *ripemd160*, *sha256* e *keccak256*,

[28] Solidity: una tipologia di linguaggio di programmazione a oggetti come C++ e C#, in grado di sviluppare applicazioni per Ethereum.
[29] Fonte esempio: https://docs.soliditylang.org/en/latest/structure-of-a-contract.html

quest'ultima rappresenta un'eccezione poiché svolge chiamate a contratti intelligenti esterni.

Le variabili immutabili possono ricevere un valore arbitrario nella costruzione del contratto o nella loro dichiarazione.

Le funzioni consistono nella parte eseguibile del codice e possono essere interne o esterne, *free functions*, al contratto:

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.1 <0.9.0;

contract SimpleAuction {
    function bid() public payable { // Function
        // ...
    }
}

// Helper function defined outside of a contract
function helper(uint x) pure returns (uint) {
    return x * 2;
}
```
[30]

Le funzioni interne consistono soltanto in funzioni e variabili di stato accessibili dal contratto stesso o da quelli che ne derivano, perciò non creano una chiamata alla EVM. Le funzioni esterne, differentemente, creano una chiamata alla EVM poiché fanno parte dell'interfaccia del contratto e possono essere chiamati da altri contratti e transazioni. Come input le funzioni ammettono i parametri digitali e restituiscono un numero arbitrario di valori output. Questi input sono dichiarati come le variabili, omettendo il nome dei parametri non utilizzati. I valori di output sono poi restituiti dal codice dopo la parola chiave *return*[31], con la possibilità di ometterne il nome e utilizzarne come variabili.

I modificatori di funzioni se utilizzati in maniera dichiarativa permettono di modificare il comportamento delle funzioni, ma non sono in grado di accedervi o modificarne gli argomenti restituendo i valori modificati, una volta invocati questi valori sono inviati esplicitamente ai modificatori. Questa tipologia fa parte della proprietà ereditabile dal contratto.

[30] Fonte esempio: https://docs.soliditylang.org/en/latest/structure-of-a-contract.html
[31] Return: in informatica consiste nella terminazione della subroutine corrente, ripristinando il codice nel punto immediatamente successivo a quello in cui la funzione è stata chiamata.

Gli eventi non possono essere modificati dagli smart contract, vengono soltanto emessi da questi ultimi e memorizzati permanentemente sulla blockchain.

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity ^0.8.4;

/// Not enough funds for transfer. Requested
`requested`,
/// but only `available` available.
error NotEnoughFunds(uint requested, uint available);

contract Token {
    mapping(address => uint) balances;
    function transfer(address to, uint amount) public {
        uint balance = balances[msg.sender];
        if (balance < amount)
            revert NotEnoughFunds(amount, balance);
        balances[msg.sender] -= amount;
        balances[to] += amount;
        // ...
    }
}
```
[32]

Il tipo *Struct* contiene mappings e *arrays* per poter creare altre tipologie Struct, ma non può contenerle.

La tipologia *Enum* è usata per creare tramite un set di valori costanti dei tipo personalizzati, sono convertibili da e verso gli interi. Può contenere più di 256 membri e minimo 1. I dati sono rappresentati a partire da 0 con i valori successivi privi di segno.

Ogni dato contenuto in un contratto deve essere assegnato ad una posizione tra *storage*[33], *memory*[34] o *stack*[35]. Nello *storage* o archiviazione, si trovano tutti quei dati che sono persistenti, ovvero che poi saranno tenuti permanentemente sulla blockchain, bisognerà definire la tipologia del dato quando verrà compilato il codice, ad esempio:

[32] Fonte esempio: https://docs.soliditylang.org/en/latest/structure-of-a-contract.html
[33] Storage: si tratta di dispositivi hardware dedicati alla memorizzazione non volatile di grandi quantità di dati in formato elettronico.
[34] Memory: elemento di un computer che garantisce la persistenza dei dati o istruzioni di programmi.
[35] Stack: o pila, si tratta di un blocco contiguo di memoria contenente dati ordinati.

```
// Solidity example
contract SimpleStorage {
    uint storedData; // State variable
    // ...
}
```
[36]

Lo storage è un archivio che mette un relazioni valori-chiave, quindi in esso viene eseguito un mapping di parole a 256 bit a parole di 256 bit. Questa tipologia di archiviazione è molto costosa da modificare o da inizializzare, quindi ciò che viene memorizzato sono solo dati utili al contratto intelligente.

Contrariamente allo storage, nella *memory* vengono memorizzati dati volatili, ovvero quei dati che non sono memorizzati permanentemente sulla blockchain ma che verranno eliminati dopo l'esecuzione di una funzione e questa tipologia di dati è chiamata variabili di memoria. La memoria legge solo dati di 256 bit, mentre in quanto al processo di scrittura può essere lungo 8 o 256 bit, si ha la possibilità di espandere la memoria, ma più cresce, più aumenta il costo in gas da pagare.

L'ultima tipologia è lo *stack*, un'area dati in cui avvengono tutti i calcoli, la sua dimensione massima è di 1024 contenente parole di 256 bit. Le operazioni svolte nello *stack* seguono il processo *LIFO*, *last in first out*[37], prendendo i due o più elementi in alto, quindi gli ultimi entrati e ne inseriscono il risultato nello *stack* uscendo per primi.

Questi smart contracts possono essere considerati delle open *APIs*[38] e sono pubblici, però lavorando singolarmente poiché non in grado di inviare richieste *HTTP*[39], non possono ottenere informazioni e dovrebbero affidarsi a informazioni esterne che porterebbero a problematiche legate al consenso, per questo motivo vengono utilizzate applicazioni dette *Oracles*, per prelevare dati esternamente e

[36] Fonte esempio: https://ethereum.org/en/developers/docs/smart-contracts/anatomy/
[37] LIFO: last in first out, definisce il concetto del modo di immagazzinare dati in cui l'ultimo valore introdotto è il primo ad uscire.
[38] API: application programming interface, si tratta di un software che permette la comunicazione di due applicazioni tra loro.
[39] http: hypertext transfer protocol, si tratta del protocollo di accesso alle informazioni.

immetterli all'interno della blockchain così che gli smart contracts possano utilizzarli.

1.3.2 Le organizzazioni autonome decentralizzate (DAO)

Per DAO s'intende un'organizzazione decentralizzata gestita da blockchain composta da un insieme di contratti, non aveva un'autorità singola, ma un gruppo di persone provenienti da tutto il mondo che gestivano le operazioni così da non permettere ad un'unica persona di sprecare i fondi degli investitori, qualsiasi nuova decisione veniva proposta e successivamente votata da tutti i membri. DAO si presenta come totalmente trasparente, il codice poteva essere visibile a chiunque sulla rete, ma questo portò a un grande problema che avvenne nel giugno 2016, alcuni degli utenti sfruttarono una vulnerabilità del codice per sottrarre un terzo dei fondi. La blockchain decise di spostare tutti i fondi tramite l'hard-fork[40], ciò divise Ethereum in due branche, ognuna con la propria criptovaluta, in cui la catena di blocchi originale continua definita Ethereum classic. Colui che scrisse il codice open source fu Cristoph Jentzsch e lo caricò sulla piattaforma GitHub, dove ha ricevuto varie modifiche e contributi. Il 30 aprile 2016 fu lanciata sul blocco Ethereum 11428757 la DAO. Nel maggio del 2016 furono rivelate una serie di vulnerabilità sulla sicurezza e si consigliò agli investitori di non investire fino a quando i problemi non fossero risolti. Nel mese successivo ci fu un attacco utilizzando a proprio favore le vulnerabilità esposte precedentemente e comportò un trasferimento di 3,6 milioni di Ether. Ciò che definisce le regole dell'organizzazione e possiede il patrimonio del gruppo è il contratto intelligente della DAO, non modificabile dopo l'attivazione, solo attraverso la votazione del gruppo, se questa è positiva, le transazioni vengono eseguite automaticamente.

Attualmente gli unici ad avere almeno una legge sulle DAO, sono il Vermount, le Isole Vergini e il Wyoming, quest'ultimo inventò la LLC.

1.3.3 Uso nell'ecosistema della finanza decentralizzata (DeFi)

La *decentralized finance* consiste in un modo differente di finanza per transazioni, scambi e servizi finanziari basati su criptovalute. Non esiste più una figura principale e centralizzata al controllo di tutte le operazioni, ma si ha un'autorità

[40] Hard-fork: consiste in una modifica al protocollo blockchain incompatibile con le versioni precedenti e richiede a tutti gli utenti di aggiornare il software continuando a partecipare alla rete.

distribuita con poteri divisi egualmente tra ognuno e le operazioni quali vendite, prestiti o acquisti avvengono tramite il processo peer-to-peer, ovvero tramite l'accordo di due parti nello scambio di criptovalute senza coinvolgerne una terza e permettendo agli utenti di custodire i propri asset. Per funzionare la finanza decentralizzata fa uso della blockchain, a sua volta anche degli smart contracts, i quali permetto alla transazione di avvenire, però questi contratti sono altamente vulnerabili e possono portare a hack[41] se vi venisse trovato un bug al suo interno. Per questo motivo le DeFi non sono completamente decentralizzate, ma per alcuni progetti gli sviluppatori hanno una sorta di chiave per poter disabilitare o semplicemente chiudere le dapps.

I vantaggi di questo modello sono:

- la decentralizzazione permette che se ci fosse uno sbaglio negli scambi, il sistema non crolli e che non sia soggetto ad avversità o fallimenti;
- la trasparenza, il codice non è nascosto, bensì qualsiasi utente può visionarlo e capirne la logica;
- la custodia, gli utenti sono responsabili della custodia dei propri asset;
- senza permesso, la logica di ogni smart contract permette le approvazioni delle transazioni;
- l'anonimità, non c'è il bisogno di conoscere o identificare l'utente;
- *Fees*, le commissioni sono inferiori con il DeFi;
- DApps, gli utenti possono utilizzare queste applicazioni per scopi finanziari e no.

Chiunque possieda una connessione ad Internet può entrare a far parte della piattaforma e avere la possibilità di avviare transazioni, negoziando i tassi di interesse tramite la rete.

DeFi	Finanza tradizionale
Ogni soggetto detiene i suoi soldi.	I soldi dei soggetti sono detenuti dalle aziende.
Ogni soggetto può controllare dove vanno i suoi soldi e come vengono	Ogni soggetto deve fidarsi delle aziende per non gestire male i suoi soldi.

[41] Hack: forzatura abusiva in una rete di calcolatori per utilizzare dati e informazioni in essa contenuti.

spesi.	
I trasferimenti di fondi avvengono in pochi minuti.	I pagamenti possono richiedere giorni a causa di processi manuali.
L'attività di transazione è pseudonima.	L'attività finanziaria è strettamente legata alla tua identità.
DeFi è aperta a chiunque.	Bisogna fare domanda per utilizzare i servizi finanziari.
I mercati sono sempre aperti.	I mercati chiudono perché i dipendenti hanno bisogno di pause
Si basa sulla trasparenza: chiunque può esaminare i dati di un prodotto e ispezionare il funzionamento del sistema.	Le istituzioni finanziarie sono libri chiusi: non puoi chiedere di vedere lo storico dei loro prestiti, il registro dei loro patrimoni gestiti e così via

Ci sono svariati modo tramite i quali la DeFi può essere utilizzata, tra questi: inviare e far girare il denaro in tutto il mondo, la gestione del portafoglio e come finanza delle idee di ciascuna persona. Nel sistema finanziario si sta assistendo allo spostamento parziale di denaro, criptovalute, online e ciò permette alla DeFi di avere un margine di sviluppo e miglioramento di tutte le vulnerabilità possedute.

1.3.4 Alcuni dei progetti su Ethereum: Uniswap, NFT

Uniswap nasce nel 2018 da Hayden Adams, consiste in un set di programmi open-source che garantiscono lo scambio decentralizzato basato su Ethereum utilizzando la strategia market making automatizzata, ovvero il possedere un intermediario automatico che garantisca la negoziabilità di assets, questo permette agli utenti di abbinare due asset per scambiarli e il prezzo finale risulterà dal rapporto dei loro singoli prezzi. Gli unicorni sono coloro che fanno avvenire gli scambi di tokens senza che i trader debbano affidare i propri fondi a nessuno. Ci sono delle riserve speciali, chiamate *liquidity pools* in cui chiunque può affidare le proprie riserve di criptovalute guadagnando delle commissioni. Il protocollo funziona grazie a un design definito *Constant Product Market Maker*, una variante del modello AMM, *Automated Market Maker*. I market maker automatizzati consistono in smart contracts contenenti le *liquidity pools*, le quali permettono ai trader di negoziare, queste riserve sono arricchite dai fornitori di liquidità e

chiunque può esserne uno, la fee pagata dal trader va distribuita a tutti loro in base alla quota del suddetto pool.

Queste riserve di liquidità sono formate generalmente dalle cosiddette *stablecoin*[42]. Al loro interno possono esservi depositati due token ETH o ERC-20, oppure un token ETH e un ERC-20. Il progetto ricevette molti fondi per permetterne il suo lancio, tra i quali ci sono i 100,000 dollari da parte della fondazione Ethereum. Il token di questo protocollo è UNI, il quale conferisce il diritto di governance a chi lo possiede, quindi di votare le modifiche di Uniswap. Alla creazione furono coniati 1 miliardo di token, di cui il 40% è a disposizione degli investitori e del gruppo, mentre il 60% è distribuito ai membri della comunità.

Un altro dei tanti progetti presenti e sviluppatosi sulla piattaforma Ethereum è l'NFT o non-*fungible token*, questi sono una tecnologia nata nel 2017, ma che ha acquisito il suo successo soltanto negli ultimi anni, specialmente nel 2021, che è registrato come l'anno in cui il mercato ha avuto vendite record. È una tipologia di criptovaluta come il Bitcoin, da cui però differisce per le sue caratteristiche, infatti il Bitcoin consiste in una moneta standard e tutte le monete sono indistinguibili l'una dall'altra, invece l'NFT non può essere scambiato poiché ognuno di esso è unico e indentifica qualcosa nel singolo, ovvero stabilisce la provenienza dell'oggetto digitale a cui è assegnato. L'oggetto digitale può essere audio, foto, video e può trovarsi in vari campi, quali arte, sport, gaming e altro. Questa nuova tecnologia presenta ancora delle criticità, ma per avere un NFT funzionante, si ha bisogno di:

- Una blockchain, in particolare il modello NFT è basato su Ethereum, su cui può eseguire i suoi contratti intelligenti;
- Smart contracts, introdotti da Szabo hanno l'obiettivo di accelerare, verificare ed eseguire la transazione digitale. Questi permettono a parti sconosciute e partecipanti decentralizzati di condurre scambi equi senza una terza persona;
- Indirizzo e transazione, nella blockchain un indirizzo identifica in maniera univoca l'utente permettendogli di inviare e ricevere risorse ed esso consiste in un numero finito di caratteri alfanumerici che sono generati da una chiave pubblica e una privata;

[42] Stablecoin: è un criptoasset ancorato a un altro asset, come valute fiat o metalli preziosi.

- Codifica dei dati, consiste nel processo di conversione di essi da una forma a un'altra, generalmente la codifica avviene su file compressi. Su Ethereum la codifica di nomi o parametri viene fatta con valori esadecimali. Se un utente possiede la proprietà intellettuale NFT la versione che ha unica, ovvero riconosciuta dal creatore e firmata da esso, altri utenti possono fare una copia dei dati grezzi dell'opera, ma non avranno mai la proprietà a meno che non la comprino.

Gli NFTs hanno uno standard con una serie di informazioni univoche al suo interno indicanti l'età, grado di rarità e popolarità, caratteristiche che differenziano quel token da altri non fungibili. Lo standard ERC-721 mostra le caratteristiche di non fungibilità e viene assegnato automaticamente alla creazione di un NFT, fornisce ad esso un'API consentendo la connessione di programmi, fu lanciato nel gennaio del 2018 da William Entriken, Jacob Evans, Nastassia Sachs e Dieter Shirley. L'ERC-721 permette il trasferimento di un singolo token. Questo è utilizzato ad esempio nei Cryptopunks o nel Bored Ape Yatch Club. I token di questo standard posseggono una cronologia di transazioni e questi differiscono dall'originario standard ERC-20. Un esempio di algoritmo:

```
interface ERC721 {

function ownerOf(uint256 tokenId) external view returns (address);

function transferFrom(address from, address to, uint256 tokenId)

external payable; ...

}
```
[43]

Nell'esempio si può notare una variabile uint256 chiamata tokenId, la quale è generale, vale a dire, posseduta da ogni NFT indipendentemente dalla sua tipologia.

Lo standard ERC-1155 consente maggiore rapidità e quantità in quanto a creazione e trasferimento di tokens contemporaneamente, anche definito multi-token standard poiché rappresenta sia token fungibili che non fungibili. Questo standard prevede una diminuzione di tariffe di conio e gas, inoltre riduce le

[43] Esempio fornito dall'articolo: https://arxiv.org/pdf/2105.07447.pdf

informazioni memorizzate su ethereum, tuttavia uno degli svantaggi è rappresentato dalla difficoltà di rintracciare i dati di proprietà, questo non lo rende adatto agli NFT.

Un altro standard è l'ERC-725, il quale contiene tutte le informazioni legate all'identità dell'oggetto digitale, definita identità auto-sovrana, ovvero gestita dagli utenti e non in possesso di un'organizzazione centralizzata.

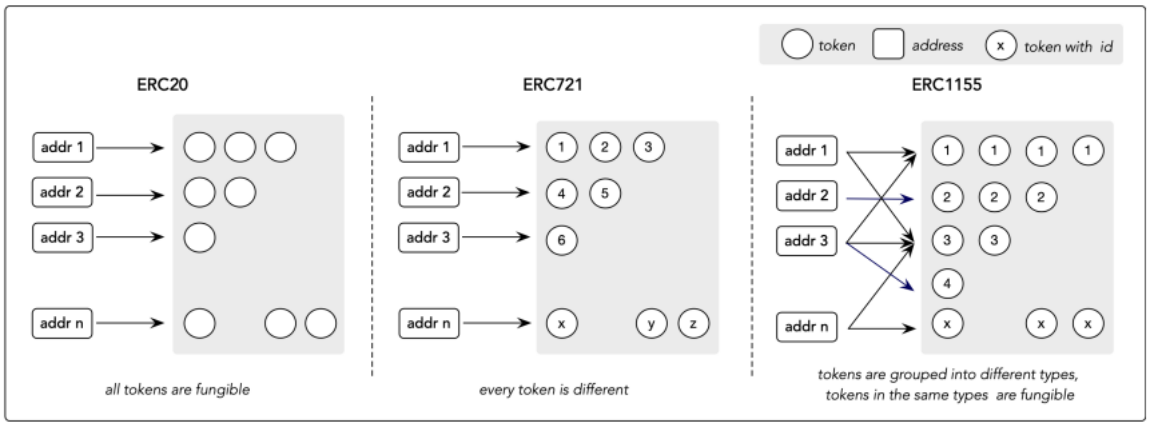

Figura 23: Token standard.

