

Dipartimento di Impresa e
Management

Cattedra di informatica

Blockchain ed NFT

Come il mondo dell'arte si sta evolvendo

Prof. Luigi Laura

RELATORE

Jacopo Lago Matr. 243931

CANDIDATO

Anno Accademico 2021/2022

INDICE

Prefazione	4
Capitolo 1	6
Blockchain	6
1.1 Nascita ed evoluzione.....	6
1.2 Meccanismi di consenso	8
1.3 Funzionamento	9
1.4 Tipologie di blockchain	11
1.5 Oracoli.....	12
1.5.1 Possibili soluzioni.....	13
1.5.2 Come funzionano gli oracoli.....	14
Capitolo 2	15
Ethereum	15
2.1 Smart contracts	15
2.2 Ether e proof of stake.....	15
2.3 Gas	16
2.3.1 Il London upgrade.....	17
2.3.2 Perché esistono le gas fees?.....	18
2.4 DAO, a Decentralized Autonomous Organization.....	18
2.4.1 Caratteristiche delle DAO.....	20
2.4.1 La trasformazione della gig economy in comunità creative.....	25
2.5 Web 3.0.....	26
Capitolo 3	29
Non Fungible Token	29
3.1 I token fungibili e non fungibili.....	30
3.2 mercati	32
3.3 Opportunità	34
3.4 relazione tra NFT e criptovalute	37
3.4.1 l'inverno delle criptovalute	38
Capitolo 4	43
Crypto-Art	43
4.1 introduzione.....	45
4.2 Crypto arte in senso pratico	48
Bibliografia e sitografia	52

Prefazione

Giorno dopo giorno la nostra quotidianità è stata invasa dalla tecnologia, grazie agli smartphone e ad un innumerevole quantità di dispositivi che ci ha reso la vita più semplice, ma che allo stesso tempo ha reso i nostri dati sensibili ancora più fragili. Con l'avvento dell'Internet of Things ossia il processo di connessione a internet di oggetti di uso comune, il potere delle aziende produttrici di software e hardware è diventato sempre più centralizzato. La centralizzazione dei poteri non è mai stata vista di buon occhio e così dalle idee rivoluzionarie di vari gruppi di informatici è nata la Blockchain, le cryptovalute e più in generale la nuova generazione del world wide web, il web 3.0.

In questa tesi non parlerò di monete virtuali, ma della blockchain, la tecnologia che le sostiene, che è spesso pensata solo in quell'ottica, ma che ha invece infinita potenzialità.

Mi concentrerò infatti sugli NFT, dei particolari token che rappresentano dei contratti scritti sulla blockchain, che conferiscono al titolare diritti di autenticità e possesso sul token stesso.

Grazie ai Non Fungible Token la proprietà intellettuale, e la sua tutela, hanno raggiunto livelli che prima sembravano utopici, creando un mercato attorno a questi token di milioni di dollari.

Capitolo 1

Blockchain

1.1 Nascita ed evoluzione

La tecnologia blockchain, in italiano catena di blocchi, è una struttura dati decentralizzata, condivisa e crittograficamente immutabile¹. Questa tecnologia si fonda su un sistema di registro distribuito, formato da dati, informazioni o transazioni che vi vengono inserite e si sviluppa sulle potenzialità di una rete informatica di nodi, nodi a cui è sottoscritta la responsabilità di inserimento e validazione dei dati.

In questo registro aperto le informazioni vengono raggruppate in blocchi concatenati tra loro grazie alla crittografia, ed è proprio questa catena di blocchi validata e condivisa tra i vari nodi che rende i dati inseriti non manomettibili.

A rendere la tecnologia rivoluzionaria è la possibilità di fare una transazione online in modo completamente sicuro senza affidarsi ad un agente terzo, ad un intermediario, che faccia da garante. Io vedo in questo passaggio la stessa carica innovativa di quando le persone, nel VII secolo a.C., iniziarono ad usare la moneta sotto l'impero di Creso.

Ho voluto accostare queste due innovazioni perché penso siano derivate dallo stesso bisogno fondamentale, o meglio dalla stessa mancanza, la mancanza di fiducia.

Nell'antichità un mercante che viveva di baratto doveva fidarsi del valore che la controparte offriva per lo scambio, doveva fidarsi della controparte riguardo allo stato di salute del bestiame, alla qualità delle sete, alla commestibilità dei cibi e più in generale doveva fidarsi che gli venisse corrisposto un bene che sarebbe poi riuscito a scambiare nuovamente. Ai giorni d'oggi abbiamo perso la fiducia verso le persone e ci affidiamo con regolarità ad istituti che ci fanno sentire tutelati, ma cosa accadrebbe se questa fiducia venisse meno?

Le recenti crisi bancarie ci hanno fatto ripensare al paradigma dell'intermediario fiduciario e dalla rinnovata mancanza di fiducia provata da qualche soggetto che potremmo chiamare anarchico è così nata l'idea di blockchain e di criptovaluta, una moneta "libera" cui garantisce la tecnologia stessa, grazie alla quale non si debba sottostare ad un governo centrale o ad un intermediario finanziario. In realtà il concetto di blockchain non nasce con bitcoin, ma nasce ancora prima dell'intero mondo dell'informatica.

¹ Gian Luca Comandini. *“Da zero alla luna, quando come perché la blockchain sta cambiando il mondo”*. 2020

Ci troviamo nell'isola di Yap in Micronesia, gli abitanti dell'isola riescono ad approdare a Palau, un'isola a circa 400km di distanza nell'Oceano Pacifico e lì vi trovano delle strane rocce. Queste rocce sono scure ed hanno un buco al centro (figura 1), gli abitanti di Yap erano così affascinati da queste rocce che decisero di portarle a casa con loro e renderle delle unità di scambio, delle valute, le chiamarono Rai.



Figura 1: Antichi Rai trovati sull'isola di Yap

Cosa accomuna Bitcoin ad una roccia con un buco al centro? In realtà più di quanto possiamo pensare. Per entrambe non esiste nessuna banca centrale che le regola, ma non solo, molte popolazioni usavano le conchiglie come forma di valuta già dall'antichità, ma gli abitanti dell'isola di Yap trovarono il modo per far sì che la gente si fidasse ad usare la “roccia-valuta”. Lo fecero attraverso l'uso di registri. Ogni abitante dell'isola possedeva un registro, una sorta di libro mastro, in cui scriveva ogni transazione che veniva effettuata, in modo che chiunque sull'isola di Yap sapesse a chi apparteneva ogni singolo Rai.

Quindi registri distribuiti e rete di “nodi” validatori, concetti fondamentali della blockchain, sorreggevano l'economia di un'isoletta già nel 1400. La blockchain, in modo sintetico, non è altro che un libro mastro decentralizzato, cioè distribuito ad una rete di computer, ciascuno dei quali contenente una copia del registro.

L'introduzione di questi concetti in ambito informatico risale solo al 1992, e la sua evoluzione può essere sintetizzata in tre passaggi chiave:

- 1) Timestamp: Nel 1991 Stuart Haber e Scott Stornetta trovarono il modo per assicurare l'autenticità di un documento digitale attraverso la marcatura temporale, il Timestamp². Utilizzarono un servizio di marcatura temporale, che al momento della ricezione del documento ne registra data e ora esatta conservandone una copia, così da poter confrontare il documento potenzialmente modificato e verificarne l'autenticità. Questa nuova tecnologia presentava però delle criticità legate al servizio di marcatura temporale, il TSS.

² Haber S, Stornetta W.S. “How to time-stamp a digital document”. Journal of Cryptology , Issue 3, 99–111, 1991.

I documenti salvati dal TSS potrebbero essere “rubati” dalla memoria; i limiti stessi della memoria potrebbero risultare un ostacolo per grandi documenti; i documenti potrebbero danneggiarsi durante la trasmissione oppure il TSS potrebbe contrassegnare data e ora inesatti.

Per risolvere questo problema Haber e Stornetta svilupparono un meccanismo di hasing crittografato, in questo modo al TSS veniva trasmesso l’ID univoco del documento, riducendo gli spazi di archiviazione e le problematiche legate alla privacy. Abbinarono a questo sistema anche la firma digitale del mandante a garanzia della avvenuta ricezione, e sottoscrizione con data e ora corretti, da parte del TSS

- 2) Alberi di Merkel: Nel 1992 Dave Bayer ha implementato questa tecnologia architettando delle strutture ad albero in grado di verificare in modo sicuro ed efficace grandi quantità di dati³. I “Merkel Trees” sono formati da nodi “foglia” contrassegnati da un blocco dati, e da nodi “non foglia” contrassegnati dall’ hash crittografico delle etichette dei loro nodi foglia corrispondenti

- 3) Bitcoin: Come annunciato in precedenza la Bitcoin Blockchain nasce da un moto rivoluzionario, è molto di più che un’innovazione tecnologica, è la volontà di liberarsi dal sistema e ridefinire il concetto di fiducia, garantendo integrità e sicurezza dei dati. Di fatto il primo blocco mai generato su questa blockchain il 3 gennaio 2009 riporta la frase “chancellor on brink on second bailout for bank” ossia “il cancelliere sta per effettuare il secondo salvataggio per le banche” riferendosi all’ennesimo salvataggio di qualche banca fatto a spese dei contribuenti. Risulta chiaro da queste parole che per Satoshi Nakamoto, pseudonimo dell’inventore di Bitcoin, la crisi del 2008 aveva messo in luce le debolezze e le instabilità che un sistema finanziario centralizzato possa riscontrare. L’utilizzo di un database distribuito consentì a Nakamoto di risolvere il problema del double spending che faceva rimanere legato il mondo delle transazioni digitali agli intermediari. Il double spending consiste nella possibilità di inviare lo stesso denaro nello stesso istante a due o più soggetti diversi, era quindi impossibile, prima dell’avvento della blockchain, verificare se il denaro necessario per una transazione fosse stato già speso.

1.2 Meccanismi di consenso

³ Bayer, Dave & Haber, Stuart & Stornetta, W. “Improving the Efficiency and Reliability of Digital Time-Stamping”, 1999.

Una grossa criticità che Nakamoto ha dovuto affrontare durante la nascita del suo progetto riguardava i meccanismi di consenso, in assenza di intermediari risultava indispensabile un alto livello di collaborazione, era necessario un meccanismo che mettesse d'accordo tutti i nodi della rete riguardo l'ordine delle transazioni. Il meccanismo di consenso adeguato è stato trovato, un meccanismo in grado di risolvere il problema dei generali bizantini⁴.

Delle truppe bizantine con i loro generali sono accampate fuori dalle mura di una città nemica pronte ad assediare o a ritirarsi, in base al volere degli altri generali. La maggioranza dei votanti deciderà il da farsi, ma i generali, che comunicano attraverso messaggeri, potrebbero risultare dei traditori che comunicando un messaggio sbagliato porterebbero ad un attacco, o ad una ritirata, non coordinate e alla conseguente sconfitta.