L'acronimo ERC significa richiesta di commento Ethereum, lo standard su questa piattaforma è rappresentato dall'ERC-20, il cui uso è la produzione di token sulla blockchain e la regolazione di token fungibili ovvero quelli intercambiabili come la criptovaluta.

1.3.5 Concetto di fungibilità e non fungibilità

Il concetto di fungibilità raggruppa tutti quelle risorse digitali che posso essere sostituite o scambiate da un'altra risorsa identica ad essa conservando valore. Qualsiasi cosa nel mondo reale può essere fungibile se scambiata con lo stesso oggetto, mentre nel mondo virtuale ci si riferisce alle criptovalute, in particolare i Bitcoin. La fungibilità del token fa riferimento alla sua divisibilità. Invece il concetto di non fungibilità afferma che un token è unico quindi non intercambiale con altre risorse, questo rende il suo valore maggiore rispetto a un token fungibile. La non fungibilità del token è data dalle sue caratteristiche intrinseche.

1.3.6 Caratteristiche degli NFT

Un NFT può essere rappresentato da qualsiasi cosa del mondo reale, musica o un'opera d'arte, ma qualsiasi cosa esso rappresenti possiede le stesse caratteristiche:

- Atomicità: come impostazione definitiva un NFT è indivisibile, non può essere scomposto in parti più piccole, ma si può parlare di una proprietà frazionata, ovvero più utenti possono possedere lo stesso NFT, questo rende semplice la rappresentazione di un asset come più NFT invece che dividere lo stesso;
- Verificabilità: è possibile verificare pubblicamente chi possiede l'NFT, la chiave privata di questo è posseduta dal creatore, il quale ha il compito di trasferire i token a qualsiasi account. I metadati dell'NFT permettono al proprietario del determinato NFT di utilizzarlo senza averne i diritti di proprietà;
- Resistenza alla manomissione: i metadati dell'NFT e i dati relativi alla sua vendita vengono persistentemente archiviati sulla blockchain senza possibilità di modifica;
- Esecuzione trasparente: le attività di scambio, vendita, conio di un singolo NFT sono accessibili pubblicamente dagli utenti;

1.3.7 Protocolli: Top to Bottom e Bottom to Top

Gli NFTs sono costruiti alla base di due modelli principali:

- *Top to Bottom*: un processo che inizia dal principio quindi dalla costruzione dell'NFT, la sua vendita e infine all'acquirente. Il creatore dell'NFT inizialmente deve accertarsi dell'accuratezza di tutti i dati che saranno poi propri del token, tra questi c'è la descrizione e il titolo del file, tuttavia a questo stadio solo soltanto dati grezzi, quindi il compito del creatore è quello di digitalizzare il file nel formato corretto. Una volta digitalizzato, il file può trovarsi memorizzato all'interno di un database esterno alla blockchain, ma non solo, i dati possono essere memorizzati anche all'interno della blockchain, questo comporta il pagamento del gas per poter portare a termine l'azione. A questo livello il file è digitalizzato e archiviato, ora il compito del creatore è quello di firmare la transazione con l'hash dell'NFT per poi inviarla ad uno smart contract, il quale inizia il processo di conio e

poi di negoziazione, questo porta alla fine del processo una volta che la transazione viene completata, l'NFT sarà associato univocamente a un indirizzo blockchain.

- *Bottom to Top*: questo processo è l'inverso del precedente, ovvero parte dall'output retrocedendo fino ad arrivare all'input, si avrà un template su cui poi ognuno può costruire il proprio NFT. Inizialmente si ha la creazione del modello da parte del creatore che tramite uno smart contract imposta una serie di caratteristiche quali possono essere diversi accessori, vestiti, stili del soggetto e alcune regole del gioco/del collectibles. L'NFT ha la possibilità di essere personalizzato dall'acquirente tramite funzionalità aggiuntive che non vengono scelte dall'utente, ma sono selezionate in maniera random da un database predefinito. Da questo punto fino alla fine del processo ci sono le stesse tappe del TtB, quindi fase di conio e inizio del processo di negoziazione, conferma della transazione.

2. Utilizzi degli NFTs

2.1 Storia dell'arte digitale

L'arte è sempre stata un'espressione creativa dell'umanità e in particolare dell'artista, espressione della cultura e della società in cui si vive, assumendo nel tempo varie forme e utilizzando diverse tecniche per poter suscitare emozioni e veicolare idee.

Si può suddividere il concetto di arte in tre macrogruppi:

- Arte statica: include pittura, scultura, fotografia e disegno. Utilizzando oggetti come la tela, la carta o la ceramica per fare in modo che il soggetto abbia equilibrio e sia ben proporzionato.
- Arte performativa: comprende le arti dello spettacolo, la danza, la musica e il teatro. Vengono utilizzati il corpo e la voce per la creazione dell'arte.
- Arte digitale: si riferisce a opere d'arte create tramite l'utilizzo di tecnologie digitali, quali computer, smartphone e software.

La storia dell'arte digitale inizia negli anni '60 quando cominciarono ad apparire sulla scena i primi computer e i primi *software* di elaborazione grafica, grazie ai

quali gli artisti di quel tempo cominciarono a sperimentare questo nuovo modo di produzione d'arte.

Nel corso degli anni l'arte digitale continuò ad evolversi e negli ultimi anni '70 venne sviluppato un software di pittura, al laboratorio di intelligenza artificiale dell'università di Stanford utilizzato dall'artista Harold Cohen. Si trattava di una macchina robotica che permetteva la realizzazione di grandi disegni su fogli di carta poggiati sul pavimento e fu denominata *AARON*. Il nome di questa macchina fu scelto su base alfabetica in modo tale che i programmi successivi potessero continuare con la B e così via.

Le versioni iniziali di *AARON* creavano disegni astratti in bianco e in nero, che venivano poi dipinti a mano dall'artista usando tintura del tessuto, con il tempo diventarono sempre più complessi fino a disegnare figure che si trovavano in ambienti interni e colorate. Agli inizi degli anni 2000 invece, *AARON* ritornò allo stile astratto ma con l'aggiunta dei colori. Questa macchina non sapeva imparare in maniera autonoma nuovi stili, ogni nuova capacità doveva essere codificata da Cohen utilizzando inizialmente il linguaggio di programmazione C e successivamente *Lisp*[44] (*List Processor*). Per programmare la sua macchina, Cohen utilizzò svariati disegni prodotti da bambini combinandoli a uno studio sull'iconografia dei nativi americani e altre tipologie di disegno. *AARON* può essere considerata nell'arte l'equivalente del *Test di Turing*[45] nell'arte digitale.

Negli anni '70 si ha l'artista tedesco Manfred Mohr trasformando il suo stile da un espressionismo astratto a una geometria algoritmica generata dal computer, influenzato dalla teoria di Max Bense, il quale si poneva l'obiettivo di oggettivare la realtà in modo tale da avere opere matematicamente estetiche. Nel 1969 programmò i primi lavori generativi programmando in linguaggio FORTRAN[46] su un computer CDC 6400[47], che si trovava nell'istituto meteorologico di Parigi.

[44] Lisp: famiglia di linguaggi di programmazione con implementazioni sia compilate sia interpretate, nel passato associata a progetti di intelligenza artificiale.
[45] Test di Turing: Criterio per determinare se una macchina possa esibire un comportamento intelligente. A.M. Turing, *Computing machinery and intelligence*, 1950, Mind.
[46] Fortran: linguaggio di tipo compilativo con tipizzazione statica delle variabili, progettato per il calcolo scientifico e numerico.
[47] CDC 6400: consiste in un mainframe facente parte della serie CDC 6000 sviluppato dalla Control Data Corporation durante gli anni '60.

Dalle prime creazioni di Cohen, le quali furono dei primi rudimenti di intelligenza artificiale, ad oggi, le nuove tecnologie combinano l'intelligenza artificiale all'apprendimento automatico, l'artista sceglie una serie di immagini e crea un *dataset*[48]*,* insegnando all'algoritmo stili già esistenti producendo come output una serie di immagini. Uno dei primi a sperimentare l'algoritmo fu Mario Klingemann, che creò arte concentrandosi sul corpo umano, allenando l'algoritmo alle possibili posture con il corpo può assumere.

Figura 24: *"The Butcher's Son" (2017)* - Mario Klingemann.

Il ritratto precedente è stato generato da un algoritmo e venduto all'asta per 432.500 dollari.

Un altro noto artista digitale è Refik Andadol, il quale grazie all'utilizzo di algoritmi basati su dati inseriti negli archivi digitali creò opere astratte e oniriche. Il suo ultimo progetto fu denominato *Machine Hallucinations: Nature Dreams,* nel quale viene mostrata l'estetica basata su degli ambienti visivi con combinazione di spazi naturali e urbani.

Dall'intelligenza artificiale si passa alla realtà aumentata, la quale implica l'interfacciarsi tra il mondo reale e quello digitale, migliorando il primo utilizzando elementi visivi digitali, suoni o stimoli sensoriali. Durante il 2020, Kaws, pseudonimo di Brian Donnelly, esibì sculture AR nelle aree metropolitane del mondo, vendendo i pezzi per circa 10.000 dollari.

[48] Dataset: insieme di dati organizzati in forma relazionale, con struttura tabellare in cui ogni colonna è rappresentata da una variabile e ogni riga un'osservazione.

Figura 25: Sculture AR ad Hong Kong.

Questo fa capire la costante sperimentazione in ambito di tecnologia digitale, aprendosi anche a un nuovo tipo di pubblico e aiutando gli artisti a non aver bisogno di rappresentazione. Recentemente, ci sono state problematiche sul valore monetario e la proprietà dell'arte digitale, la quale rappresentava un problema già prima dello sviluppo della tecnologia *blockchain*, delle criptovalute e degli NFT.

2.1.1 Primi casi di uso degli NFT nel mondo dell'arte

L'opera d'arte *NFT*, denominata *crypto art,* rappresenta una delle varie modalità in cui vengono impiegati gli NFT.

La prima forma di crypto arte si fa risalire al 2014, alla trasformazione di *Quantum* in NFT, un'opera precedentemente creata da Jennifer e Kevin McCoy sul *Namecoin*[49]. Coniata per ragioni di proprietà, ovvero il creatore voleva trovare un modo per poter vendere il pezzo nella sua forma digitale, però in quegli anni non aveva la possibilità di stabilirne la proprietà e chi fosse il creatore. Dopo l'anno di trasformazione in *NFT*, *Quantum* fu dimenticata, ma una volta che questo mondo di *tokens* non fungibili esplose, ebbe molto successo poiché considerato il primo NFT e fu venduta poi attraverso *Sotheby's* per 1.47 milioni di dollari nel 2021. Dopo aver venduto l'opera, *Namecoin* non attestava esattamente chi fosse il possessore di *Quantum*, poiché la piattaforma circa ogni 40 settimane richiedeva di rinnovare l'elemento coniato per mantenerne la proprietà e quest'azione non è mai stata svolta da McCoy.

Questo fece sì che i diritti di proprietà su *Quantum* furono acquisiti da *EarlyNFT* prima dell'asta e contestò con una causa la validità di *Sotheby's.*

[49] Namecoin: si tratta di un progetto il cui obiettivo è di creare un DNS decentralizzato e sicuro e un sistema di identità utilizzando la tecnologia blockchain.

Nei due anni successivi, viene sviluppata una collezione di carte digitali, coniate nella blockchain.

Rare Pepe Wallet

Il *Rare Pepe Wallet* consiste in un *wallet o* portafoglio crittografato creato da Joe Looney ed eseguito su *Counterparty,* una piattaforma finanziaria *peer-to-peer*, dove inizialmente venivano scambiati NFT per poi essere venduti anche su *OpenSea*. Di tutte le carte che furono create, circa 1.800 raccolte in 36 serie, la prima carta è omaggiata a *Satoshi Nakamoto*.

Figura 26: Carta di Nakamoto, PEPE Pope e Pepellum.

Rare Pepe è basato sul meme circolante su internet di *Pepe the Frog* creato da Matt Furie nel 2005. *Pepe the Frog* consiste in una rana antropomorfa con un corpo umanoide, usata nel 2010 dal movimento di estrema destra e i suprematisti bianchi come loro simbolo, diventando così nel 2016 uno dei simboli d'odio inserito nel database dalla *Anti-Defamation League*[50]*,* che però non fu utilizzato solo in contesti legati all'odio.

[50] Anti-Defamation League: consiste in un'organizzazione non governativa ebraica internazionale con sede negli Stati Uniti specializzata in diritto dei diritti civili.

Figura 27: (da destra a sinistra) meme delle elezioni del 2016 rappresentate Donald Trump, la seguente rappresenta la campagna per salvare Pepe nel 2016, infine il tentato funerale di Pepe da parte del creatore nel 2017.

Successivamente, il creatore di *Pepe the Frog*, vedendo come veniva inteso dalle persone il suo personaggio avviò una compagna *#SavePepe*, per salvare l'immagine della rana, tuttavia non ebbe alcun successo, così nel 2017 inserì in un fumetto il funerale di Pepe stesso, sperando di portare a termine la fama e i significati negativi associatovi, ma anche questo non ebbe successo e *Pepe the Frog* continuò ad avere successo. Così Matt Furie iniziò a far valere i suoi diritti creativi del personaggio contro le immagini di estrema destra tramite consulenza e uso di avvocati 'pro bono', i quali diedero assistenza volontaria e gratuita. Grazie alla comunità asiatica il personaggio *Pepe the Frog* cominciò ad essere associato a un simbolo di speranza, usato nelle proteste di Hong Kong del 2019 dei cittadini verso la legge imposta dal governo cinese sull'estradizione.

Figura 28: Proteste a Hong Kong del 2019.Proteste a Hong Kong del 2019.

Furono creati in contemporanea due componenti che lavorano insieme per consentire l'interazione e il continuo scambio di risorse:

- *Rare Pepe Wallet*, portafoglio crittografato basato sul web che consente l'acquisto, la vendita e la conservazione dei Pepes rari agli utenti, per

portare a termine queste azioni si ha bisogno della moneta di scambio, denominata *PepeCash*.

- *Rare Pepe Directory*, fu una *directory*[51] utilizzata per la catalogazione di tutti i Rare Pepe contenente anche le linee guida, infatti la fondazione Rare Pepe eliminava tutte le immagini risultanti offensive prima che esse sarebbero diventate visibili a tutti. Questa *directory* non accettò più carte a partire dal 2018, però poi nel 2021 Matt Furie creò la sua carta *Rare Pepe* intitolata *FEELSGOODMAN*, ricordando il film uscito l'anno precedente che riassumeva la storia della rana, così da completarne la collezione.

Figura 29: (da destra a sinistra) Il documentario "Feels Good Man" del 2020, La Pepenopoulos card messa all'asta al Sotheby's nel 2021.

Con il crescente successo degli NFT e l'impossibilità di creare altre carte Rare Pepe, l'artista Scrilla creò un progetto chiamato *Fake Rares*, a cui poi venne creato il rispettivo *wallet* da Joe Looney.

CryptoPunks

CryptoPunks è una delle prime collezioni di NFT, creata da Matt Hall e John Watkinson, degli sviluppatori che dopo il college formarono il *larva lab.* Questa collezione è composta da immagini 24x24 *pixel*[52] e tramite un algoritmo vengono generate diverse caratteristiche in tal modo da avere immagini sempre diverse tra loro. È la rappresentazione dei non conformisti e disadattati, l'ispirazione fu presa dal movimento dei punk di Londra del 1970, ma la sua caratteristica distopica è conferita dal film *Blade Runner* e dal romanzo neuromante di William Gibson. Due

[51] Directory: in informatica consiste nell'indice dei documenti contenuti in una determinata unità di memoria.
[52] Pixel: il più piccolo elemento (distinto per colore, intensità, ecc.) in un'immagine digitale.

anni prima dell'effettiva creazione e poi uscita dei *Cryptopunks*, fu creato da Hall e Watkinson un generatore digitale di personaggi sottoforma di esperimento, tramite il quale decisero successivamente di creare i *Cryptopunks*, facilmente visualizzabili e scaricabili da Internet, ma con un solo proprietario presente sulla *blockchain* per ogni immagine.

A seguire, per facilitare la funzione del mercato che permette alle persone di acquistare e vendere i punks, i due programmatori crearono uno *smart contract*, poi la collezione fu postata sul *subreddit*[53] di *Ethereum* e soltanto 100 persone reclamarono un punk e i due li offrirono gratuitamente, poiché non si aspettavano che questo progetto potesse diventare un successo come poi accadde una settimana dopo. Infatti, dopo un articolo riguardante questa collezione appena creata di crypto arte pubblicato da *Mashable*, molte persone comprarono un punk e dopo un giorno non erano più disponibili poiché venduti tutti.

Il valore di questi è dato dalla loro rarità, le immagini meno rare e quindi aventi meno valore sono quelle che raffigurano ragazze e ragazzi punk, tuttavia si possono trovare anche soggetti diversi, come zombies, alieni e scimmie. Il valore non è dato soltanto dal soggetto raffigurato, ma anche dagli accessori che esso ha, quali possono essere orecchini, berretti, sigarette, occhiali, capigliature particolari, barbe e altro. L'intervallo di attributi va da 0 a 7, più attributi possiede un'immagine e più rara sarà. Ad esempio, il cryptopunk8348 ha 7 attributi:

Figura 30: cryptopunk8348.

Sono presenti anche *cryptopunks* con 0 attributi che sono considerati egualmente rari. In totale ci sono 10.000 immagini, di cui solo 9 raffigurano alieni.

[53] Subreddit: i forum presenti sul sito Internet di social news denominato Reddit.

Il cryptopunk3100 raffigurante un alieno ha un solo attributo, ovvero la fascia per capelli, la quale è presente in 406 punks.

Il seguente punk è ancora in vendita dal proprietario per 7.3KΞ, vale a dire 11.93M di dollari.

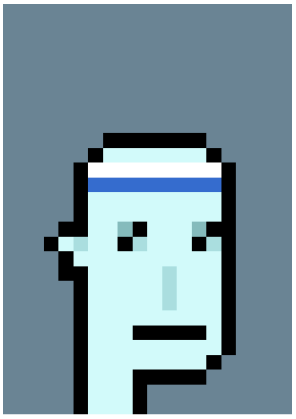

Figura 31: Cryptopunk3100.

Figura 32: Cryptopunks con fascia per capelli.

Alcuni punks sono più ricercati rispetto ad altri. La presenza di attributi non determina l'aumentare o diminuire il prezzo di vendita, il fluttuare dei prezzi varia in base alla richiesta del particolare punk sul mercato, quindi il prezzo s'innalza all'innalzarsi dalla richiesta.

Il primo a esibire una collezione di nove *cryptopunks* stampati fu George Bak nella galleria *voss* nel 2018. Nello stesso anno i due programmatori Hall e Watkinson fecero delle litografie di 24 punks, che furono poi firmate da entrambi. Ognuna di queste litografie aveva con sé una busta sigillata contenente la chiave privata definita *paper wallet*, una volta aperta avrebbe conferito la proprietà di quel crypto

punk alla persona. Queste furono vendute all'asta Sotheby's per centinaia migliaia di dollari.