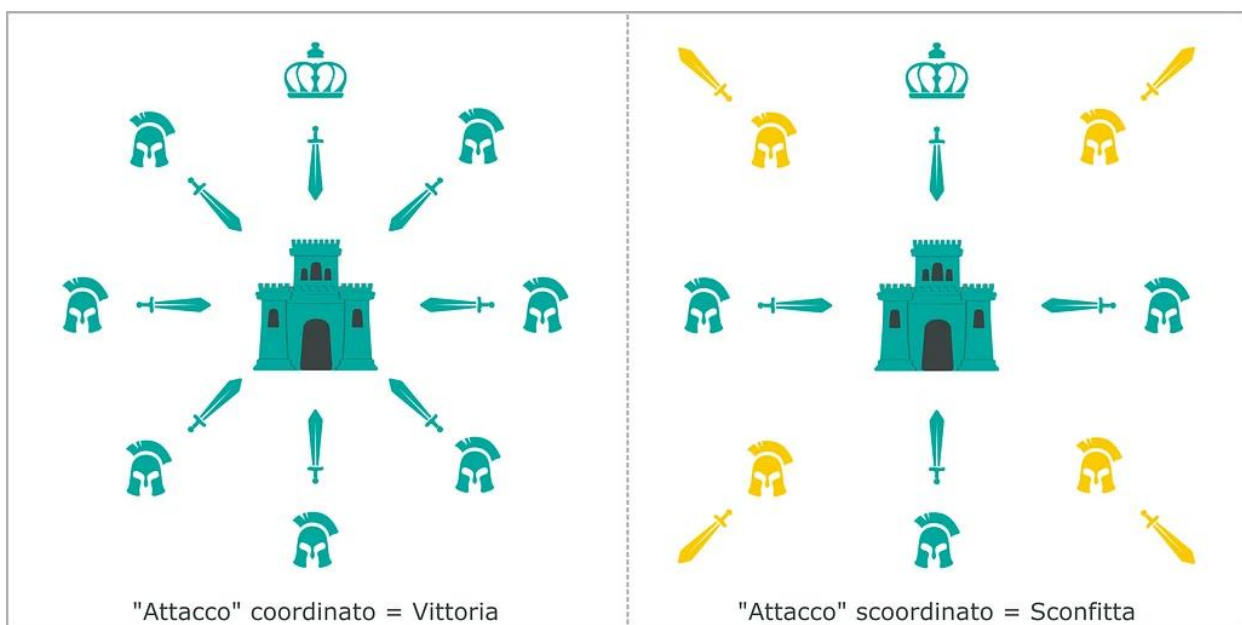


Figura 2: problema dei generali bizantini

La metafora indica la possibilità di errore e corruzione di un nodo in un sistema decentralizzato. Il meccanismo di consenso applicato alla blockchain elimina questa possibilità, facendo in modo che ogni attore verifichi la veridicità delle informazioni trasmesse durante le transazioni, respingendo quelle non autentiche. Una volta approvate le operazioni vengono inserite sulla rete rendendole immutabili e visibili da tutti gli attori.

1.3 Funzionamento

⁴ Lamport, Leslie & Shostak, Robert & Pease, Marshall. "The Byzantine Generals Problem", 2002.

L'infrastruttura elementare di una blockchain è formata da un database distribuito, un meccanismo di consenso e dai tokens. In questa parte del documento prenderemo in considerazione la Bitcoin blockchain che è formata dai seguenti elementi principali:

- **blocchi, transazioni e nodi**

L'architettura di una blockchain è una lunga catena formata da blocchi di dati che contengono le transazioni, protetti da una crittografia a chiave pubblica e privata e da firme digitali. Le transazioni consistono nello scambio di risorse digitali e vengono memorizzate in una rete peer-to-peer distribuita. I nodi servono per far rispettare i meccanismi di consenso, ed hanno la funzione di scegliere quali transazioni devono essere mantenute nella blockchain per garantire la corrispondenza tra i diversi rami.

- **hash**

La funzione hash fornisce la capacità di identificare un blocco in maniera inequivocabile e serve per convertire un messaggio in stringhe di grandezza predeterminata. Questo processo viene definito mappatura, la mappatura consente di creare una stringa dalla quale sarà impossibile risalire al messaggio. Oltre ad avere il proprio hash, ogni blocco possiede l'hash del blocco precedente, così da rendere più facile il processo di validazione e controllo nella catena.

- **registro (ledger)**

Esistono 3 tipi di registri o network:

- rete centralizzata (centralized): il network dipende da un intermediario. Se questo dovesse essere attaccato o smettere di funzionare l'intera rete si fermerebbe (figura 3a).
- rete decentralizzata (decentralized): i nodi dialogano tra loro, se un nodo venisse attaccato il resto della rete continuerebbe a funzionare (figura 3b).

- rete distribuita (distributed): tutti i nodi hanno stessa autorità, possono vedere tutto ed esiste un sistema di timestamp distribuito (figura3c).

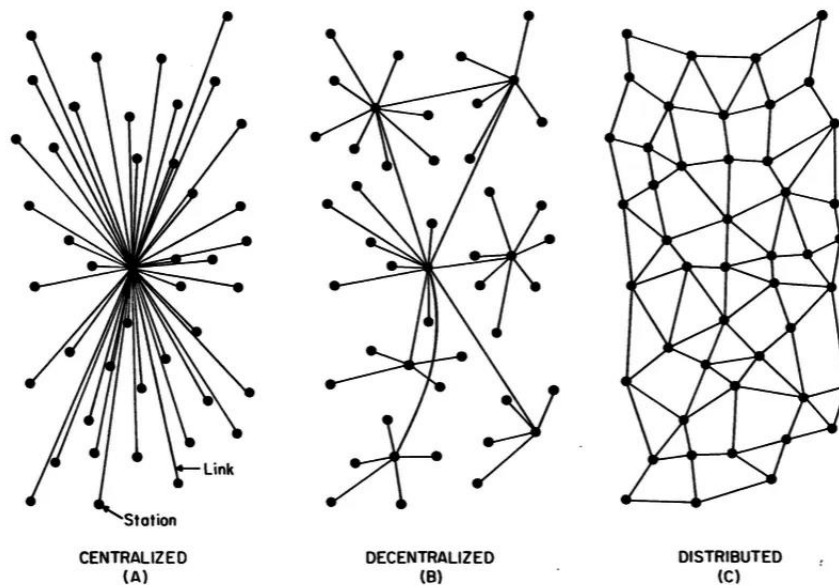


Figura 3: rappresentazione grafica delle tre distinte tipologie di network

La blockchain sfrutta l'ultimo sistema, per ovviare ai problemi dati dai primi due. Il registro distribuito, anche chiamato ledger, prende nota delle transazioni e di conseguenza fornisce sempre informazioni adeguate sullo stato della catena. Grazie al registro tutti i nodi posseggono informazioni aggiornate in tempo reale sulla catena rendendo impossibile, dal punto di vista di potenza di calcolo, una manomissione dei blocchi.