Figura 33: Litografia e il paper wallet.

Dal febbraio 2021 al marzo 2021 ci fu una crescente domanda dei *cryptopunks*, di cui la conoscenza venne resa sempre più pubblica e non solo tra gli appassionati, tramite i social media, di conseguenza il costo della collezione continuo ad alzarsi.

Art Blocks

Art Blocks lanciato nel 2020 da Erick Calderon semplificò la creazione di arte generativa, ovvero quell'arte digitale realizzata tramite l'uso di un algoritmo informatico. Si tratta di una piattaforma basata su *Ethereum,* che utilizzando delle tipologie di *script*[54] generativi crea opere d'arte ognuna distinta dall'altra, generate al computer. Il processo consiste nella creazione di un progetto *art blocks* NFT, da parte di un'artista, caricando gli algoritmi unici sulla piattaforma e fornendo anche il numero specifico di quanti possono essere coniati ciascuno, gli investitori possono coniare questi NFT, ma non sapranno l'aspetto del token finale finché non lo avranno acquistato. L'*output* di questo processo è considerato un ERC-721 NFT poiché è costruito usando la rete Ethereum.

Snowfro ebbe l'idea di creare questa piattaforma dopo aver partecipato nel 2017 in *CryptoPunks*, anche se il suo progetto differisce da quest'ultimo. L'idea dietro la piattaforma era quella di poter coniare gli NFT al momento dell'acquisto, infatti furono crittografate le proprietà NFT durante la realizzazione di *Art Blocks NFT*. La

[54] Script: insieme di strumenti per la programmazione, più semplici da utilizzare rispetto ai linguaggi tradizionali.

prima collezione lanciata fu *Chromie Squiggle*, 10.000 pezzi cui caratteristica principale era la loro semplicità, costituiti solo da opacità, colori e intrecci diversi.

E' possibile calcolare la quantità della tonalità di colore di ogni scarabocchio:

(Passi tra i segmenti * numero di segmenti) / diffusione del colore

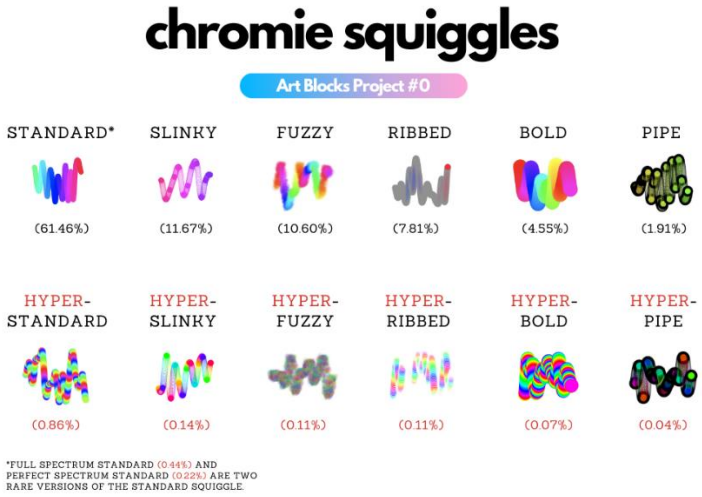

Figura 34: La prima collezione.

Sulla piattaforma *Art Blocks*, il conio e l'acquisto di NFT è molto semplice e diretto, ciò di cui si ha bisogno è un portafoglio crittografico *Ethereum*.

Il processo si può riassumere nei seguenti passaggi:

- Creazione e caricamento del codice scritto utilizzando il framework *Javascript*[55], sulla piattaforma *Art Blocks NFT* da parte dell'artista;
- Creazione sulla piattaforma di un codice esadecimale randomizzato, definito *seed*;
- All'interno del *seed* ci sono vari elementi rappresentanti l'attributo costituente l'opera d'arte già esistente;
- Creazione dell'NFT finale, solo dopo l'acquisto da parte dell'investitore.

Lo stesso codice può produrre diversi NFT, che saranno simili tra loro e allo stesso tempo nessuno di essi sarà identico, garantendo l'unicità dell'opera.

La nascita dell'arte generativa non risale agli ultimi anni, bensì esiste da decenni, tuttavia non era disponibile un mercato intorno ad essa fino alla nascita degli NFT.

[55] Javascript: linguaggio di scripting lato client utilizzato per rendere interattive le pagine Web.

Ci sono tre collezioni accessibili da parte degli artisti:

- *Curated collection*: include tutti gli NFT che hanno attraversato un processo di verifica, cui durata può arrivare fino ai due anni, svolto dai membri del gruppo di *Art Blocks*. Viene aggiunto un nuovo set di opere ogni trimestre.
- *Playground collection*: una volta che le opere di un'artista sono nella collezione curata, sarà poi in grado di inserirle nella sezione playground, in cui i progetti non vengono sottoposti ad alti processi di verifica come accade nella collezione precedentemente, però ciò non sta a significare che l'artista è libero di caricare ciò che vuole in un momento qualsiasi, ci sono delle regole da seguire.

  Può essere pubblicato un soggetto alla volta e c'è incoraggiamento per gli artisti alla sperimentazione. Se cambia una specifica dopo la pubblicazione del progetto, l'artista inizierà di nuovo il processo e verrà sottoposto a nuova verifica nella raccolta *Curated* prima di potersi riunire a *Playground*. Il tempo di attesa prima di iniziare un altro progetto è un mese.
- *Factory collection*: include le opere degli artisti che sono stati rifiutati dalla collezione curated e chi non vuole aspettare di essere aggiunto ad essa. I progetti vengono avviati rapidamente, senza processo di verifica, l'unico requisito è che siano funzionali.

  Lo svantaggio è rappresentato dall'impossibilità di possedere contemporaneamente opere d'arte in questa e nella collezione precedente.

2.1.2 Evoluzione nel tempo: dall'arte al gaming

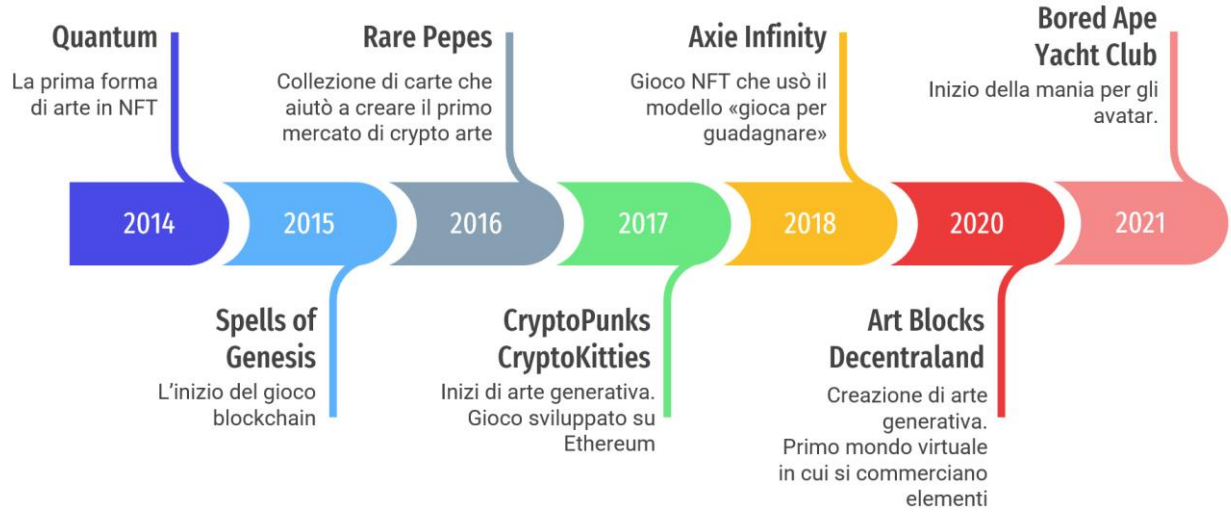

Figura 35: Linea del tempo sull'evoluzione degli NFT.

CryptoKitties

CryptoKitties fu creato da uno studio canadese chiamato *Dapper Labs* e fu poi lanciato nel novembre 2017. Il mese successivo alla creazione, la rete *Ethereum* fu notevolmente rallentata dall'alto numero di transazioni svolte in essa.

Il sito web dei *CryptoKitties* presenta quattro tipologie principali di gatti: normali, di fantasia, edizione speciale ed esclusiva. I gatti normali sono composti semplicemente in base alla loro genetica, quelli di fantasia si distinguono essendo un'opera d'arte e aventi caratteri unici.

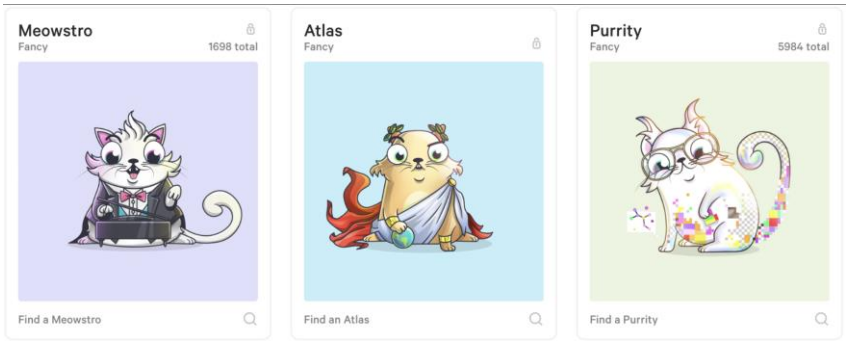

Figura 36: Tre diversi gatti di fantasia.

I gatti esclusivi sono simili a quelli di fantasia con l'unica differenza di essere molti più rari, potrebbe esserci solo un gatto per ogni tipo. Questa categoria è usata specialmente in occasione di eventi, per questo non vi è possibilità di allevamento.

Figura 37: Cathena #500000, gatto esclusivo.

I gatti edizione speciale sono opere d'arte che vengono rilasciate per la vendita in quantità limitata maggiore rispetto ai gatti esclusivi. Per alcuni di loro c'è la possibilità di essere allevati, mentre per altri non è possibile.

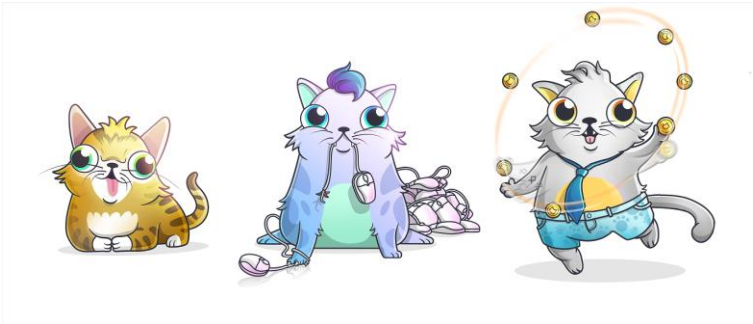

Figura 38: Lil BUB, Purremy Allaire, Catzy.

CryptoKitties opera sulla rete *blockchain* di *Ethereum*. Ogni crypto gatto ha un valore diverso, come per i *cryptopunks*, più la rarità dell'NFT è alta e più sarà alto il suo prezzo poiché ci sarà una grande domanda, meno raro è il token e minore ne sarà la domanda e il conseguente prezzo.

Ogni *cryptokitty* è unico e non trasferibile ad altri, poiché dopo la validazione sulla *blockchain* esso appartiene solo al proprietario. È possibile per gli utenti soltanto acquistare gli NFT, venderli o allevarli. Dopo l'acquisto, il proprietario può far riprodurre due dei suoi *cryptokitties*, il gattino terzo sarà unico secondo il suo fenotipo ma possederà quei geni immutabili derivati dai genitori, ovvero il cosiddetto genotipo. Questo può avvenire un'infinità di volte, ma dopo ogni riproduzione il periodo di recupero del crypto gatto diventa sempre più lungo da un minuto a una settimana o più e fa perdere il valore dell'NFT.

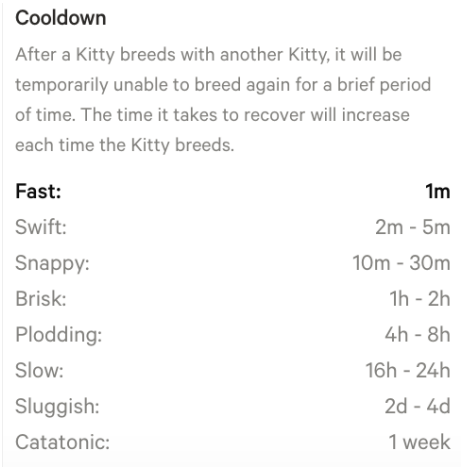

Figura 39: Periodo di recupero del gatto dopo la riproduzione.

La velocità del riposo è anche data dall'appartenenza del gatto a una determinata generazione, più è basso il numero della generazione, più veloce sarà il riposo.

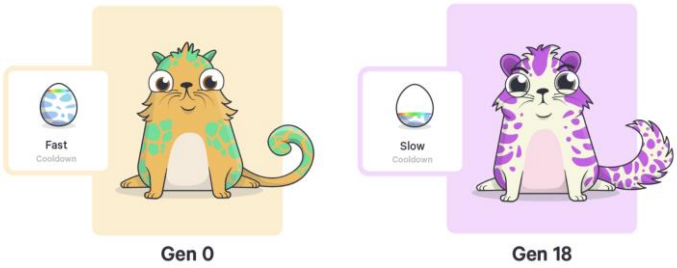

Figura 40: Velocità di riposo in base alla generazione.

Secondo il fenotipo, che limita il numero dei possibili gatti, ci possono essere 4 miliardi di possibili combinazioni di design per i *cryptokitties* derivate da un genoma a 256 bit.

I *miners* della *blockchain* controllano il processo e lo verificano, per questo motivo si deve pagare attraverso due possibili processi il *gas* ai *miners*. Può essere effettuata una transazione standard, la quale più veloce o un trasferimento a basso costo di una durata di 30 minuti. Il costo di ogni transazione è variabile, dipende dal volume, la capacità di estrazione della rete e il momento in cui viene svolta. Normalmente essa costa circa 12/13 centesimi, ma il prezzo può aumentare nei periodi di maggior volume.

Nel 2017 il volume aumentò improvvisamente e di conseguenza anche il costo delle transazioni, questo portò a un accumulo e a delle transazioni in sospeso, ci vollero alcuni mesi prima che i prezzi tornassero normali, poiché i *miners* installavano nuove capacità per far fronte agli elevati costi.

Ci sono due modalità secondo le quali si possono creare *cryptokitties*, al momento del lancio, furono rilasciati 50.000 gatti ogni 15 minuti denominati Gen 0 o anche il gatto dell'orologio e venduti ad un'asta. Durante lo stesso anno i numeri dei gatti creati furono 34.928, poi coniati altri 3.087 e infine 12.000 rimanenti, questi ultimi tenuti per poter essere poi rilasciati in occasioni speciali. I gatti della gen 0 hanno un alto valore dato dall'impossibilità di essere creati attraverso l'allevamento.

Nel maggio 2018 fu lanciato il primo *cryptokitty* dedicato ad una celebrità del basket, ovvero Steph Curry.

Figura 41: Steph Curry CryptoKitty.

Questo fu soltanto l'inizio di quello che era l'intento principale, ovvero allargare la possibilità di avere dei token brandizzati, che vanno oltre i semplici gatti creati fino ad allora. Lo scopo era anche un altro, quello di far conoscere queste nuove tecnologie a un pubblico non più composto di soli esperti.

Tuttavia, durante il 2019 e gli inizi del 2020 il volume medio dei *cryptokitties* è crollato del tutto, verso la fine del 2020 e gli inizi del 2021 fu registrata un'attività regolare di transazioni secondo cui ogni gatto veniva venduto alla cifra di circa 100 dollari ciascuno.

Axie Infinity

Axie infinity è incluso nei giochi *play-to-earn,* 'P2E', fu lanciato nel marzo del 2018 dai suoi tre creatori Trung Thanh Nguyen, Aleksander Leonard Larsen e Jeffrey Zirlin.

Axie Infinity è un mondo virtuale, dà la possibilità di collezionare delle creature dall'aspetto feroce, chiamate *Axie*, i giocatori ne possiedono la proprietà e possono quindi acquistarle, venderle o scambiarle. Per alcuni rappresentano

semplicemente delle carte fisiche collezionabili, per altri, oggetti da collazione. All'interno del gioco agli utenti verranno date diverse opportunità, come: completare missioni, sconfiggere boss, competere tra di loro per arrivare a un livello alto nella classifica, ma anche giocare ai giochi all'interno di questo mondo.

Ci sono infinite combinazioni di Axie, ognuna possiede un codice genetico unico che corrisponde a delle diverse parti del corpo.

Figura 42: Alcuni Axie con i propri codici.

I giocatori sono in grado di avanzare nel gioco grazie a cinque possibilità:

- Collezionare gli Axie più rari;
- Allevare gli Axie e produrne di nuovi cercando di creare combinazioni corporee molto particolari;
- Competere in battaglie con altri utenti per ricevere premi e il token *Smooth Love Potions*;
- Accogliere i nuovi arrivati in questo mondo.

Tutt'oggi sono stati spesi da parte dei giocatori più di 1 milione di *ETH* all'interno di questo mondo virtuale e corrispondono a circa 4 miliardi di dollari.

Il gioco è estremamente attrattivo per i suoi futuri utenti, grazie alla caratteristica di essere un gioco *play-to-earn*, fornisce la possibilità di giocare e guadagnare soldi veri, criptovalute, non monete fittizie. L'emissione del gioco rappresenta solo il 20% della fornitura del *governance token Axie Infinity Shards*. Basato sulla tecnologia *blockchain*, ha più di 1 milione di giocatori attivi giornalmente premiando il completamento delle loro missioni giornaliere con *token SLP*, o *Smooth Love Potion*, che rappresenta la fonte principale di reddito per i giocatori che possono scambiare con altre criptovalute. Un'altra fonte di guadagno è rappresentata dalla vendita degli *Axie* in cambio di *Ethereum* come *NFT*, tramite *l'Axie Infinity Marketplace*.

Inizialmente *Axie Infinity* è stato costruito sulla rete *Ethereum* per l'elevato numero di sviluppatori che costruivano sulla piattaforma e la quantità di membri che la *community* accoglieva quindi gli *Axies* erano token *ERC-721*, mentre le sue due criptovalute *AXS* e *SLP* erano *token ERC-20*, tuttavia successivamente fu sviluppata una *sidechain* compatibile con *Ethereum* per poter ospitare il gioco, denominata *Ronin*, lo spostamento del gioco avvenne 3 anni dopo nel 2021 e fu completo, ovvero tutt'oggi è possibile comprare *Axies* e allevarli soltanto sulla loro *sidechain,* questo passaggio avvenne per la problematica della scalabilità presentata da *Ethereum* che avrebbe dato al team problemi futuri.

Tutti gli elementi all'interno del gioco sono NFTs collazionabili, *axie*, terreni e oggetti vari con la possibilità di rivenderli sul mercato del gioco, ma per poter comprare dal mercato bisogna possedere un *Ronin wallet*.