-miners

Il processo di convalida dei blocchi e inserimento nella catena viene definito mining, il miner è il nodo coinvolto in questo processo. Il miner approva la validazione di un blocco attraverso la risoluzione di problemi matematici. Questo processo prende il nome di "proof of work", nella Bitcoin blockchain ogni utente può mettere a disposizione la propria CPU per verificare e raggruppare le informazioni che ancora non sono state inserite in un blocco e svolgere questo complicato problema matematico. Il lavoro dei miners è fondamentale ed essi vengono quindi ricompensati con dei token. I token sono l'insieme delle informazioni digitali che conferiscono un diritto ad uno specifico soggetto. Bitcoin è il primo e più "famoso" token, ma ad oggi ne esistono a migliaia di diversi tipi.

1.4 Tipologie di blockchain

La blockchain di cui abbiamo discusso in questo documento è definibile pubblica. Col passare del tempo si è optato anche per tipologie diverse di blockchain, spesso distanti dai principi filosofici che

hanno portato alla creazione di questa tecnologia, ma che comunque riescono a garantire la sicurezza dei dati. Le tipologie in questione sono:

Blockchain pubblica: In questa blockchain chiunque è in grado di diventare un nodo della rete; chiunque è in grado di far parte del meccanismo di consenso diventando un miner e chiunque può effettuare e validare le transazioni, che saranno poi inserite nei vari blocchi. Questa tipologia viene definita “completamente decentralizzata” e garantisce la sicurezza verso qualunque attacco esterno⁵.

Blockchain privata: In una blockchain privata tutte le operazioni di scrittura all’interno dei blocchi avvengono in maniera centralizzata. Le operazioni di lettura possono essere invece pubbliche o limitate ad un certo numero di utenti. Queste caratteristiche rendono la blockchain privata più vicina agli odierni modelli di business, è infatti molto usata nel settore finanziario.

Blockchain permissioned: Si differenzia dagli altri perché il meccanismo di consenso viene gestito da specifici nodi preselezionati. Viene definita anche blockchain “decentrata”, perché il potere è distribuito ad un insieme di nodi definiti “congresso”. Anche in questo caso la lettura dei blocchi può essere pubblica o limitata ad alcuni utenti.

La tabella riassume le principali differenze tra le blockchain

BLOCKCHAIN	PUBBLICA	PERMISSIONED	PRIVATA
Determinazione consenso	Tutti i miner	Nodi selezionati	Nodi selezionati
immutabilità	forte	Non definita	Non definita
Permesso di lettura	pubblico	Pubblico o limitato	Pubblico o limitato
centralizzazione	no	circoscritta	si
efficienza	Bassa	alta	alta
token	si	dipende	no

1.5 Oracoli

La produzione di programmi affidabili, sicuri e a prova di manomissione è oggi possibile grazie allo sviluppo di applicazioni blockchain e contratti intelligenti. Tuttavia, queste garanzie fornite dalla

⁵ Vitalik Buterin, 2015. Accesibile: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

blockchain esistono perché l'ecosistema è per sua natura limitato a tutto ciò che non sembra essere on-chain, rendendo inaffidabile tutto ciò che è al di fuori dell'ecosistema.

Il requisito dell'interazione tra i programmi on-chain e quelli off-chain, o esterni alla blockchain, diventa sempre più importante con l'aumentare della complessità delle applicazioni decentralizzate. La condivisione delle informazioni tra le parti è diventata particolarmente importante perché il costo della computazione o della memorizzazione in un ambiente blockchain è spesso diventato proibitivo a causa dei limiti dei blocchi.

Grazie a una terza parte che funge da ponte tra ciò che è attendibile sulla catena e ciò che non lo è (tutto quello al di fuori della catena) è possibile entrare in contatto con elementi esterni alla blockchain. Oracolo è il termine utilizzato per indicare questi intermediari. La scelta di questo appellativo allude alla capacità di queste terze parti di rispondere a richieste che sono al di fuori dell'ecosistema blockchain, ma che possono essere considerate legittime.

Il paradigma della blockchain è pensato per essere decentralizzato, ma con questo nuovo tipo di entità terza, tutte le informazioni provenienti dall'esterno sono fornite dall'oracolo stesso, che per le sue qualità può essere considerato come dotato di una qualche forma di autorità centralizzata. La fiducia di questa parte ponte è un problema significativo che non è stato risolto. Poiché i contratti intelligenti si affidano a queste informazioni, anche se sono state alterate o filtrate, l'oracolo centralizzato in questo scenario rappresenta un collo di bottiglia.

1.5.1 Possibili soluzioni

Il principio degli oracoli decentralizzati viene utilizzato per risolvere parzialmente il problema dell'autorità centrale. Gli oracoli decentralizzati si basano su una rete di computer che funzionano come vari nodi; ognuno di questi è chiamato miner. Poiché dipende da come viene sviluppata la funzione aggregata degli oracoli decentralizzati, il problema è solo parzialmente risolto. L'algoritmo di consenso utilizzato per questo tipo di aggregazione varia tipicamente in base alle politiche di rete dell'oracolo. L'origine delle fonti non è presa in considerazione nella maggior parte dei casi; quindi, spetta allo sviluppatore selezionare solo entità affidabili per recuperare questo tipo di informazioni.

1.5.2 Come funzionano gli oracoli

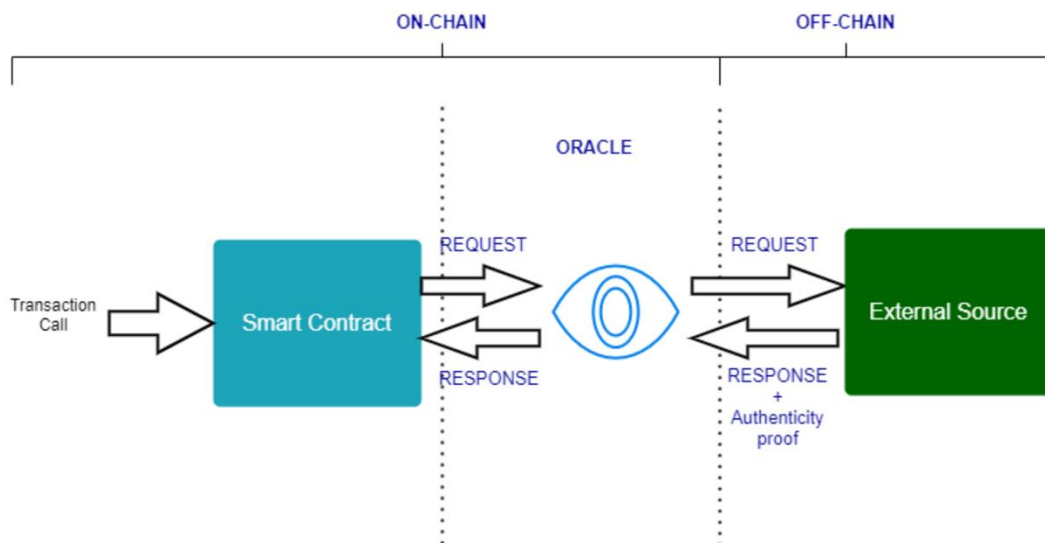


Figura 4: come funziona un oracolo

Gli oracoli hanno un'ampia gamma di utilizzi e alcune delle loro funzionalità comuni più utili includono l'ottenimento di dati dall'ambiente esterno alla catena o l'assegnazione di calcoli a fonti esterne. Alcune infrastrutture hanno implementato l'uso della rete decentralizzata di oracoli per garantire l'equità delle transazioni nell'ambiente blockchain (ad esempio DON). La raccolta di oracoli indipendenti in questa soluzione fornisce dati che non sono contenuti nella blockchain. Poiché tutto funzionerà per consenso e senza la necessità di un'unica autorità centrale, ciò aumenterà la sicurezza del sistema. In DON, i nodi vengono scelti in base alla politica della rete e svolgono i compiti necessari. L'algoritmo di consenso verifica quindi l'accuratezza dei dati recuperati o calcolati e, a seconda della politica della rete, i minatori possono essere ricompensati per i loro sforzi o addirittura penalizzati se viene rilevata una frode. È necessario pensare ai minatori come a computer che eseguono software, ricevono e completano compiti. Il token unico della rete viene solitamente consegnato al minatore come pagamento per aver eseguito correttamente il suo lavoro. I contratti intelligenti utilizzano in genere un'interfaccia standardizzata per comunicare con gli oracoli. In generale, le interfacce oracolo forniscono alcune funzioni di interrogazione per recuperare/compilare i dati off-chain utili all'applicazione.

Capitolo 2

Ethereum

Ethereum è una piattaforma decentralizzata e open source, basata su un sistema di blockchain pubblica, che ha la caratteristica di creazione e pubblicazione di contratti intelligenti. La piattaforma è stata lanciata nel 2015 dall'ideatore Vitalik Buterin con l'intento di creare una piattaforma sulla quale fosse possibile creare e distribuire applicazioni decentralizzate sulla sua rete, le cosiddette Decentralized apps (Dapps). Mentre le funzionalità di Bitcoin si fermano alla possibilità di effettuare transazioni in tutta sicurezza; Ethereum è più simile ad un marketplace di servizi finanziari, giochi, social media e di molte altre applicazioni⁶, con lo scopo di creare una nuova generazione del world wide web, il web 3.0.

2.1 Smart contracts

Nick Szambo parlava di contratti intelligenti (smart contracts) già dal 1996, ma solamente l'avvento della piattaforma ethereum ha reso questa idea realizzabile⁷.

Gli smart contracts sono dei contratti auto eseguibili, che grazie alla blockchain rendono l'utilizzo di un intermediario superfluo, pur mantenendo la completa tutela delle parti. Più che di veri e propri contratti potremmo parlare di codici if-this-than that che leggono e verificano le clausole poste al momento della stipula e si auto-eseguono se la verifica ha esito positivo. Questo meccanismo, tornando all'argomento iniziale, consente di eliminare la necessità di un rapporto fiduciario tra le parti perché il contratto è sia definito sia eseguito dal codice stesso.

I contratti intelligenti hanno 3 caratteristiche principali:

- autonomia: i contratti si eseguono nel momento della sottoscrizione; quindi, una volta sottoscritto non c'è bisogno che le parti rimangano in contatto tra loro
- autosufficienza: gli smart contracts sono in grado di "gestire" le risorse ossia raccogliere i fondi necessari emettendo servizi
- decentramento: i contratti essendo sulla rete sono decentralizzati e distribuiti

2.2 Ether e proof of stake

⁶ Sito ufficiale Ethereum, ultimo aggiornamento settembre 2015. Accesibile: <https://ethereum.org/it/what-is-ethereum/>

⁷ Szabo N. "Smart Contracts: Building Blocks for Digital Markets", 1996.

Ether (ETH) è la criptovaluta nativa della piattaforma ethereum. Oltre ad essere una valuta scambiabile sulla piattaforma, viene generata dalla stessa come ricompensa per i miners.