Sul sito di *Axie* si afferma di aver provveduto alla migrazione di chain poiché i costi delle transazioni applicati su *Ethereum* era in constante crescita, quindi la permanenza iniziale sulla piattaforma ha garantito il suo lancio, tuttavia per poter crescere è stato necessario questo cambiamento.

"Ronin is bringing economic freedom to an entirely new generation of Axie players by streamlining user experience and reducing the burden of expensive gas fees"[56]

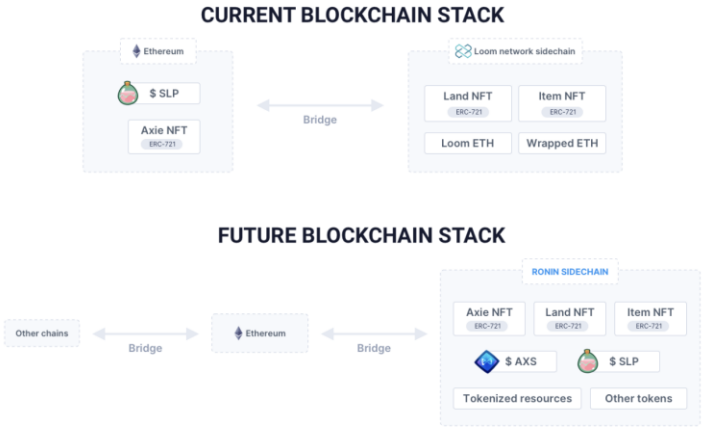

Figura 43: La blockchain al momento e quella futura.

[56] "Ronin sta portando la libertà economica a una generazione completamente nuova di giocatori Axie semplificando l'esperienza utente e riducendo l'onere delle costose tariffe del gas" – (https://axie.substack.com/p/migration)

Uno dei due token presenti sul gioco è *Axie Infinity Shards*, o AXS, un token di *governance* ERC-20 con la possibilità di essere richiesto dai giocatori giocando o partecipando a delle importanti votazioni.

Quello che i creatori cercarono di fare tramite i tokens fu di incentivare ed entusiasmare i giocatori attuali e futuri, lo fecero per portare avanti due obiettivi:

- La decentralizzazione della proprietà e della governance di *Axie Infinity*;
- Incentivazione degli utenti a conservare le due tipologie di tokens e premiando il raggiungimento di obiettivi;

In quanto alla decentralizzazione fu portato avanti per anni come progetto, con la visione di poter avere una community, definita *Treasury*, che riceverà i ricavi del gioco. Questi ricavi provengono per il 4.25% dalle transazioni avvenute sul mercato *Axie* e una parte, invece, dalla quota per l'allevamento di *Axie*, futuri influssi verranno poi da altre transazioni aggiunte in seguito.

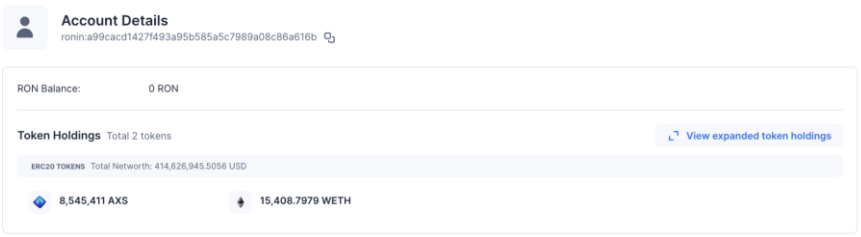

Figura 44: La Community Treasury sulla piattaforma Ronin.

Nel luglio dell'anno di rilascio il token aumentò oltre l'800%, possedendo una fornitura di 270 milioni con una schedule di allocazione e sblocco predeterminata con un'iniziale fornitura di 59.985.000 di AXS, il 22.22% della fornitura totale. Come si può vedere dal grafico successivo l'emissione di AXS non eccede i 270.000.000.

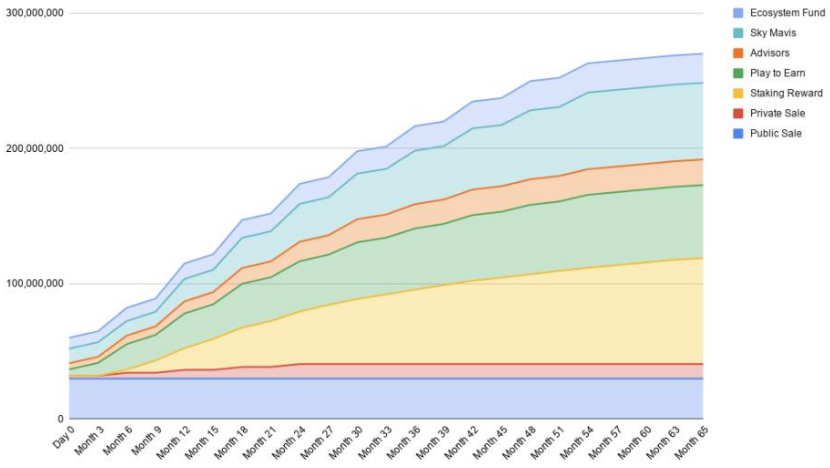

Figura 45: Axie Infinity grafico della durata di 65 mesi.

Oltre all'obiettivo di rendere il gioco un *DAO*, il team sta sviluppando *Lunacia SDK*, che inizialmente sarà un editor di mappe dove gli utenti saranno in grado di creare nuovi giochi che poi saranno salvate come *NFT* e possono essere scambiati.

Decentraland

Decentraland è stata co-fondata da Ari Meilich ed Esteban Ordano dal 2015, per poter creare un mondo tenuto da utenti, aperto al pubblico nel 2020.

Figura 46: Decentraland.

È una piattaforma basata su browser del mondo virtuale in 3D, agli utenti viene data la possibilità di comprare con la criptovaluta MANA, appezzamenti NFT di terreni. Questo mondo è proprietà degli utenti, poiché possono creare e monetizzare su contenuti creati da loro stessi. Un esempio può essere fornito dai designer, i quali hanno la possibilità di creare e vendere i loro vestiti sulla piattaforma.

I tipi di terreni sulla piattaforma sono due:

- Lotti o LAND, in totale 90.601 di misura 16x16 m, acquistati e venduti sul mercato e utili per la costruzione di distretti;
- Distretti, più appezzamenti di terreno uniti e creati da chiunque, utilizzati per ospitare eventi, negozi e creare giochi.

Il distretto più grande nel gennaio 2021 è stato rappresentato dal distretto *Aetheria* con tema *cyberpunk*, comprensivo di 8.008 LAND.

Questo mondo possiede una propria criptovaluta chiamata MANA, utilizzata per l'acquisto di terreni o in generale di servizi e beni, una volta acquistati vengono memorizzati sulla *blockchain*.

MANA è utilizzato anche per molte altre azioni, quali: apertura di un *wallet*, investimenti di proprietà, guadagno di soldi, ottenimento di un mutuo e per la sua *governance*. Coloro che possiedono MANA hanno controllo decisionale sul mondo virtuale e sui futuri aggiornamenti per il suo sistema di organizzazione autonoma decentralizzata o DAO. Il *token* della piattaforma può essere acquistato, venduto o scambiato su 100 piattaforme diverse, poiché gode di una liquidità alta, alcune di queste sono *OKEx*, *Coinbase Pro* e *Binance*, può essere anche scambiata con *Bitcoin*, *Tether* e *Ethereum*, acquistata con un alto ventaglio di valute legali. Il valore odierno del token risulta essere 0,606552 EUR con un volume di trading in 24 ore di 122.429.652 EUR.

Figura 47: Prezzo del MANA il giorno 27/01/2023.

La piattaforma è costruita sulla *blockchain* di *Ethereum*, utilizzando i *token ERC-20* e i *smart contracts*, essendo così un gioco immutabile. La funzionalità di *Decentraland* è data dal suo protocollo decentralizzato, *Decentraland Network*, in

grado di gestire utenti e applicazioni. Al suo interno possiede un sistema di chat integrato in modo tale da far comunicare tra loro gli utenti e un sistema di aste fondiarie per offerte all'acquisto degli appezzamenti di terreno, ci sono anche varie applicazioni come un motore di gioco, strumento di modellazione 3D e un *software development kit* o SDK che danno libero spazio all'utente di creare le proprie esperienze.

Bored Ape Yatch Club

Bored Ape Yatch Club o BAYC fu fondato da quattro persone che inizialmente utilizzarono due pseudonimi: Gordon Goner e Gargamel, No Sass ed Emperor Tomato Ketchup. Un anno dopo i loro veri nomi vennero resi pubblici. BAYC fu sviluppato ad aprile 2021 da *Yuga Labs* creato da loro per realizzare arte digitale su *blockchain* e poi lanciato nel 2021, si tratta di una raccolta di 10.000 NFT raffiguranti scimmie con lo stile dei cartoni animanti, posizionate sulla *blockchain* di *Ethereum*.

La creazione delle scimmie avviene tramite la scelta randomizzata e la combinazione di 170 caratteristiche, quali possono essere i cappelli o i vestiti. Perché proprio le scimmie? Perché nel mondo delle crypto, le scimmie sono animali comuni e anche i *trader* si riferiscono l'uno l'altro con il termine *ape*, l'inglese di scimmia, e si ricollega anche ai *Cryptopunks* in cui sono presenti scimmie e sono considerate uno degli NFT più rari.

Al lancio il costo di ogni *token* era di 0,08 ETH corrispondenti a 220$, non avendo molto successo poiché furono venduti in 12 ore e circa 650 NFT, mentre un anno dopo il costo aumentò fino ad arrivare a un minimo di 76 ETH = 100.418$, molte più persone, comprese quelle più ricce cominciarono a possederne almeno uno, come Steve Aoki o Josh Hart.

Ci sono vari motivi secondo i quali una collezione può essere di successo, quelli generali sono quattro:

- L'utilità che i token possono avere per i membri;
- Quanto i tokens sono attrattivi per la comunità;
- La popolarità acquisita sulle varie piattaforme;

- Il coinvolgimento di celebrità di alto livello, come il token della foto successiva, acquistato da Eminem per più di 450 mila dollari.

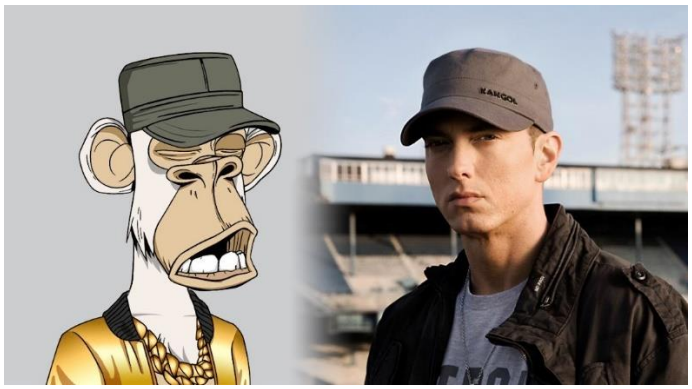

Figura 48: Scimmia NFT di Eminem.

Figura 49: Adidas con BAYC.

Questo stesso gruppo lanciò anche *Bored Ape Kennel Club*, rappresentante cani e *Mutant Ape Yatch Club,* quest'ultimo con scimmie mutanti ebbe un gran successo già nel lancio, avendo un *sold out* in un'ora e una somma di circa 96 milioni di dollari, ogni proprietario di *ape* ricevette un siero per poter mutare la sua scimmia con tratti geneticamente modificati.

La collezione è diventata ad oggi uno *status symbol*, ovvero qualcosa che le persone sono disposte a pagare molti soldi per averne uno e che utilizzano come immagini del profilo su vari *social media*, specialmente *Twitter,* essendo visibili a una grande quantità di persone, non solo gli appassionati.

Con lo sviluppo delle altre due collezioni, viene anche sviluppata una propria moneta utile per acquistare dal mercato, definita *Apecoin,* amministrata dalla fondazione APE. *Apecoin* è la valuta principale e si tratta di un *token governance* che dà la possibilità ai possessori di partecipare ad *Apecoin DAO*, con protocollo ERC-20 usato per migliorare la comunità decentralizzata IPFS, ci sono 1 miliardo di token sul mercato, di cui una parte sarà bloccata all'inizio, poi verranno sbloccati per un periodo di 48 mesi.

La fondazione facilita la governance decentralizzata, migliorandola con il tempo così da creare e gestire una community globale.

La particolarità di BAYC è rappresentata dalle utilità. I proprietari dei tokens hanno accesso a un esclusivo gruppo *Discord* privato in cui possono chattare, creano una rete con altri possessori di NFT e l'accesso comprende anche quello di *The Bathroom*, una sorta di muro virtuale del bagno, su cui ogni 15 minuti è possibile disegnare. Nell'aprile del 2022 l'account Discord e Instagram fu hackerato tramite l'invio di un link *mint*, il quale ha compromesso i portafogli di coloro che vi hanno cliccato sopra, sono state rubate circa 54 scimmie cui valore ammonta a circa 13,7 milioni di dollari.

VeeFriends

La creazione di *VeeFriends* è abbastanza recente, risale al maggio del 2021 grazie a GaryVee e possono essere acquistati in mercati di terze parti come *OpenSea*, poiché tutti gli NFT originali sono stati venduti. La prima serie si tratta di un set di 1,242 tokens chiamato G.O.O., *Gary Originally Owned*, ogni token possiede un personaggio dei 268 disegnati da Vaynerchuk.

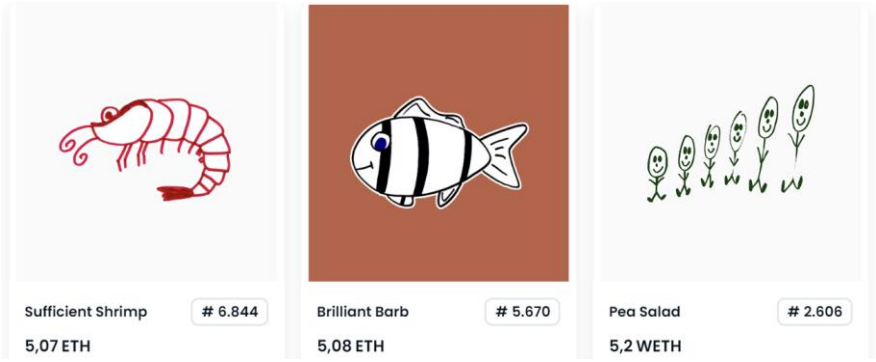

Figura 50: Series 1 dei VeeFriends.

I prodotti fisici *VeeFriends* possiedono un codice QR e se scannerizzato si collegherà a film animati in 3D e a canzoni associate al rispettivo personaggio, rivelando la sua vera storia personale. Si tratta di una collaborazione tra *VeeFriends* e *Macy*.

GaryVee annunciò successivamente l'uscita del *Book Games*, legato all'ecosistema dei *VeeFriends* e dava in cambio dei premi agli acquirenti. Si tratta di un secondo livello di NFT, ovvero si riferisce alle soluzioni *blockchain* progettate per ridurre le applicazioni e distaccandole dalla rete principale, possono essere utilizzati 125.000 token per giocarvi. Il creatore decise di utilizzare *Immutable X* come secondo livello così da minimizzare le quote delle transazioni o del gas.

Successivamente a *Book Games*, venne lanciato il *VeeFriends Mini Drops*, consistette in una sotto-raccolta di *VeeFriends* limitati, i primi 31 ad essere stati creati erano ispirati ad Halloween e per questo motivo furono stati caricati sulla piattaforma quello stesso giorno.

I possessori di questi nuovi NFT hanno avuto il privilegio di entrare a far parte della *community* e di poter partecipare alla prima conferenza definita 'super conferenza' e a quelle successive. Questa prima conferenza era accessibile solo a coloro che erano in possesso di un *VeeCon* NFT e ospitò anche molte celebrità.

Nell'aprile del 2022, l'artista lanciò la seconda serie dei *VeeFriends* dividendo l'uscita dei token in varie giornate durante l'intero mese. Il 12 aprile alcuni dei possessori del *Book Games* furono inseriti randomicamente nella *whitelist*, ovvero le liste di amici, avendo la possibilità di coniare i 32.000 NFT della serie 2 messi a disposizione e quei NFT che non vengono coniati in questa fase, saranno aggiunti all'ammontare dei token non fungibili disponibili per il pubblico, quindi di base 10.000.

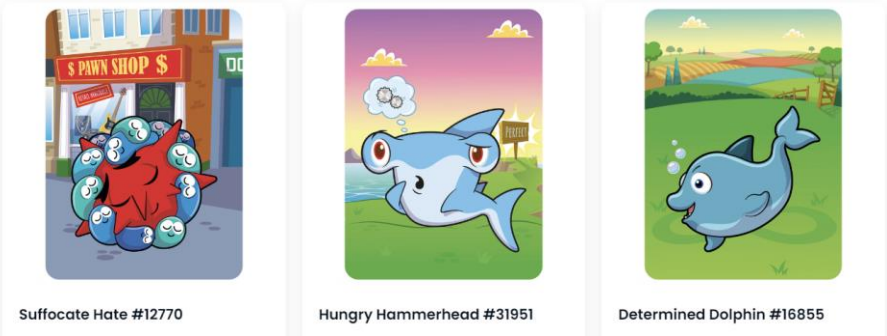

Figura 51: Serie 2 dei VeeFriends.

A differenza della prima serie, questa non garantisce ai possessori l'accesso a *VeeCon*, soltanto dei vantaggi nel sistema *VaynerNFT*. Possono essere acquistati anch'essi sulla piattaforma *OpenSea*.

Beeple

Beeple è il nome d'arte di Mike Winkelmann, un artista digitale del sud carolina. L'artista seguì con interesse l'esplosione nel 2020 della nuova forma d'arte chiamata NFT, avendo esperienza pregressa nel mondo dell'arte digitale e avendo un numeroso seguito sui vari social media, decise di dare una nuova immagine alle sue opere d'arte e così alla fine dell'anno 2020, *Beeple* rilasciò sulla piattaforma *Nifty Gateway*[57] il suo primo NFT, un disegno di carattere politico creato appositamente per lo scontro elettorale tra Trump e Biden denominato '*Crossroads'*. La prima vendita consisteva in tre pezzi separati di arte e ognuno di questi aveva al suo interno 100 opere, così da avere in totale 300 opere d'arte. Il prezzo stabilito dall'artista era estremamente basso e ammontava a 1 $ poiché il profitto non era il suo obiettivo finale, ciò che gli interessava era il valore di rivendita, infatti mesi dopo queste sue prime opere furono rivendute con un valore molto più alto di quello iniziale, ovvero 6 milioni di dollari su cui il creatore possiede circa il 10% della transazione.

[57] Nifty Gateway: una piattaforma di proprietà dei gemelli Winkelvoss, consiste in un mercato d'arte NFT online in cui avviene il conio e la vendita di opere digitali.

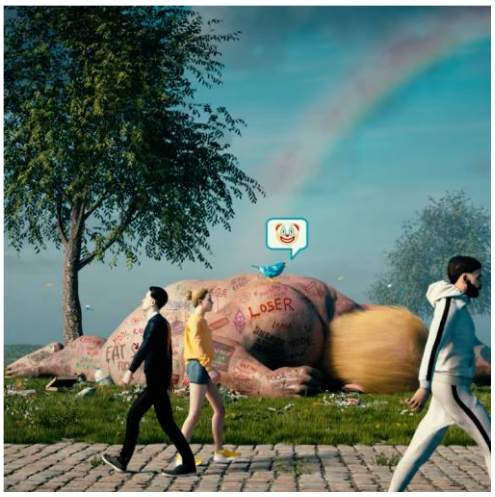

Figura 52: "Crossroads" di Beeple.

Nel secondo lancio avvenuto a dicembre dello stesso anno, l'artista non diede un prezzo stabilito a '*The Complete MF Collection*', ma permise ai possibili acquirenti di fare delle offerte, alla fine il prezzo di vendita fu all'incirca 777,777 $ con un guadagno dell'asta dell'ammontare di circa 3,5 milioni di dollari.

Nell'anno successivo, in una delle case d'asta Christie's venne esposto, con un prezzo di partenza pari a 100 dollari, un'opera come NFT di *Beeple* denominata '*Everydays: the First 5000 Days*' e le offerte si prolungarono per la durata di sue settimane per poi vendere l'opera a più di 69 milioni di dollari. Quest'opera consiste in una collezione dei suoi disegni creati dall'artista ogni giorno sperimentando stili di disegno diversi l'uno dall'altro, dallo stile psichedelico a quello di figure sproporzionate.

Figura 53: Opera "Everydays: The First 5000 Days" di Beeple.

2.2 Uso corrente degli NFTs

Gli NFTs in poco tempo sono diventati molto popolari, non solo nell'ambito dell'arte e del gaming come descritto precedentemente, ma anche nello sport, infatti è possibile collezionare oggetti e cimeli sportivi sottoforma di NFT. Nel 2021, fu venduto sulla piattaforma della NBA chiamata *Top Shot*[58], LeBron James NFT a una cifra di $208.000.

Figura 54: Video di LeBron James come NFT.

Questo nuovo mercato non riguarda soltanto i fan, ma è anche un modo per gli atleti di avere altri flussi di entrate mettendo in vendita contenuti esclusivi, quali possono essere dei video NFT delle loro sessioni di allenamento, incuriosiscono i loro fan e gli danno modo di creare una connessione non tradizionale. Più atleti con il tempo stanno sperimentando questa nuova tecnologia, ma anche organizzazioni come *National Football League* e *Major Basketball League*. Gli NFT sono utilizzati anche per cause di beneficienza, infatti per quando riguarda lo sport, nell'aprile del 2021, l'associazione giocatori NFL fece una collaborazione con una piattaforma *blockchain* per poter raccogliere fondi e donarli in

[58] Top Shot: piattaforma che consente ai fan di acquistare, scambiare e vendere oggetti da collezione NBA con la licenza ufficiale sotto forma di NFT.

beneficienza. La raccolta dei fondi avviene tramite l'asta di oggetti da collezione, arte o biglietti per eventi virtuali o altre risorse per questo scopo ci sono state anche collaborazioni artistiche, come quella nel maggio 2021, che vede l'uscita dell'album dei *Kings of Leon* di cui una parte del ricavato veniva donata a un'associazione senza scopo di lucro che sostiene i locali di musica dal vivo colpiti dalla pandemia del COVID-19.

Questa nuova risorsa sta cominciando a essere usata anche il settore della musica per monetizzare e lo mette in atto attraverso il rilascio di risorse digitali esclusive, quali possono essere brani musicali o album, in quantità limitate o per un periodo di tempo limitato. Tra queste risorse vengono inclusi anche i biglietti per concerti, *pass* per il *backstage* o messaggi diretti da parte dell'artista a un determinato fan, tutto ciò crea un filo connettore tra artista-fan così da rendere quest'ultimo più coinvolto nella vita dell'autore. Dal lato del creatore, gli NFT possono essere utilizzati per la gestione dei diritti di proprietà per brani musicali e album, così da non dover assumere intermediari come etichette discografiche per la vendita della propria musica.

Gli NFT compaiono anche nelle piattaforme social offrendo un nuovo modo di monetizzazione, dal vendere arte digitale e collezionabili, alla rappresentazione di immobiliare virtuale e al sistema di ricompensa, quest'ultimo consiste nel guadagno di NFT da parte di utenti dopo aver svolto attività nell'interazione con i contenuti. Un esempio di questa categoria può essere rappresentato dalla vendita da parte del CEO Jack Dorsey del suo primo tweet come NFT alla cifra di 2.9 milioni di dollari.

2.2.1 Distribuzione di opere d'arte digitali

Le opere digitali possono essere divulgate attraverso l'uso di varie piattaforme online quali mercati, social media e piattaforme basate su *blockchain*.

In quanto a mercati di NFT, ovvero dove viene permesso ai creatori di coniare i propri NFT per la vendita dando la possibilità agli acquirenti di acquistarli tramite criptovaluta. Alcuni di questi sono:

- *OpenSea*, la più ampia piattaforma creata nel 2017, che ospita 2.4 milioni di utenti attivi con il suo pieno controllo e accesso ai portafogli di criptovaluta, il volume di vendite giornaliere è pari a 6.03 milioni di dollari e permette la

creazione, la vendita e/o l'acquisto di vari NFT, quali arte, collezionabili, lotti virtuali, musica o risorse sportive. *OpenSea* venne costruito su un protocollo open-source che alimenta lo scambio peer-to-peer delle risorse digitali, chiamato protocollo *Wyvern* operante come una serie di contratti intelligenti sulla *blockchain* di *Ethereum*, quindi oltre ad utilizzare i standard ERC-721 e ERC-1155, vennero integrati anche Solana e Polygon. L'interfaccia usata da questa piattaforma è molto intuitiva e adatta ai principianti, il primo passo da eseguire è la creazione, se non lo si possiede, e la seguente connessione del portafoglio *crypto* a *OpenSea* per permettere l'inizio delle transazioni, quindi per pagamenti e ricevere depositi. Una caratteristica della piattaforma è quella di *noncustodial* ovvero non custodita, quindi tutti gli NFT caricati dal creatore non vengono archiviati su di essa, ma vengono inviati all'indirizzo del portafoglio. Vi sono vari *crypto wallets* supportati da *OpenSea*: *MetaMask*, *Portis*, *Bitski*, *Coinbase Wallet*, *Phantom*, *Opera Touch* per mobile, *Glow*, *Torus*, *Dapper*, *Trust Wallet*, *Authereum*, *Venly*, *Fortmatic*/*Magic* e *Kaikas*. Per tutta questa lista il processo di connessione alla piattaforma è lo stesso e una volta svolto, si possono vedere tutti gli NFTs posseduti, tramite la pagina dell'account, mentre per poter visualizzare tutti gli NFTs disponibili sulla piattaforma, si accederà alla pagina esplora o a statistica, quest'ultima sarà provvista di caratteristiche analitiche, quali filtri per il tempo che di default è su 24 ore, categoria, volume o schede di blockchain. Quando si vuole comprare un NFT e viene già scelto, verrà aperta una pagina sulle informazioni riguardanti quel determinato NFT o collezione, andando poi nella sezione elementi, sarà possibile visualizzare informazioni riguardo le offerte, trasferimenti, vendite e listini, per ristringere il campo di ricerca si può far uso dei quattro filtri posseduti da questa sessione, quali: compra ora, ha offerte ovvero gli NFTs con le ultime offerte, all'asta e nuovo in cui vengono visualizzati solo i nuovi NFT rispetto ai vecchi.

- *Rarible o RARI* consiste in una piattaforma che permette la creazione, la vendita e l'acquisto della proprietà di risorse digitali come NFT, basata sulla *blockchain* di *Ethereum*, quindi fa uso dei due standard noti, ERC-721 e ERC-1155, il primo per la creazione di elementi unici mentre il secondo per la creazione di collezioni. I portafogli utilizzati da questa piattaforma sono

quelli basati su *Ethereum*, dopo averlo collegato si può cominciare a cercare sulla piattaforma risorse digitali da acquistare che secondo la scelta del loro creatore possono avere un presso fisso o appartenere ad un'asta. *Rarible* può essere usata dal creatore di opere d'arte per coniare i propri NFTs semplicemente per archiviarli o per venderli, tuttavia questo processo richiede due tipi di *fees* che non saranno tenute dalla piattaforma ma servono per permetterle di interagire con la blockchain, la prima per il conio, quindi per concedere il permesso al portafoglio di interagire con *Rarible* e l'altra per chiamare la funzione *mint* che si occuperà d'inserire il file nel sistema dell'*InterPlanetary File*, *IPFS*, e nella blockchain di *Ethereum*. Quando un artista vende le sue opere su questa piattaforma ne raccoglie direttamente i proventi anche dopo la prima vendita ed è possibile visualizzare i propri NFTs anche su *OpenSea*, poiché *Rarible* è stato integrato con essa.

- *SuperRare* consiste in un mercato di criptovalute, in cui vengono mostrate delle serie di opere d'arte digitale, come la maggior parte di questo tipo di piattaforme, è nata come una piattaforma centralizzata con al controllo un gruppo di persone incaricate di controllare opere e artisti, però con il tempo e precisamente nel 2021 fu introdotto il token governance specifico della piattaforma chiamato *RARE*, così da diventare una DAO comprendente di una community. Viene considerata una piattaforma esclusiva, poiché la sua attenzione principale riguarda la qualità di sole opere d'arte rispetto che la quantità, per questo viene considerata quasi una piattaforma di élite. Le opere che possono essere visualizzate su questa piattaforma comprendono una varia gamma di stili artistici, dall'arte psichedelica a illustrazioni. La piattaforma gode di alcuni tra i più importanti investitori come Mark Cuban, Ashton Kutcher e Samsung Next.
- *Nifty Gateway*, anche in questo caso si tratta di una piattaforma online su cui è possibili comprare, vendere e scambiare NFTs, fondata nel 2018 da Duncan e Griffin Cock Foster, ed è stata acquisita nell'anno successivo dai Winklevoss twins. La piattaforma pubblicizza e acquisisce opere digitali appartenenti alla fascia alta e le collezioni ben curate, per questo speso vengono instaurate partnership e rilasciate collezioni limitate con vari artisti come: Beeple, Refik Anadol, Pak e Daniel Arsham. *Nifty Gateway* si

differenzia dagli altri mercati per le sue caratteristiche differenti, tra le quali ci sono: opzione custodiale, ciò vuol dire che viene utilizzato un portafoglio omnibus o un conto di deposito principale in cui vengono spostati gli NFT sulla piattaforma senza l'elaborazione delle transazioni sulla blockchain, ciò porta alla mancanza delle commissioni sul gas, il vantaggio nell'uso di quest'opzione è la garanzia dell'intervento della piattaforma nel caso in cui un utente perda l'accesso e consente ai trader di poter effettuare il pagamento tramite svariati metodi, quali carte di credito o debito, ETH presenti sul portafoglio. Un'altra opzione offerta da *Nifty Gateway* è il *wallet 2 wallet*, *w2w*, che garantisce agli utenti di acquistare e vendere NFT in ETH direttamente dai portafogli crittografici esterni, però ciò avviene sulla blockchain, quindi bisogna aggiungere le commissioni per il gas, invece quest'ultime sono coperte completamente dalla piattaforma durante il conio di un NFT. Tutti i nuovi NFT prima di essere venduti passano per un processo di verifica da parte del team, essendo un mercato centralizzato.

2.2.2 Processo di creazione e vendita di NFT

Come primo passo bisogna capire quale tipologia di *token non-fungibile* si vuole creare e successivamente vendere, che sia arte digitale, video o foto, e se si vuole creare *collectables* oppure singoli NFTs. Una volta deciso, si passa alle fasi effettive:

1. Decidere il marketplace più adatto al progetto, uno tra questi è *OpenSea*[59] fornito di strumenti intuitivi per creare NFT e scelto per la maggior parte da principianti poiché possiede un ampio pubblico. La scelta del marketplace non è un passaggio obbligatorio, poiché se si ha conoscenza approfondita degli *smart contracts*, si può scrivere il proprio, caricarlo sulla blockchain e usarlo per il *minting*[60].

2. Creazione del portafoglio *crypto*: il *wallet crypto*[61] decentralizzato o anche portafoglio digitale, gestisce tutto quello che riguarda scambi e saldo del proprietario. Permette di effettuare i pagamenti utilizzando la crittografia,

[59] OpenSea: la più grande piattaforma online per vendere, comprare e scambiare varie tipologie di NFT, usando protocolli aperti come Ethereum e standard come ERC-721 e ERC-1155.
[60] Minting: il processo di conio di nuovi token utilizzando il metodo Proof-of-Stake.
[61] Walet crypto: un portafoglio digitale riservato alle criptovalute.

nello specifico tre codici generati alla creazione del portafoglio: chiave privata, pubblica e l'indirizzo. Un portafoglio corrisponde a un indirizzo della *blockchain*, indicante il luogo in cui sono posizionati i dati sulle criptovalute.
La chiave pubblica e quella privata consistono in una serie di lettere e numeri. Quella privata funziona come se fosse una password e farà aprire il *wallet* solo se viene usata la combinazione giusta, questo rende importante che rimanga segreta. Mentre, la chiave pubblica deve essere resa pubblica così da poter ricevere criptovalute.
Esistono diverse categorie di portafogli per criptovalute:

- *Wallet non custodial*, adibisce al proprietario il controllo dei fondi e l'utente dovrà ricordarsi le chiavi private.
- *Wallet custodial*, detto *hosted* perché ospitato da piattaforme online affidando a terze parti la conservazione delle chiavi.
- *Hot wallet*, consiste di software online che permettono di eseguire transazioni in maniera veloce e con facilità d'uso.
- *Cold wallet*, consiste in dispositivi fisici e offline, non avendo accesso a internet rallenta il processo, ma al contrario li rende più sicuri poiché non esposti ad attacchi hacker.
- *Hardware wallet*, si tratta di dispositivi fisici che conservano le chiavi private offline e hanno bisogno di un software installato nella periferica.
- *Paper wallet*, sono fogli di carta con scritto gli indirizzi e chiavi private, anche sottoforma di QR code.
- *Software wallet*, consiste in un programma per computer, smartphone o browser connesso a Internet.

Dopo la creazione del portafoglio, bisogna associarlo a *OpenSea* e creare l'account.

3. Scelta della blockchain per la creazione dell'NFT. Ci sono varie *blockchain* con caratteristiche differenti e costi di *gas* per transazioni diverse, tra le

tante, le più conosciute sono *Ethereum*, *Polygon*[62], *Solana*[63], *Arbitrum*[64] e *Optimism*[65].

4. Caricamento dell'opera d'arte: gli NFT che possono essere venduti sono associati a qualsiasi cosa, un disegno, un audio, un'immagine 3D. Quando si crea un nuovo elemento, bisognerà caricare il file dell'opera, il suo nome, la descrizione e un'eventuale collezione in cui sarà presente quel determinato NFT.
5. Scelta del prezzo.
6. Pubblicizzazione dell'opera.

2.3 Vantaggi e svantaggi dell'uso degli NFT

Qualsiasi forma artistica può diventare un token non fungibile, dalle opere d'arte all'immobiliare.

Ma quali sono i vantaggi e i conseguenti svantaggi dell'uso degli NFT?

Primariamente, gli NFT migliorano l'efficienza del mercato poiché la digitalizzazione di una risorsa porta al miglioramento delle catene di approvvigionamento, l'aumento della sicurezza e la riduzione degli intermediari nelle transazioni di scambio-vendita. In quanto all'arte la digitalizzazione delle opere porta l'artista a non dover assumere un agente che faccia da intermediario tra artista-acquirente, ma il creatore dell'opera si rapporta in maniera diretta con il pubblico e i possibili acquirenti, questo fa risparmiare tempo eliminando la fase di "passa parola" e diminuisce l'ammontare dei soldi spesi, permettendo all'artista di vendere una vasta gamma di opere dopo che esse siano state coniate.

Dal lato dell'acquirente invece, la digitalizzazione dell'opera d'arte e il contatto diretto con il creatore, garantisce il processo di verifica. Un altro vantaggio consiste nell'utilizzo del token non fungibili per frazionare la proprietà dei beni fisici che generalmente sono difficili da dividere fisicamente, quali possono essere opere d'arte, gioielli o addirittura immobili, mentre una volta che la risorsa viene

[62] Polygon: consiste in una piattaforma blockchain che consente alle reti blockchain di connettersi e scalare. Mira a creare un ecosistema blockchain multi-catena compatibile con Ethereum.
[63] Solana: una piattaforma blockchain progettata per ospitare applicazioni decentralizzate e scalabili.
[64] Arbitrum: un tipo di tecnologia noto come rollup ottimistico, consente agli smart contracts di Ethereum di ridimensionarsi passando messaggi tra contratti intelligenti sulla catena principale di Ethereum e quelli sulla catena di secondo livello di Arbitrum.
[65] Optimism: è una rete di livello 2, una sorta di bockchain costruita su un'altra blockchain di livello 1, per velocizzare le transazioni e ridurre le commissioni.

digitalizzata, il processo risulta essere più semplice. Alcuni esempi sono *Futurent*, *RealT*, *Labs Group* e *Aqar Chain* che si impegnano nella vendita di immobili frazionati come NFT, ma anche la vendita di un album come NFT da parte della band *Kings of Leon*. La tecnologia alla base degli NFT è la *blockchain* e una delle caratteristiche affidatogli è l'estrema sicurezza poiché non può essere violata, le informazioni non possono essere alterate o eliminate.

Tuttavia, gli NFT possiedono altrettanti svantaggi, tra i quali, essendo ancora nelle loro prime fasi, il settore che li circonda manca di liquidità e sono poco compresi dai possibili acquirenti, quindi il trading può risultare impegnativo da portare a termine e i prezzi possono variare altamente. Possono esistere frodi legate ai token non fungibili, questo non riguarda la sua tecnologia di base, ma gli NFT singoli che possono essere usati per il compimento di frodi, ciò è stato notato da svariati artisti, i quali hanno trovato le proprie opere in vendita su piattaforme come NFT senza però avere il permesso da parte del creatore. Un'altra problematica è rappresentata dalla vendita di una replica contraffatta, ovvero viene eseguita una copia elettronica dell'opera, alla quale vi si allega un token e poi viene caricata su una piattaforma online per venderla, questo token quindi è affidato ad un'opera che non è l'originale, pratica che rende difficile risalire a quale sia l'originale e quale una copia.

Le conseguenze degli NFT possono riscontrarsi nell'ambiente, infatti questi sono dannosi per l'ecosistema. Per poter costruire i registri delle blockchain si ha bisogno di un grande dispendio di energia di computer e ciò a lungo termine può causare problematiche serie per l'ambiente, poiché le emissioni di carbonio per il *mining* delle criptovalute e degli NFT supereranno quelle emesse dalle più grandi città metropolitane.

2.3.1 Considerazioni riguardanti l'etica

Come per la maggior parte delle tecnologie emergenti, anche riguardo gli NFT è necessario prendere in considerazione l'etica, nella quale sono sorte delle problematiche legate alla novità di produzione di arte digitale.