Il meccanismo di consenso utilizzato viene definito “proof of stake”, in cui l’utente dovrà bloccare una parte dei suoi capitali per partecipare al processo di “forgiatura” dei blocchi. Con l’aiuto di una selezione casuale, l’algoritmo sceglierà il nodo che dovrà partecipare alla creazione del nuovo blocco, in maniera proporzionale alla quantità di attività messe in “staking”, cioè la quantità di capitale bloccata in precedenza. Ad esempio, se possiedo il 10% delle attività, allora parteciperò al “forging”, cioè alla creazione del nuovo blocco, per il 10%; in questo modo la rete risparmia energia e potenza, aumentando l’efficienza dell’ecosistema. Questo meccanismo conferisce anche un elevato livello di sicurezza, perché per manomettere un blocco sarebbe necessario possedere più della metà delle attività in circolazione

2.3 Gas

Ogni criptovaluta ha una piccola tassa associata all'invio di monete lungo la sua blockchain per evitare che gli utenti inondino la rete con transazioni infinite. Inoltre, l'invio di ETH tra portafogli Ethereum comporta dei costi che sono in genere pagati ai miners che convalidano le transazioni. Una commissione per le transazioni di ETH ha un'ulteriore utilità, in quanto la rete Ethereum applica delle commissioni per l'esecuzione di applicazioni che utilizzano la sua tecnologia blockchain. Queste commissioni sono anche chiamate "gas", poiché forniscono l'energia, o la potenza, necessaria per l'esecuzione delle applicazioni.

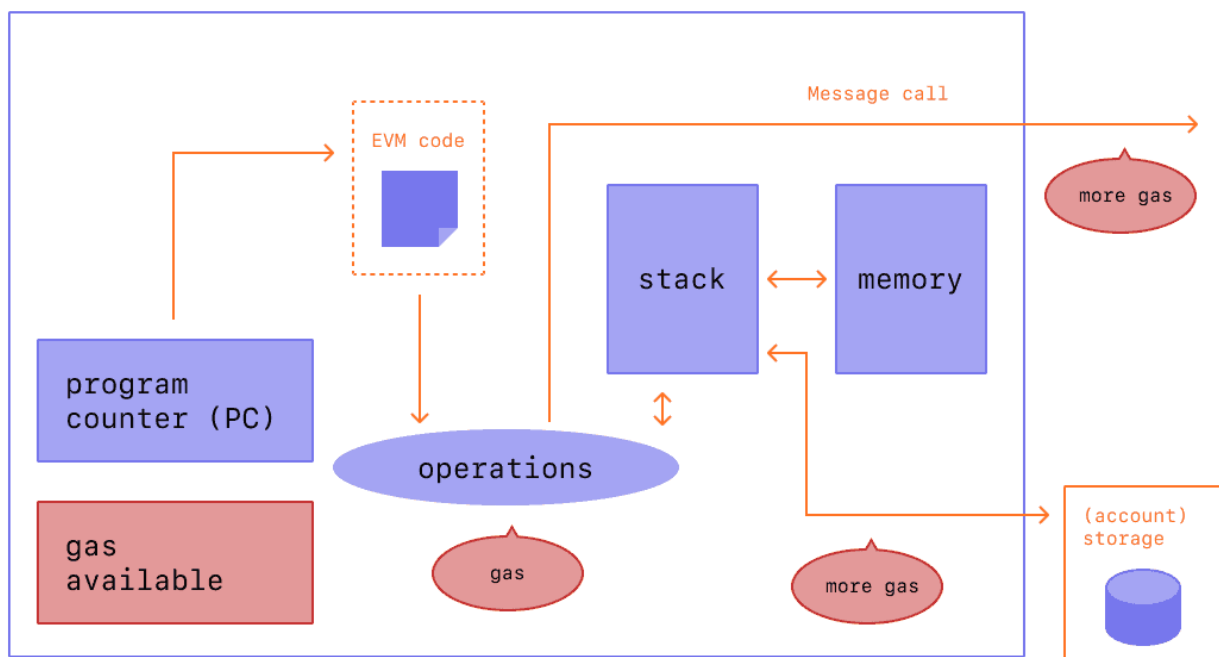


Figura 5: rappresentazione di come il gas viene "speso"

Il termine "gas" si riferisce alla metrica utilizzata per esprimere la quantità di lavoro computazionale necessario per eseguire particolari operazioni sulla rete Ethereum. Ogni transazione di Ethereum ha un costo, poiché tutte necessitano di risorse di calcolo per essere completate. Il costo per completare una transazione su Ethereum è la quantità di gas necessaria.

La valuta nativa di Ethereum, l'ether, viene utilizzata per pagare il gas (ETH). Ogni gwei equivale a 0,000000001 ETH (10^{-9} ETH). Ad esempio, si può dire che il gas costa 1 gwei piuttosto che 0,000000001 ETH. La parola stessa "gwei" indica un giga-wei, ovvero un miliardo di milioni di wei. L'unità più piccola di ETH si chiama Wei, dal nome di Wei Dai, l'inventore della b-money.

L'idea di b-money, presentata per la prima volta nel 1998 dall'informatico Wei Dai, era quella di creare un sistema di denaro elettronico distribuito e anonimo. Si sforzava di offrire molte delle caratteristiche e dei servizi che le moderne criptovalute offrono oggi.

Con l'aggiornamento di Londra dell'agosto 2021, è stato introdotto un nuovo metodo di calcolo delle commissioni di transazione sulla rete Ethereum. Quello che accadeva prima era il seguente:

Supponiamo che Elena debba dare a Francesco 1 ETH. Il limite di gas e il prezzo di questa transazione sono rispettivamente 19.000 unità e 300 gwei. Il costo totale sarebbe stato: unità di gas (limite) * Il prezzo unitario del gas, che è $19.000 * 300$, cioè 5.700.000 gwei (o 0,0057 ETH). Il conto di Elena verrebbe addebitato di 1,0057 ETH quando invia il denaro. 1 ETH verrebbe accreditato a Francesco. Il minatore otterrebbe 0,0057 Ethereum.