Una delle problematiche principali è legata all'impatto ambientale degli NFT, per quanto riguarda due processi il *minting* e le negoziazioni, le quantità di energia utilizzata sono significative e questo contribuisce alle esponenziali emissioni di

carbonio prodotte che conseguentemente aggravano la problematica del cambiamento climatico. Per limitare ciò alcuni mercati fanno uso di energia rinnovabile, metodi per compensare l'emissione del carbonio prodotta o ancora la possibilità di utilizzare un algoritmo di consenso che sia più vantaggioso dal punto di vista energetico e/o ambientale. Quella legata all'ambiente è un evidente problematica, ma anche una speranza per il futuro, poiché si crede che per risolverla ci si interrogherà e spingerà all'utilizzo di fonti rinnovabili, fornendo finanziamenti a chi non può permetterselo definendo ciò *banking the unbanked* e fornendo anche responsabilità ai fornitori di servizi.

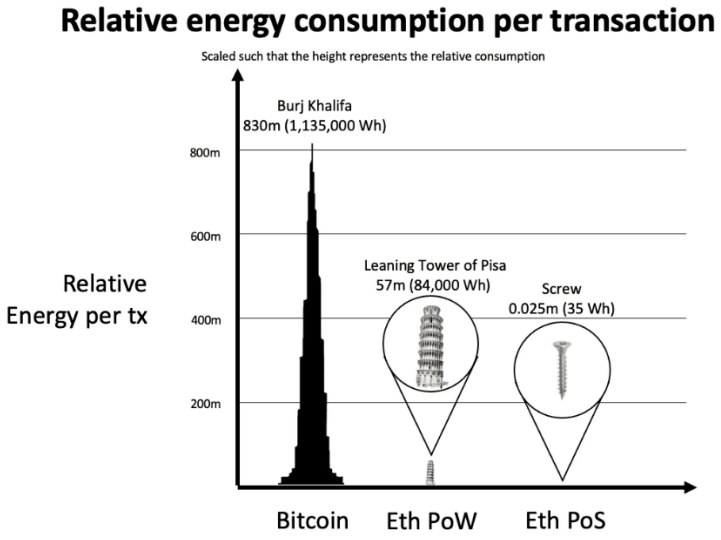

Figura 55: Grafico del consumo di energia di ETH e Bitcoin.[66]

La negoziazione delle criptovalute non causa danni solo all'ambiente, ma anche alle persone stesse, esse possono sentire ansia e stress date dalla volatilità di questo mercato e dall'alta probabilità di perdita dei soldi che posseggono, infatti sono coloro che hanno di partenza grosse quantità di capitale ad arricchirsi e non chi possiede capitale inferiore, per questo non ci sono vantaggi per quanto riguarda il benessere umano. Alcuni progetti NFT donano il 10% dei proventi a beneficienze sulla salute mentale.

Un'altra preoccupazione riguarda la facilità di frode e riciclaggio di soldi tramite gli NFTs, favorite dalle caratteristiche di non rintracciabilità e anonimato delle transazioni eseguite sulla blockchain, quest'ultima le valida solo

[66] https://www.sciencefocus.com/future-technology/can-nfts-solve-their-massive-carbon-footprint-problem/

crittograficamente, infatti non c'è un controllo per verificare che quella determinata transazione sia avvenuta in maniera volontaria. Queste caratteristiche se usate da malintenzionati, possono portare alla vendita di opere rubate o false, senza la possibilità di attuare un ricorso.

Per le persone sembra valere molto la privacy, che nel contesto della *blockchain*, non viene preservata. Tutte le transazioni eseguite sono pubbliche, anche avendo degli pseudonimi, gli autori di queste possono essere facilmente rintracciabili sia perché generalmente sui loro profili vengono pubblicati links rimandanti ai loro social media, sia perché essendo pubbliche sono più propense e facili da attaccare da malintenzionati. Per arginare questa violazione sono state sviluppate delle possibili soluzioni, ma che ad oggi non funzionano per una vasta gamma di dati.

L'etica degli NFT è un argomento complesso e in continuo movimento poiché il suo mercato è in continua crescita, con l'arrivo di sempre nuove problematiche su proprietà, autenticità, impatto ambientale e numerosi altri argomenti.

3. Aspetto legale

Come già mostrato nei capitoli precedenti, i *crypto-assets* consistono in risorse digitali posizionate su una *blockchain* e dipendenti dalla crittografia, possono essere distinti in tre tipologie:

- *Token* pagamento, i quali sono il mezzo di scambio o pagamento;
- *Token* di utilità, che permettono l'accessibilità a un servizio o prodotto;
- *Token* d'investimento, possessori di diritti di profitto allegati.

A livello europeo le transazioni avvenute tramite *crypto assets* non sono coperte finanziariamente e questo implica che ci siano molti rischi da parte degli acquirenti ma anche dei venditori. Nonostante la mancanza di regole, alcuni stati hanno adottato delle regole su questo ambito a livello nazionale, questo secondo la commissione europea porta a una frammentazione normativa. Per questo motivo, si è cercato di attuare delle misure di sicurezza che dall'Aprile 2022 fino al 30 giugno 2022 fecero discutere e far arrivare a un accordo provvisorio, il quale prevedere che l'emittente dei *cryptoassets* dovrà provvedere a un rimborso per

poter fornire una garanzia per la ricezione di valute equivalenti a coloro che possiedono i *crypto-assets*. Inoltre, venne ribadito che il ruolo di regolatore e supervisore è stato preso in carico dall'EBA[67], il quale avrà più poteri per la richiesta di informazioni riguardo l'EMT, sarà anche presente l'ESMA[68] che si occuperà delle informazioni che gli saranno trasmesse. L'accordo fu approvato durante lo stesso anno nel mese di ottobre.

Precedentemente, nel 2018 all'EBA e all'ESMA fu attribuito il compito di valutare l'adeguatezza e l'applicabilità delle attività che circondano le criptovalute.

Per quanto riguarda l'Italia, non sono presenti leggi specifiche per questi certificati di proprietà, infatti possono rientrare nello spettro di altre leggi, quali quelle relative al diritto d'autore, della proprietà intellettuale e anche la legge per la protezione del consumatore, nel caso in cui vengono considerati degli investimenti.

3.1 Problematiche di prezzi

Una delle problematiche relative agli *NFTs* è quella dei prezzi, i quali sono fluttuanti e venduti con differenze sostanziali di prezzo, le quali guidate da speculazione, dai possibili valori di utilità dell'*NFT*, dalla volatilità della criptovaluta o dal cambiamento della domanda nel mercato, generalmente, l'arte *NFT* è considerata oggetto da collezione, quindi il valore dei prezzi è determinato dalla disponibilità delle persone di pagare per la singola risorsa digitale, per questo motivo alcune di esse sono state vendute a prezzi esorbitanti. Il mercato degli *NFT* venne definito come una bolla economica, causata da un possibile eccesso di liquidità di quel mercato, che consiste nel superamento dei prezzi degli *NFT* rispetto al loro valore calcolato probabilmente in maniera eccessivamente ottimistica per un determinato periodo di tempo nel quale rimane fisso, ma non in maniera completamente statica. Come accade con qualsiasi servizio o prodotto

[67] EBA o European Banking Authority: si occupa della creazione di un corpo unico di norme standard per il settore bancario dell'UE, assicurando una comunicazione centralizzata dei dati di vigilanza sulle banche dell'UE, per migliorare la trasparenza, la disciplina del mercato e la stabilità finanziaria in tutta l'Unione europea.

[68] ESMA o European Securities and Markets Authority: si tratta di un'autorità indipendente dell'UE il cui obiettivo è quello di migliorare la protezione degli investitori e promuovere mercati finanziari stabili e ordinati.

sul mercato, all'aumentare della domanda, aumenta anche il suo prezzo, al contrario, al diminuire della domanda, cala anche il prezzo correlato.

Agli inizi del 2021 il volume degli scambi finanziari corrispondeva a circa 324 milioni di dollari, mentre soli due mesi prima, nel dicembre 2020 gli *NFTs* scambiati per 12 milioni di USD e durante tutto l'anno circa 200 milioni di USD. Con il tempo questa risorsa digitale ha avuto un crescente interesse, e nel marzo 2021 un solo *NFT* è stato venduto alla cifra di 69,3 milioni di dollari, posseduto da Mike Winkelmann. Nell'anno successivo si è avuto un enorme successo di queste nuove risorse digitali:

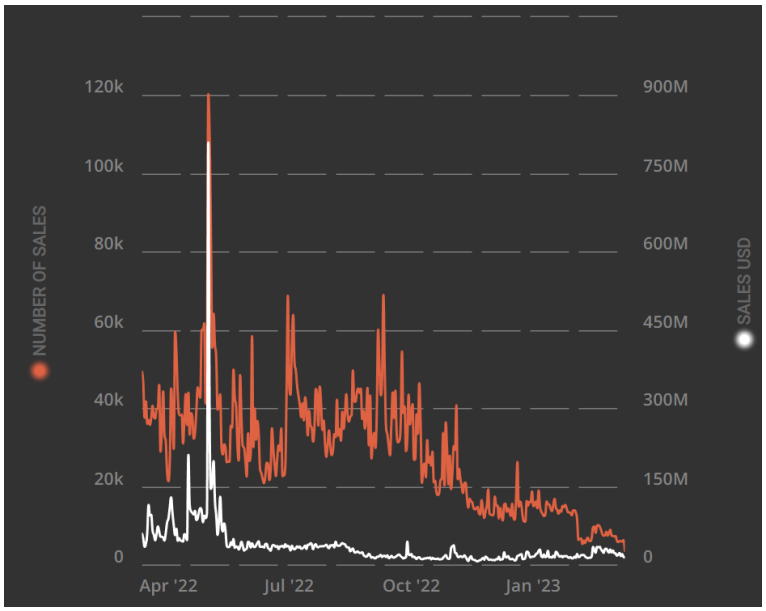

Figura 56: Vendite nel 2022.

Nel grafico si può notare l'alto numero di vendite e il loro andamento nei mesi e negli anni 2022-2023.

Le variazioni di prezzo tra un *NFT* e un altro possono dipendere da vari fattori, questi includono:

- La reputazione dell'artista, la quale ha un grande impatto nello stabilire il prezzo di un *NFT*, accade similarmente con l'arte tradizionale, in cui più un artista ha un seguito elevato, più il prezzo della sua arte sarà elevato rispetto a un artista con meno visibilità.
- La qualità e lo stile dell'opera d'arte hanno un impatto determinante per il prezzo, l'arte con tecniche sorprendenti e tecnicamente impressionanti

hanno prezzi più alti rispetto a quella con caratteristiche banali e confondibili.

- L'unicità, la quale rende l'NFT raro e meno disponibile rispetto a una serie più ampia, determina l'aumento dei prezzi.
- La funzionalità: i *token* di utilità sono importanti poiché i proprietari possono utilizzarli nell'acquisto, quindi il creatore deve considerare anche i bisogni dei possibili acquirenti.
- La domanda: il prezzo in gran parte è determinato dalla domanda e dall'offerta, come in qualsiasi altro mercato di un altro bene.
- La piattaforma sulla quale l'opera d'arte è venduta: poiché alcune di queste piattaforme sono più conosciute e di conseguenza più utilizzate di altre.

Questo fa capire che non esiste un modello di prezzi standard, ma sono in continua fluttuazione e soggetti a cambiamenti rapidi in un breve periodo di tempo.

Nella creazione e successiva vendita di un *NFT* ci sono diverse tipologie di costi fissi cui valore è soggetto a fluttuazioni da parte di determinati elementi, uno tra questi è il costo di conio che varia a seconda della tariffa del gas, le commissioni di mercato per il conio, commissioni di vendita addebitate dal mercato scelto e il costo della commercializzazione dell'*NFT*. A questi si possono includere dei costi non necessari per tutti gli artisti, ovvero il costo relativo all'uso di una piattaforma per chi non ha conoscenze di sviluppo software di tokenizzazione a codice zero o il pagamento di un artista capace di utilizzare una tecnologia che al creatore è sconosciuta.

3.2 Problematiche di proprietà di un'opera digitale

All'interno degli *NFTs* sono presenti gli *smart contracts*, programmi utilizzati per la verifica della proprietà di queste risorse digitali. In alcune piattaforme di vendita, gli *NFTs* possiedono nei termini e condizioni generali informazioni riguardanti la proprietà intellettuale di cosa si sta acquistando, tuttavia molte di queste non possiedono nulla che lo confermi. Il *copyright* consiste nel diritto di impedire altre persone di compiere determinate azioni con l'opera creata, senza avere l'autorizzazione di colui che ne detiene i diritti, all'interno di questo macro-diritto ne vengono inclusi altri cinque:

- Il diritto di riproduzione dell'opera protetta dai diritti di autore,
- Il diritto della preparazione dei derivativi dell'opera, ovvero se viene creato un dipinto e un'altra persona ne scattasse una foto, quest'ultima verrebbe considerata un'opera derivativa o quando si utilizza una canzone all'interno di un video,
- Il diritto di distribuzione di copie dell'opera al pubblico,
- Il diritto di eseguire o visualizzare l'opera protetta dal diritto d'autore.

Questo significa che, se un artista crea un'opera, quale può essere arte o musica combinando vari elementi non interamente prodotti da lui, ma presi da altri creatori, quest'ultimi potrebbero impedirgli i diritti precedenti nonostante l'artista sia il creatore originale dell'opera.

Diviso dal diritto di autore è il diritto di pubblicazione, ovvero se si sta utilizzando un'immagine o qualcosa appartenente ad un'altra persona, lo si sta violando nel caso in cui questa determinata persona avrebbe potuto trarre un particolare vantaggio commerciale o il diritto di privacy sull'*NFT*. Quando si vuole distribuire un *NFT* o una risorsa digitale, bisogna assicurarsi che si abbiamo tutti i seguenti diritti: sulla propria creazione, su tutti gli elementi incorporati all'interno di esso, se sono presenti violazioni di privacy. Quindi bisogna assicurarsi di possedere la proprietà di tutti gli elementi inclusi nell'opera d'arte prima di vendere una risorsa digitale. Generalmente, sulle piattaforme di vendita di NFT, se esse non posseggono una licenza, l'acquirente non sta possedendo tutti i precedenti diritti, ma possiede solo la proprietà di quella copia che ha acquistato, ciò non gli rende possibile di scannerizzare questa copia per poi rivenderla sul mercato.

Ci sono anche degli *NFT* che sono venduti *copyright free,* come l'opera seguente:

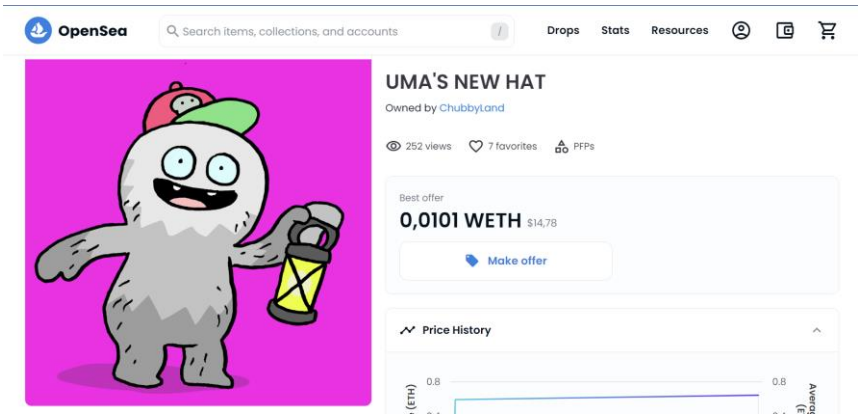

Figura 57: Opera venduta copyright free.

In cui nella descrizione si incoraggia la persona a trarre beneficio dell'opera:

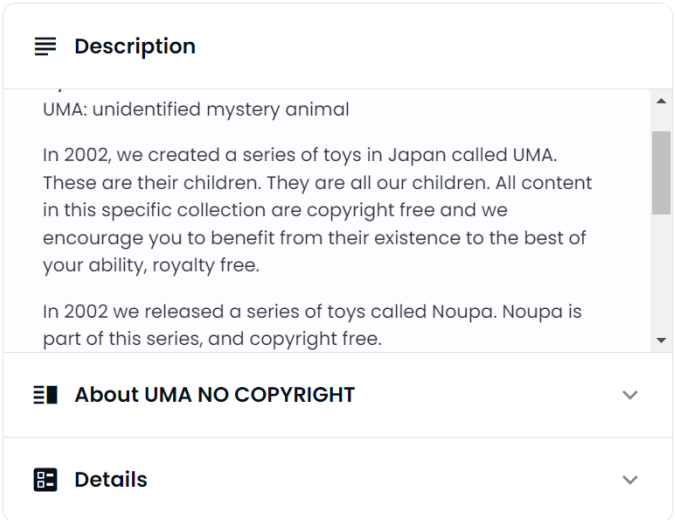

Figura 58: Descrizione del venditore dell'opera precedente.

Quindi è possibile comprare questi *NFTs*, i quali non sono coperti dai diritti d'autore, ma al momento dell'acquisto, l'acquirente ne risulta il proprietario, anche se il diritto di visualizzazione, riproduzione e ridistribuzione dell'opera è fruibile da tutto il pubblico.

In Italia, la legge sulla protezione del diritto d'autore viene garantita automaticamente al creatore dell'opera nel momento in cui essa è creata, tuttavia c'è la possibilità del trasferimento di questo diritto o la sua concessione, a qualcun altro, in licenza.

3.3 Problematiche di provenienza dell'opera

La problematica di provenienza dell'opera *NFT* rappresenta uno tra i temi più discussi dopo il successo acquisito da questa nuova tecnologia. Con il termine

‘provenienza’ si riferisce alla storia della proprietà di una determinata risorsa e ne determina la sua legittimità o valore, sia versione digitale che fisica. In quanto alla versione digitale, l’importanza di determinarne la fonte accresce, poiché un *NFT* è facilmente duplicabile e condivisibile sulle piattaforme, ma soltanto una è la sua versione originale e autentica.

La provenienza può essere stabilita attraverso vari metodi, quali:

- Una ricerca approfondita sull’artista e sull’opera interessata per verificarne la sua reputazione nel campo artistico, ma anche assicurarsi chi sia effettivamente l’artista cercando delle conferme ufficiali.
- Attraverso l’utilizzo dell’indirizzo dell’opera NFT per esaminare la transazione originale sulla blockchain, tramite la quali accedere alla catena di proprietà dell’opera e sui trasferimenti avvenuti nel tempo.
- Rivolgendosi alla comunità di collezionisti di NFT, attraverso forum, gruppi di discussione o social media dove cercare feedbacks dagli altri membri.
- Controllo del rilascio di certificati o documenti di autenticità da parte dell’artista per le opere NFT.

Queste metodologie non offrono una garanzia assoluta e per la natura decentralizzata e digitale degli NFT può rendere complesso il tracciamento completo e accurato della provenienza.