2.3.1 Il London upgrade

Il 5 agosto 2021 è entrato in vigore il London Upgrade per migliorare la prevedibilità delle transazioni su Ethereum per gli utenti. Una migliore stima dei costi delle transazioni, un'inclusione delle transazioni tipicamente più rapida e la compensazione dell'emissione di ETH bruciando una percentuale delle commissioni di transazione sono solo alcuni dei principali vantaggi apportati da questo adeguamento.

Ogni blocco ha una tariffa di base, che la rete determina in base alla domanda di spazio per i blocchi, a partire dall'aggiornamento della rete di Londra. Questa tariffa di base è il prezzo più basso per unità di gas da includere nel blocco. Gli utenti sono tenuti a fissare una mancia (tassa di priorità) nelle loro transazioni, oltre alla normale tassa di transazione, che viene bruciata. La mancia dovrebbe essere fissata a 1 dollaro e ricompensa i minatori per l'esecuzione e la propagazione delle transazioni degli utenti nei blocchi.

Prima dell'aggiornamento di Londra, i blocchi di Ethereum avevano dimensioni fisse. Questi blocchi funzionavano a pieno regime quando l'utilizzo della rete era elevato. Di conseguenza, gli utenti

dovevano spesso aspettare che la forte domanda diminuisse prima di essere aggiunti a un blocco, il che rendeva l'esperienza dell'utente pessima.

Ethereum ha ricevuto blocchi di dimensioni variabili come risultato dell'aggiornamento di Londra. L'obiettivo di ogni blocco è di 15 milioni di gas, ma la dimensione di ogni blocco fluttuerà a seconda della domanda della rete, fino al limite del blocco di 30 milioni di gas (2 volte la dimensione del blocco target). Grazie all'uso del tâtonnement, il protocollo riesce a raggiungere una dimensione di blocco di equilibrio di 15 milioni in media. Ciò significa che il protocollo aumenterà il prezzo base per il blocco successivo se la dimensione del blocco supera quella prevista. Analogamente, se la dimensione del blocco è inferiore a quella prevista, il protocollo ridurrà la tariffa di base. La tariffa di base viene modificata in base alla deviazione della dimensione del blocco corrente rispetto all'obiettivo.

2.3.2 Perché esistono le gas fees?

Le gas fees contribuiscono alla sicurezza della rete Ethereum. Per impedire agli utenti malintenzionati di spammare la rete, imponiamo un prezzo su ogni calcolo che viene eseguito. Ogni transazione deve stabilire un limite al numero di passi computazionali di esecuzione del codice che può utilizzare, per evitare loop infiniti involontari o dolosi o altri sprechi computazionali.

Anche se una transazione ha un limite, tutto il gas che non viene consumato in essa viene restituito all'utente.

Il termine "limite di gas" descrive la quantità massima di gas che si può utilizzare in una transazione. Le transazioni degli smart contracts, che sono più complesse, richiedono più lavoro di calcolo e richiedono un limite di gas più alto rispetto a un pagamento semplice. Il limite di gas tipico per un trasferimento di ETH è di 21.000 unità.

Ad esempio, se si imposta un limite di 50.000 unità di gas per un semplice trasferimento di ETH, l'EVM (Ethereum Virtual Machine) utilizzerà 21.000 unità di tale limite prima di restituire le restanti 29.000 unità. Se provassimo impostando un limite ad esempio a 20.000, L'EVM utilizzerà le 20.000 unità di gas nel tentativo di completare la transazione, ma fallirà se si imposta un limite di gas troppo basso. L'EVM annulla qualsiasi modifica, ma poiché il minatore ha già speso 20.000 unità di gas, quel gas viene utilizzato.

2.4 DAO, a Decentralized Autonomous Organization

Si tratta di una soluzione organizzativa inserita nella blockchain di Ethereum. Christoph Jentzsch è stato colui che l'ha presentata e sviluppata. È apparsa per la prima volta nel suo white paper chiamato

“Decentralized Autonomous Organizations to Automate Governance”, in cui spiega come realizzare il controllo distribuito del denaro da parte dei partecipanti in strutture di governance formalizzate e basate su software⁸. Il modello di governance di Slock.it (Il blog dei fratelli Christoph e Simon Jentzsch) È stato implementato dal team di Jentzsch allo scopo di consentire agli azionisti di esprimere il proprio voto su dove l'azienda dovrebbe spendere la propria liquidità.

Dopo il completamento del lavoro di sviluppo, più di 5000 persone si sono unite a The DAO Slack, un canale di comunicazione online, e si è creata una community in relazione al progetto open-source. Dopo aver distribuito "The DAO" su Ethereum il 30 maggio 2016 e aver raccolto quasi 150 milioni di dollari in sole quattro settimane, pari al 14% dell'intera quantità di ETH disponibile al tempo, è diventato il più grande progetto di crowd-funding fino a quel momento. Il fondo sarebbe stato utilizzato per investire nelle iniziative che gli venivano proposte e i suoi partecipanti avrebbe votato su tali progetti.

Il 26 maggio 2017, verso la fine della terza settimana di attività di The DAO, un gruppo di accademici ha chiesto una sospensione temporanea del progetto. Utilizzando un approccio basato sulla teoria dei giochi, hanno esaminato e descritto dieci modi distinti in cui la sua struttura può portare ad aggressioni e abusi. Il 6 maggio 2016, uno degli sviluppatori che lavorava su Ethereum, Christian Reitwießner, che all'epoca ricopriva il ruolo di Curatore, ha trovato una condizione nel linguaggio di programmazione Solidity che poteva essere sfruttata per attaccare gli smart contract. Questa condizione è stata successivamente identificata in The DAO da un utente del forum di The DAO Hub. Sebbene sia stato detto che non ci sarebbe stata alcuna perdita di ETH a causa di ciò, la falla era in realtà localizzata da qualche altra parte all'interno di The DAO. Il 17 giugno 2016, l'utente ledgerwatch ha pubblicato il seguente messaggio sul subreddit di Ethereum: "Sospetto che TheDAO sia stato prosciugato in questo momento". Un DAO figlio è stato finanziato utilizzando circa 50 milioni di dollari di ETH che erano stati rubati da The DAO da un "attaccante".