Un esempio può essere rappresentato dall’opera *NFT* di Beeple, *Everydays: The First 5000 Days*, venduta dall’asta *Christies* per 69 milioni di dollari. Per questa fu facile stabilirne la provenienza, poiché fu garantita dalla tecnologia *blockchain*, includendo informazioni come la data di creazione, la firma del creatore e la cronologia delle transazioni.

3.4 Potenziale di frode

Un modo in cui gli *NFTs* possono essere utilizzati per la frode è attraverso la creazione di *NFT* contraffatti, questo è uno dei crimini rappresentanti di una piccola ma notevole parte degli investimenti. Contraffare un *NFT* può coinvolgere la replicazione dell’aspetto visivo/grafico di un’opera in modo da sembrare autentica, per creare un falso è necessario la manipolazione dei metadati, come la

data di creazione, la cronologia delle transazioni. Questa manipolazione di dati può far credere all'acquirente che l'autore dell'opera d'arte sia un artista famoso.

Un'altra tipologia di potenziale di frode può avvenire attraverso la vendita di risorse digitali rubate, il truffatore riesce ad ottenere accesso non autorizzato a una piattaforma o a un archivio di opere digitali potrebbe prenderle e creare un nuovo *NFT* con esse, vendendole come proprietà legittima, per smascherare questo tipo di frode può risultare difficile in particolare se l'opera non è molto conosciuta o se il truffatore ha apportato delle modifiche importanti ad essa. Oltre a queste tipologie di frode ci sono quelle concernenti transazioni o mercati *NFT* fraudolenti, nei quali può essere verificata l'autenticità di *NFTs* di cui quel determinato mercato non possiede la giusta autorizzazione per portare a termine ciò, questo porta gli acquirenti all'acquisto di *NFT* che non hanno valore o che non vengano consegnati dopo il pagamento.

Un esempio di truffa avvenuta riguarda quello che si mostrava come un gioco P2E chiamato *Frosties NFT*, il quale prometteva agli investitori di poter guadagnare molti ricavi generati da questo gioco nel metaverso, che tuttavia non esisteva. Subito dopo aver venduto tutti i pezzi di NFT creati, circa 8.888, gli sviluppatori disattivarono tutti gli account e scapparono con 1.3 milioni di dollari ottenuti dall'acquisto delle risorse digitali da parte degli investitori. Una cosa simile a *Frosties NFT* accadde su Solana *blockchain*, nella quale venne sviluppato un progetto chiamato *Iconics*, questo avrebbe avuto il compito di distribuire circa 8.000 opere d'arte 3D randomizzate agli investitori. Durante la prevendita vennero vendute 2000 opere per 0,5 SOL ognuna, ciò significava che al momento dell'effettiva vendita ogni NFT valeva circa 140000 dollari, in questo caso gli investitori ricevettero in cambio qualcosa che non era però ciò per cui avevano pagato, ovvero ricevettero una raccolta casuale di emojis. Successivamente a ciò vennero cancellati sia l'account *Twitter* e il gruppo *Discord* del progetto.

A causa delle numerose truffe di *NFTs* che circolano sulle varie piattaforme, anche numerose risorse digitali legittime tendono a fallire, poiché i media riportano di più notizie riguardanti truffe che progetti reali e di successo e questo con il tempo sta danneggiando la reputazione del settore al contorno degli *NFTs*. Per questo

motivo da gennaio del 2022 al giugno dello stesso anno si è registrato un calo drastico degli investimenti effettuati.

Per poter arginare queste problematiche, una delle possibili soluzioni sarebbe di ricercare in maniera approfondita prima di vendere o comprare, verificando se i metadati risultino sospetti e utilizzare unicamente mercati affidabili, come *OpenSea,* valutato a gennaio del 2022 a 13,3 miliardi di dollari. La piattaforma per arginare le problematiche di frode ha nel tempo incluso procedure come quella di approvazione per la prevenzione degli abusi online, che però fu rimossa e nel mese di gennaio del 2022 venne permesso agli utenti di creare fino a un limite di 50 NFT per evitare falsi o plagi, anche questa regolamentazione fu rimossa poiché non accolta dagli utenti. Nello stesso anno, a maggio, viene introdotto un sistema automatizzato per l'iniziale identificazione e la successiva rimozione delle copie di *NFTs* autentici.

Altre soluzioni prevedono il non condividere le informazioni del proprio portafoglio con altre persone nella rete, l'ispezionare l'account del marketplace del venditore prima di procedere con l'acquisto e controllare i prezzi dell'NFT per guardare le offerte precedenti di un determinato progetto, assicurandosi su altre piattaforme il prezzo degli NFT simili. Infine, non si deve cliccare su nessun link che sembri sospetto e quindi evitare il *phishing*[69].

In Italia, la legge che cerca di far fronte alle frodi è la 'legge di protezione del consumatore'.

3.5 Problematiche di tassazione

Attualmente gli *NFTs* non possiedono una propria regolamentazione fiscale specifica, però ciò non esente le transazioni legate ad essi dalle tasse. L'aliquota fiscale che deve essere pagata può variare in base a vari fattori, tra questi ci potrebbero essere la durata di tempo per la quale si è detenuto l'NFT o la variazione di prezzo dell'NFT dal momento in cui l'investitore lo ha acquistato.

[69] Phishing: indica una frode informatica finalizzata all'ottenimento di dati personali sensibili e perpetrata attraverso l'invio di un messaggio di posta elettronica a nome di istituti di credito, finanziarie, agenzie assicurative, in cui si invita l'utente, generalmente al fine di derubarlo, a comunicare tali informazioni riservate. https://www.treccani.it/enciclopedia/phishing (ultimo accesso effettuato il 13/03/2023)

Se l'acquisto degli NFT avviene per scopo personale e una volta sola, non dà origine a reddito, in queste stesse circostanze la vendita della risorsa digitale sarà in grado di generare reddito e farà parte del 'reddito diverso' dell'art. 67 TUIR:

> L'art. 67, comma 1, lettera d), del TUIR prevede che costituiscono redditi diversi le vincite delle lotterie, dei concorsi a premio, dei giochi e delle scommesse e i premi derivanti da prove di abilità o della sorte nonché quelli attribuiti in riconoscimento di particolari meriti artistici, scientifici o sociali.[70]

Ovvero, la vendita occasionale di *NFT* rientra in quelle attività commerciali considerate non abituali, tuttavia bisogna inserirne i valori all'interno del quadro RL della dichiarazione dei redditi e a questi valori verrà applicata successivamente la tassazione marginale, che apposta all'ultima porzione di reddito tasserà l'importo derivante da un incremento del reddito. Per l'acquirente invece, non viene imposta nessuna imposizione fiscale.

Si ha un cambiamento nella tassazione se si passa da una vendita occasionale a una abituale. Nella vendita abituale, nel caso in cui si vende l'opera e con essa tutti i diritti compreso il diritto d'autore, di conseguenza il venditore viene escluso dall'IVA e genererà reddito autonomo secondo l'articolo 53 del TUIR:

> I redditi di lavoro autonomo sono disciplinati dall'art. 53 del TUIR 917/86 il quale stabilisce al 1° comma che: "Sono redditi di lavoro autonomo quelli che derivano dall'esercizio di arti e professioni".[71]

Se il venditore opera in un'attività d'impresa abituale, dovrà aprire una partita IVA e far riferimento al codice Ateco 47.91.10:

> Relativo al commercio al dettaglio di qualsiasi tipo di prodotto effettuato via internet. Con questo codice ATECO è possibile vendere online qualunque tipo di prodotto fisico o digitale con alcune eccezioni.[72]

[70] Articolo 67 del testo unico delle imposte sui redditi.
[71] Articolo 53 del TUIR.
[72] Codice ATECO 47.91.10 utilizzato da ISTAT.

Figura 59: Processi di compravendita di un NFT.

Ci sono molti casi che complicano l'inserimento di questi asset in dei precisi processi economici.

3.6 Regolamentazione MiCA

Il 20 aprile 2023, il Parlamento Europeo ha votato per il *'Markets in Crypto-Assets Act'* o MiCA, che fu ratificata successivamente dal Consiglio per gli affari economici e finanziari dell'UE il 16 maggio 2023.

MiCA consiste in un quadro normativo unico nell'Unione Europea comprendente tutte le azioni crittografiche, in modo tale da offrire una maggior chiarezza di regole interne a questo settore in fase di sviluppo. Mira a garantire che l'UE sia favorevole all'innovazione e che non venga ostacolata l'applicazione di nuove tecnologie.

Gli obiettivi della regolamentazione sono:

- Dare uniformità alle normative dei singoli paesi, per permettere vantaggi ai fornitori di servizi di cripto-asset nel mercato interno,
- Provvedere a fornire sicurezza per le risorse crittografiche,
- Fornire trasparenza nel settore delle risorse digitali.

Le regole nazionali applicate da alcuni Stati verranno sostituite interamente da MiCA, quando queste non rispettino la legislazione dell'UE. Le aziende che garantiranno di una copertura da MiCA comprendono tutte le società di consulenza di criptovalute e i gestori di portafogli crittografici, le piattaforme di scambio di criptovalute e i portafogli di custodia. Tutte le imprese menzionate precedentemente devono rispettare dei requisiti dettati dall'UE, i quali

comprendono la registrazione dell'impresa presso l'autorità competente dello Stato UE in cui si trova la sede principale, devono soddisfare dei requisiti di governance, attuare delle misure per la protezione dei fondi dei clienti e procedure per identificare e arginare i rischi dell'attività cripto. Tra i requisiti vengono inclusi il rispetto delle norme antiriciclaggio, la normativa sulla protezione dei dati, la fornitura di informazioni complete, chiare e corrette agli investitori.

Mentre, i beni coperti da questa regolamentazione sono di varia tipologia:

- *Transferable Crypto-Assets* TCAs, includono tutti quei cripto-asset che possono essere trasferiti, come Bitcoin, Ethereum e Ripple,
- *Asset-Reference Tokens* ARTs, utilizzati per fare riferimento a un altro tipo di asset,
- *E-Money Tokens* EMTs, ovvero dei cripto-asset che vengono utilizzati per la rappresentazione digitale della valuta fiat,
- *Crypto-Asset Service Providers* CASPs, entità che forniscono servizi relativi a cripto-asset, come i fornitori di portafogli custoditi.

Questo regolamento porterà vari benefici ai paesi dell'UE, creando un quadro di regole equilibrate, fornirà coerenza e facilità nelle attività transfrontaliere, fornendo una certezza legale per le aziende operanti nell'Unione Europea. Tuttavia, la protezione non riguarda soltanto le aziende, ma coinvolge anche i consumatori con requisiti di trasparenza, divulgazione dei rischi, aggiunta delle misure mirate alla salvaguardia degli investitori e utenti, che possono portare anche i più scettici ad immergersi nel mercato garantendone lo sviluppo. Vengono introdotte misure per prevenire degli abusi sul mercato e di conseguenza migliorarne l'integrità, tramite requisiti per i fornitori di servizi criptoasset per garantire il rispetto delle norme antiriciclaggio *AML* e antiterrorismo *CTF,* essendo validi e sempre egli stessi per tutti i fornitori presenti su suolo Europeo creano un livello di parità.

Nel caso in cui questa regolamentazione verrà adottata, il supervisionamento avverrà da diverse entità, tra le quali: autorità competenti nazionali, comitato europeo delle autorità di vigilanza del mercato dei valori mobiliari (*ESMA)* per la supervisione e il coordinamento delle autorità competenti nazionali nel settore delle attività cripto. Queste due istituzioni avranno il compito di cooperare e scambiarsi informazioni riguardanti il monitoraggio delle attività delle imprese di

attività legate all’ambito cripto, i potenziali indicatori menzionati per il monitoraggio sono:

- Numero e volumi di emissioni di cripto-attività nell'UE,
- Numero di soggetti autorizzati nell'UE come fornitori di servizi per le cripto-attività,
- Numero di soggetti autorizzati nell'UE come emittenti di cripto-attività garantite da attività o emittenti di token collegati ad attività significativi,
- Numero e valore delle frodi e dei furti di cripto-attività nell'UE,
- Numero di soggetti autorizzati da una ANC come infrastruttura di mercato basata sulla DLT nell'ambito del regime/regime pilota,
- Volume di transazioni negoziate e regolate da infrastrutture di mercato basate sulla DLT,
- Numero di casi di abusi di mercato relativi a cripto-attività segnalati alle ANC e oggetto di indagine da parte delle stesse,
- Capitalizzazione di mercato delle cripto-attività garantite da attività e dei token collegati ad attività significativi,
- Volume dei pagamenti effettuati mediante l'impiego di token collegati ad attività e token collegati ad attività significativi,
- Valutazione del raggiungimento o meno di un livello sistemicamente rilevante da parte di altre cripto-attività/infrastrutture o partecipanti al mercato che utilizzano la DLT e/o che hanno a che fare con le cripto-attività,
- Numero e volume di strumenti finanziari emessi come cripto-attività nell'UE,
- Numero di prospetti di strumenti finanziari come cripto-attività approvati dalle ANC,
- Numero di soggetti autorizzati dalle ANC a fornire servizi ai sensi della vigente legislazione dell'UE (ad es. MiFID II/MiFIR, CSDR, SFD) e che utilizzano la DLT/strumenti finanziari in forma di cripto-attività,
- Volume di transazioni negoziate e regolate da fornitori di servizi autorizzati ai sensi della vigente legislazione dell'UE (ad esempio MiFID II/MiFIR,

CSDR, SFD) e che utilizzano la DLT/strumenti finanziari in forma di cripto-attività[73].

La proposta fu presentata dalla Commissione europea nell'ottobre del 2020, inserita all'interno di altre misure che mirabo a regolamentare la maggior parte delle attività cripto nell'UE. L'iter standard dopo avvenuta la proposta è quello della negoziazione e approvazione dal Parlamento europeo e dal Consiglio dell'UE con eventuali modifiche.

Non è stata annunciata una data di attuazione sicura del MiCA, un'ipotesi riguarda la piena messa in pratica dalla metà del 2024.

4. Caso Studio

Il seguente capitolo si propone di esaminare in dettaglio il processo di creazione e vendita di un token non fungibile nel contesto di un progetto specifico. Gli NFT sono diventati uno strumento sempre più popolare nel mondo digitale, consentendo agli artisti, ai creatori e agli appassionati di monetizzare e autenticare opere d'arte, oggetti digitali e collezioni uniche.

Nel contesto del mio progetto ho deciso di adottare lo stile pixel per l'opera d'arte NFT. Questa scelta è stata influenzata da delle considerazioni, innanzitutto, lo stile pixel è legato alla cultura dei videogiochi ma anche delle grafiche dei primi computer, in modo tale da evocare una sensazione di nostalgia e appartenenza a una generazione cresciuta con questi mezzi di intrattenimento digitale. Caratteristica appetibile per i collezionisti, i quali ricercano opere uniche nel loro genere ed evocative. Un'altra motivazione è rappresentata dalla semplicità delle forme, soprattutto quelle geometriche, eliminando dettagli superflui. Dal lato della tecnologia, la semplificazione visiva garantisce un forte impatto visivo e facilmente visibile su schermi di diverse dimensioni.

L'opera raffigura un astronauta che salta dalla luna passando per i vai pianeti e cui ultimo è rappresentato dal sole:

[73] Commissione Europea, *Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva* (UE) 2019/1937, 24.9.2020, Bruxelles, p. 155-156 (ultimo accesso 20/06/2023)

Figura 60: Il mio lavoro *"The Courage to Explore and Conquer".*

Rappresenta un simbolo di ambizione e scoperta, in cui un astronauta salta da un corpo celeste ad un altro, conquistandoli nel suo cammino. I pianeti simboleggiano mete e traguardi desiderati, invitando a una contemplazione delle vaste possibilità che si estendono davanti a noi. L'immagine mira a una riflessione sull'innata voglia dell'uomo di superare i propri limiti ed esplorare nuovi mondi e orizzonti. Il cammino può essere inteso sia come desiderio di crescita personale o il coraggio della persona nel perseguire i propri sogni.

Ho inserito parte dell'interpretazione all'interno della descrizione dell'opera al momento della creazione dell'NFT:

This immersive pixel art NFT invites you to contemplate the boundless possibilities that lie before us. In this artwork, an astronaut fearlessly leaps from one celestial body to another, symbolizing the spirit of ambition and discovery. Each planet represents a desired goal or aspiration, inspiring us to push beyond our limits and explore new worlds and horizons. And each flame represents the reward that drives man forward.

You will receive the ownership, for this reason, you will be the sole owner of this unique digital artwork, allowing you to display it in your personal collection and enjoy it exclusively.

Please note that the purchase of this NFT does not grant any commercial reproduction rights. This artwork is protected by copyright and may not be reproduced, distributed, or used commercially without explicit permission.

La piattaforma che ho scelto per caricare il mio NFT è OpenSea. Ho considerato OpenSea come scelta più adatta per diversi motivi. Innanzitutto, è una delle piattaforme NFT più popolari e di maggior successo, con un'ampia gamma di utenti, offrendo così un'opportunità di visibilità ed esposizione delle opere d'arte NFT a collezionisti, investitori e appassionati di arte digitale in modo tale da aumentare le possibilità di vendita e di raggiungere un pubblico più ampio. Un'altra ragione per cui ho scelto OpenSea è la varietà di NFT che la piattaforma supporta, tra cui arte, giochi, collezionabili e *virtual real estate* che consente agli artisti di esplorare diversi tipi di opere d'arte e di raggiungere potenziali acquirenti interessati a diverse forme di NFT.

Inoltre, l'interfaccia di OpenSea è molto intuitiva e semplice da utilizzare anche per chi non ha molta esperienza nel settore delle criptovalute o della blockchain. Al suo interno vengono supportati diversi standard di token e blockchain, tra i quali Ethereum, Polygon e altri per offrire una maggior flessibilità nella scelta.

In termini di reputazione, OpenSea è conosciuta come una delle principali piattaforme NFT più popolari e di maggior successo. Sempre più persone vi si affidano, essendo sicura per il commercio degli NFT e fornendo allo stesso tempo intuitività e solidità in quanto a infrastruttura blockchain.

Per quanto riguarda le commissioni, la piattaforma trattiene il 2,5% del valore di vendita di ogni NFT e inoltre vengono applicate delle gas fees, le quali consistono in commissioni di rete richieste dalla blockchain Ethereum per elaborare le transazioni. Queste commissioni possono variare nel tempo dipendendo da diversi fattori.

Prima di poter caricare l'opera d'arte su OpenSea, bisogna connettere il wallet di criptovaluta, sono disponibili vari portafogli disponibili sul mercato: MetaMask,

Coinbase Wallet, WalletConnect e Phantom. Tra questi ho scelto Metamask, uno dei wallet più popolari e ampiamente utilizzati nel contesto degli NFT e della blockchain Ethereum.

Alcuni motivi per i quali ho considerato di utilizzare Metamask anziché altri wallet sono:

- La sua facilità d'uso: tramite un'interfaccia utente intuitiva e facile da utilizzare, sia per gli utenti esperti che per i principianti. Il processo d'installazione è risultato semplice, poiché disponibile come estensione per i browser comuni, una volta installato, si ha la possibilità d'installare un nuovo portafoglio o importare un proprio portafoglio esistente tramite l'utilizzo di una frase di backup (*seed phrase*) che consiste in una serie di parole. La seed phrase permette di ripristinare il proprio portafoglio su un altro dispositivo. Dopo l'installazione e la creazione di un wallet, un'icona apparirà nel browser e permetterà di accedere al saldo del portafoglio, eseguire altre transazioni, la gestione degli NFT e l'interazione con le dApp, agevolando la connessione in modo sicuro e diretto senza l'inserimento manuale delle proprie informazioni di accesso.
- La compatibilità con Ethereum: Metamask è compatibile con la blockchain Ethereum. Per questa ragione, supporta gli standard di token ERC-20 e ERC-721.
- La sicurezza: metamask mette a disposizione delle funzionalità di sicurezza avanzate per proteggere i propri fondi e le informazioni personali. Il wallet memorizza le chiavi private in modo crittografato sul proprio dispositivo, consento di mantenere il controllo completo dei propri fondi e per ogni transazione richiede un'autorizzazione, fornendo un ulteriore livello di sicurezza.
- L'interoperabilità: il wallet è compatibile con una vasta gamma di dApp e servizi blockchain. Quindi metamask può essere utilizzato per diverse attività, come il commercio e gestione degli NFT.
- La comunità di sviluppatori che si occupano di Metamask è attiva e c'è un lavoro costante per miglioramenti da apportare al wallet, con aggiornamenti costanti per la sicurezza ma anche per nuove funzionalità, permettendo in

questo modo che il wallet sia all'avanguardia e tenga testa a un mercato in continuo sviluppo.

In quanto alla blockchain da scegliere, ho scelto Polygon e non Ethereum. Uno dei vantaggi di Polygon rispetto ad Ethereum è la sua scalabilità. Utilizza una soluzione di secondo layer che consente di elaborare un numero maggiore di transazioni a costi inferiori rispetto a Ethereum, rendendo Polygon più economica per utenti come me che vogliono evitare commissioni elevate. La scalabilità porta anche ad avere una velocità di transazioni maggiore rispetto a Ethereum, quest'ultima può richiedere diversi minuti per confermare una transazione, mentre Polygon può completarla quasi in maniera istantanea.

Essendo Polygon basato sulla blockchain di Ethereum, si ha una compatibilità con gli smart contracts e i token, permettendo un facile trasferimento da una blockchain all'altra.

In quanto a sicurezza, la blockchain Ethereum è la più robusta e sicura, ma Polygon beneficia della sicurezza di Ethereum operando come una rete di secondo layer su di essa, garantendo che qualsiasi attività svoltasi su Polygon abbia il supporto dell'infrastruttura Ethereum.

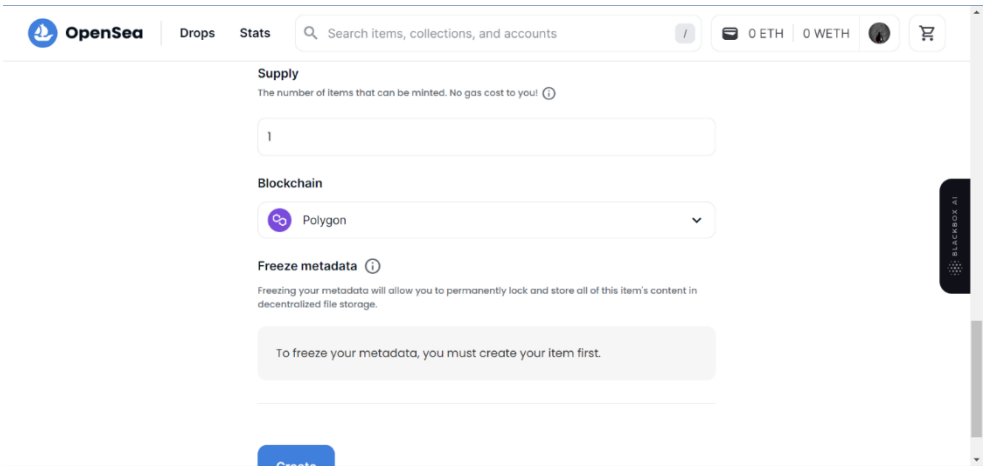

Figura 61: Scelta della blockchain al momento della creazione.

Su OpenSea ci sono vari metodi di vendita disponibili per gli NFT, alcuni dei principali sono:

- Asta: viene impostato un prezzo di partenza e una durata per l'asta, in modo che gli acquirenti possano fare offerte sull'opera e l'offerta più alta vincerà l'asta al termine del periodo stabilito. L'effetto delle aste può essere

l'interesse e la competizione che ha luogo tra gli acquirenti, portando a prezzi più alti l'opera.

- Prezzo fisso: viene impostato un prezzo fisso per l'NFT, quindi gli acquirenti possono acquistare l'opera immediatamente senza dover fare offerte e al prezzo stabilito. Il metodo più semplice e veloce per la vendita.
- Offerta: gli acquirenti fanno offerte sull'NFT in vendita e il proprietario può accettare o rifiutare. Inizia una vera e propria negoziazione diretta tra acquirente-venditore, senza intermediari.
- *Bundles*: possibilità di creare pacchetti di più NFT venduti insieme come unica unità, utile nel caso in cui si vuole vendere una collezione di NFT correlati o creare offerte speciali per gli acquirenti.
- Acquisto immediato con offerta: viene combinato il prezzo fisso con la possibilità di fare delle offerte superiori al prezzo stabilito.

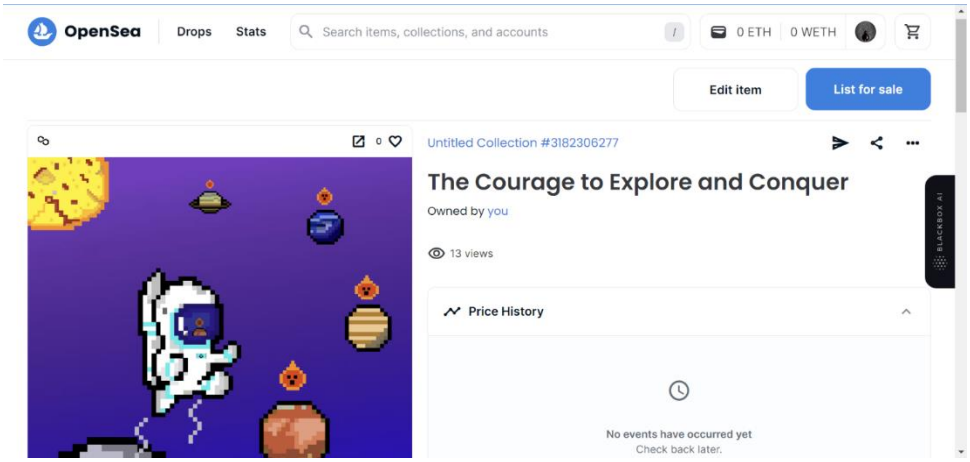

Figura 62: Schermata dell'NFT su OpenSea.

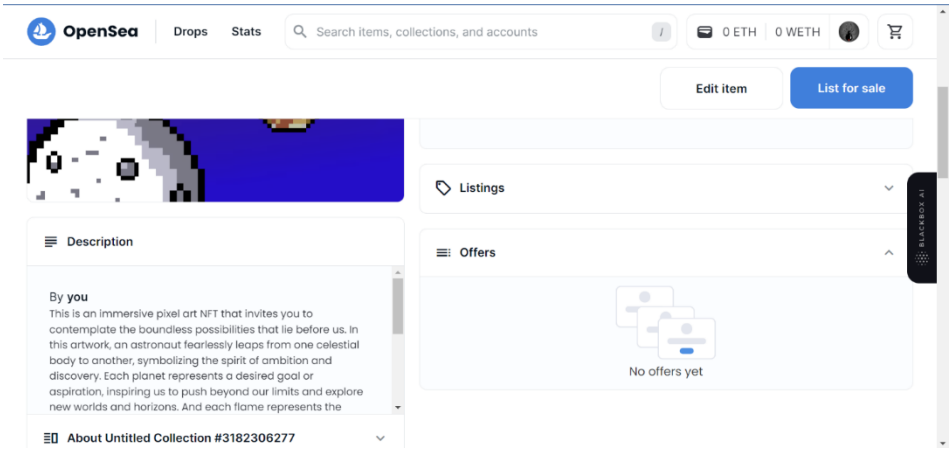

Figura 63: Schermata della descrizione e sezione "offerte" dell'NFT.

Come già spiegato nei capitoli precedenti, per stabilire il prezzo di un NFT devono essere presi in considerazione alcuni fattori, come: il valore artistico, la domanda di mercato, la sua esclusività, la storia dell'artista (se è noto o se non lo è) e fattori esterni (dimensione di mercato, concorrenza e condizioni economiche).

Essendo alla mia prima esperienza nella creazione di NFT e la mia non fama come artista, ho deciso di mettere in vendita il mio lavoro come offerta anziché stabilirne un prezzo fisso. Questa mia scelta deriva dalla mancanza di esperienza pregressa nel settore. Secondo la mia opinione l'offerta permette un approccio più flessibile, in cui gli acquirenti interessati possono presentare delle offerte e negoziare il prezzo in base al valore percepito dell'opera.

Attraverso questa esperienza, ho scoperto in maniera pratica tutto ciò imparato nei capitoli precedenti, come l'importanza della piattaforma OpenSea, strumento di visibilità ed esposizione delle opere d'arte NFT, la sua reputazione, essendo una delle piattaforme più popolari e con un pubblico ampio, il funzionamento della tecnologia blockchain che mi ha portata alla valutazione di quale sarebbe stata la migliore per questo mio lavoro.

Essendo un mercato in cambio continuo ci saranno sempre variazioni e conoscenze d'acquisire.

Conclusione

Questa tesi ha esplorato in maniera dettagliata il concetto di *NFT*, *Non-Fungible Token* con le sue implicazioni nel contesto dell'arte digitale e della blockchain. Partendo dalla domanda centrale "In che modo gli *NFT* stanno influenzando l'arte, l'economia e la cultura digitale?", sono stati esaminati diversi aspetti fondamentali.

In primo luogo, è stata analizzata la storia dell'arte digitale e il passaggio agli *NFT,* considerando anche il ruolo della blockchain e gli algoritmi di consenso. In particolare, è emerso che la blockchain *Ethereum* rappresenta la piattaforma chiave per utilizzo degli *NFT*, grazie alla sua capacità di supportare *smart contracts* e le DAO.

Successivamente, sono stati esplorati i vantaggi e gli svantaggi nell'uso degli *NFT* nell'arte, concentrandoci sulle problematiche legate all'età, ai prezzi, alla proprietà, alla provenienza, alla frode e alla tassazione. Infine, l'insieme delle competenze teoriche acquisite durante la ricerca e la successiva scrittura dei capitoli ha visto la loro applicazione in un caso studio in modo da avere una conoscenza ampia di queste innovazioni tecnologiche e non limitata alla teoria.

Alla luce di quest'analisi è emerso che gli *NFT* hanno allargato lo spettro di prospettive sia per artisti già famosi ma anche per i meno noti e per gli appassionati di arte digitale, offrendo loro opportunità di distribuzione, autenticazione e monetizzazione delle opere.

Tuttavia, sono emerse sfide legali legate alla mancanza di una regolamentazione accurata in questo ambito. L'Unione Europea sta cercando di colmare questa lacuna al fine di garantire la protezione dei diritti degli artisti e allo stesso momento la fiducia degli acquirenti.

In conclusione, si può affermare che gli *NFTs* rappresentano un'innovazione invitante nell'ambito dell'arte digitale, eliminando gli intermediari tradizionali così da consentire agli artisti di raggiungere un vasto pubblico, allo stesso tempo, sono state sollevate delle questioni per le adozioni di questa tecnologia riguardanti vari ambiti, specialmente la necessità di una regolamentazione accurata. Pertanto, l'approccio al potenziale degli *NFT* dovrebbe tenere conto di tutti gli aspetti circostanti, garantendone un uso corretto e sostenibile, aperto all'innovazione della tecnologia delle opere d'arte digitale.

Indice elenco figure

Bibliografia

Chris Collins, *NFT Art and Collectibles for Beginners: The Must Have Guide for Understanding Non-Fungible Tokens (NFTs)*, 2021, Marketing Forte LLC, Arizona US

Nakamoto Satoshi, *NFT INVESTING FOR BEGINNERS – Non-fungible Tokens (NFT) & Collectibles Money Guide: Invest in Crypto Art Token-Trade Stocks-Digital Assets. Earn Passive Income with Market Analysis Royalty Shares*, 2022, David's House Inc.

Mark J. Davies, NFT: Guida completa ai Non Fungible Token. Come collezionare arte digitale e beni unici nel mondo virtuale, 2021

Commissione Europea, *Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva* (UE) 2019/1937, 24.9.2020, Bruxelles

Éder Pereira, Paulo Ferreira, Derick Quintino, Non-Fungible Tokens (NFTs) and Cryptocurrencies: Efficiency and Comovements, 2 Ottobre 2022, FinTech

Tax & Legal Partners, *Il fenomeno degli NFT ("Non Fungible Token") alla ricerca di un corretto inquadramento giuridico-fiscale*, 17.01.2022, Milano

Herian, Robert; Di Bernardino, Claudia; Chomczyk Penedo, Andres; Ellul, Joshua; Ferreira, Agata; von Goldbeck, Axel; Siadat, Alireza and Siedler, Nina-Luisa (2021). *NFT – Legal Token Classification.* EU Blockchain Observatory & Forum.

Usman W. Chohan, MBA, PhD, *Non-Fungible Tokens: Blockchains, Scarcity, and Value,* 24 marzo 2021, Centre for Aerospace & Security Studies (CASS); Critical Blockchain Research Initiative (CBRI); International Association of Hyperpolyglots (HYPIA); University of New South Wales (UNSW)

Borri, Nicola and Liu, Yukun and Tsyvinski, Aleh and Tsyvinski, Aleh, *The Economics of Non-Fungible Tokens*, 7 marzo 2022

C. Vijai, Elayaraja M., Suriyalakshmi, Joyce, *The Blockchain Technology and Modern Ledgers Through Blockchain Accounting,* Dicembre 2019, SSR Electronic Journal

Q. Wang, R. Li, Q. Wang, S. Chen, *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges (Tech Report)*, 25.10.2021

C. Flick, *A critical professional ethical analysis of Non-Fungible Tokens (NFTs),* Dicembre 2022, Journal of Responsible Technology

A. Barolini, E. Tramonto, C. Fontana, M. Carozzi, M. Meggiolaro, *Gli NFT, speculazione o nuova frontiera del copyright?*, maggio 2021, Valori.it

Commissione Europea, *REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937,* 24.9.2020, Bruxelles

Dragos I. Musan, *NFT.finance Leveraging Non-Fungible Tokens*, 15.6.2020, Imperial College London

N. Borri, Y. Liu, A. Tsyvinski, *The Economics of Non-Fungible Tokens*, Marzo 2022

M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. Maria Aiello, A. Baronchelli, *Mapping the NFT revolution: market trends, trade networks, and visual features*, 22.10.2021, Scientific Reports

D. Tawadros, *Towards the Blockchain and Decentralizing Data Security*, 2019, ResearchGate

Sitografia

Ethereum, definizione NFT e i loro usi, DeFi, smart contracts: https://ethereum.org/en/nft/

https://cointelegraph.com/ethereum-for-beginners/history-of-eth-the-rise-of-the-ethereum-blockchain | https://erc725alliance.org/ | https://docs.soliditylang.org/en/latest/introduction-to-smart-contracts.html

https://opensea.io/blog/guides/non-fungible-tokens/

https://nftnow.com/guides/nft-timeline-the-beginnings-and-history-of-nfts/

Fondamenti della Blockchain: https://www.ibm.com/topics/blockchain

https://www.grcteam.it/news-e-iniziative/dettaglio-notizia/Blockchain-Registri-distribuiti-Blocchi-Nodi-Wallet-Crittografia-e-

Chiavi/#:~:text=I%20Nodi%2C%20sono%20Account%20informativi,tutti%20i%20nodi%20sono%20uguali

https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between

https://www.bitstamp.net/learn/blockchain/how-does-hashing-work/

APECOIN: https://apecoin.com/about

P2P: https://academy.binance.com/it/articles/peer-to-peer-networks-explained

Axie: https://axie.substack.com/p/migration

https://forkast.news/what-is-axie-infinity-nft-gaming-3-0/#:~:text=Axie%20Infinity%20was%20initially%20built,Ronin%20began%20in%20April%202021.

Algoritmi di consenso: https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp#:~:text=Proof%20of%20elapsed%20time%20(PoET)%20is%20a%20consensus%20algorithm%20developed,every%20node%20the%20same%20chance.

https://www.techtarget.com/whatis/definition/consensus-algorithm

Merkle trees: https://academy.binance.com/it/articles/merkle-trees-and-merkle-roots-explained

Copyright: https://www.legal500.com/developments/thought-leadership/nfts-and-copyrights/

Problematiche legali: https://wessexfairchild.com/commentary/what-are-the-legal-issues-around-nfts/#:~:text=With%20NFT%20sales%20now%20running,laundering%20regulations%20and%20estate%20planning.

https://www.borsaitaliana.it/notizie/sotto-la-lente/fiscalita-nft.htm

https://wessexfairchild.com/commentary/what-are-the-legal-issues-around-nfts/

Quantum: https://nftnow.com/art/quantum-the-first-piece-of-nft-art-ever-created/

Giochi “Play-to-earn”: https://nftnow.com/guides/the-best-play-to-earn-games-for-nft-and-crypto-lovers/

Cryptokitties: https://guide.cryptokitties.co/guide/

https://www.coindesk.com/markets/2018/05/07/nba-superstar-steph-curry-is-now-the-first-celebrity-cryptokitty/

BAYC: https://boredapeyachtclub.com/#/ | https://opensea.io/collection/boredapeyachtclub

https://chaindebrief.com/bored-ape-yacht-club-history-rise-of-bayc/

VeeFriends: https://veefriends.com/ | https://www.nftculture.com/nft-news/the-story-of-veefriends/

Problematica d'impronta di carbonio: https://www.sciencefocus.com/future-technology/can-nfts-solve-their-massive-carbon-footprint-problem/

OpenSea: https://www.investopedia.com/what-is-opensea-6362477

Beeple: https://blog.artsper.com/en/a-closer-look/how-beeples-nft-art-is-changing-art-history/

https://forbes.it/2021/03/19/la-digital-art-e-il-fenomeno-di-mercato-del-momento-il-caso-di-beeple/

Decentraland: https://equity.guru/2022/03/31/the-cryptocurrency-guide-for-the-perplexed-decentraland-mana/

RarePepe: http://rarepepedirectory.com/?cat=62 | https://mlo.art/news/blog-posts/a-brief-history-of-rare-pepes/

Digital art: https://magazine.artland.com/digital-art/ | https://magazine.artland.com/how-the-crypto-art-boom-is-changing-the-art-market/