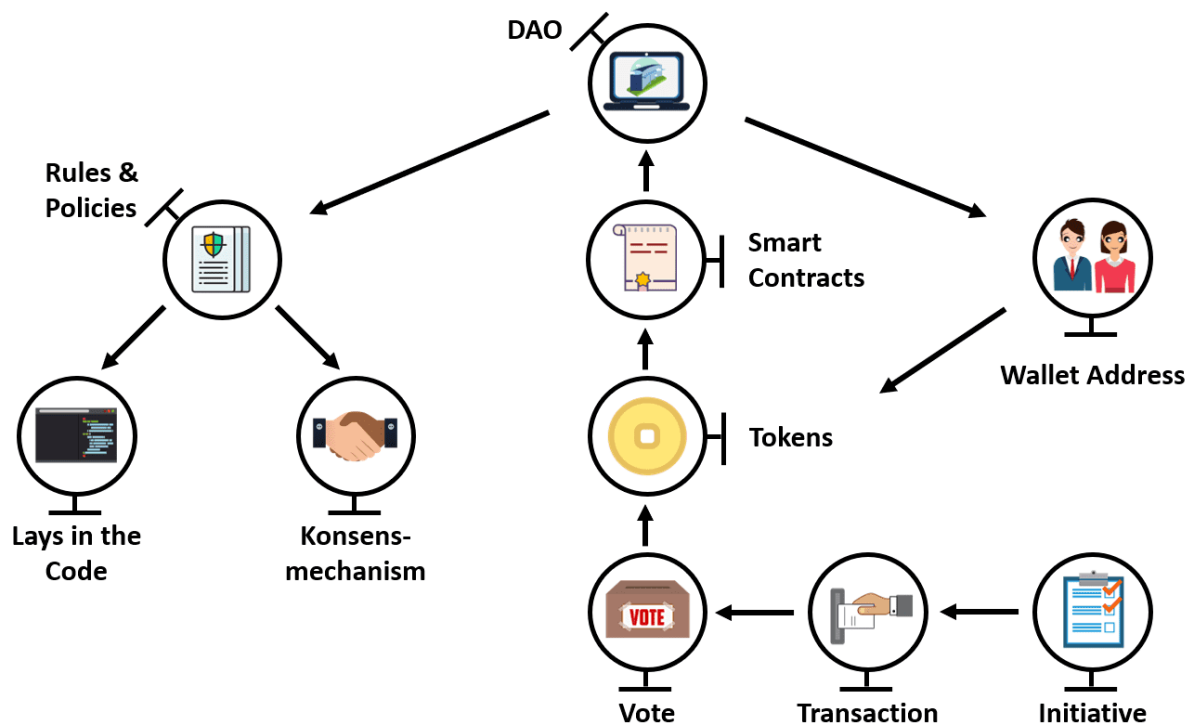
L'hard-fork che ha permesso il ritiro di tutti i token di The DAO è risultato l'unica soluzione possibile al problema. La maggior parte della comunità ha adottato questa opzione aggiornando il proprio client software. Tuttavia, la vecchia catena ha continuato a esistere e a essere minata, il che ha fatto sì che nascesse una copia precedente della blockchain di Ethereum, la chiamarono Ethereum Classic.

ETH può essere acquistato e venduto sulle borse delle criptovalute insieme a ETC, che è la nuova valuta della catena Classic. I trader di criptovalute hanno riconosciuto il valore immagazzinato nella catena ereditata, il che significa che i possessori di Ethereum ether hanno visto una "copia" dei loro

⁸ *Ethereum Classic Website, 201).* Accessibile: <https://ethereumclassic.github.io/>

token aumentare di valore sul mercato. La nuova comunità di Ethereum Classic è entusiasta di continuare la sua catena e ha avuto un certo successo nel farlo.

Nella catena di Ethereum Classic, "il codice è legge" e i minatori possono passare da una catena all'altra, così come gli investitori possono scambiare le due monete⁹. Inoltre, gli sviluppatori hanno la possibilità di scegliere per quale catena Ethereum creare espressamente.



2.4.1 Caratteristiche delle DAO

Nonostante l'ampia varietà di DAO, ci sono diverse caratteristiche che sono condivise da tutti, in questo capitolo ho provato a riassumerle.

Permission

Sebbene le organizzazioni autonome decentralizzate (DAO) siano attualmente sviluppate su blockchain per loro natura pubbliche e prive di permessi per entrarvi (permissionless), questa non è una regola per una DAO e gli utenti potrebbero dover ottenere un'autorizzazione prima di aderire.

Online-Native

La caratteristica principale delle DAO è che sono nate e cresciute nel regno digitale. Al momento, le organizzazioni autonome decentralizzate operano su Internet; tuttavia, non sono limitate e potrebbero,

⁹ Jentsch, C. (2016a). *The History of the DAO and Lessons Learned*. Medium. Accessibile: <https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5>, 22 October 2016

ad esempio, utilizzare una rete mesh. La Blockchain è la tecnologia utilizzata per le DAO, ma non c'è motivo per cui non si possa utilizzare un'altra tecnologia decentralizzata crittograficamente sicura.

Distribuite e decentralizzate

Shermin Voshmgir sostiene che nessuna DAO può essere completamente decentralizzata; ci sarà sempre una componente di centralizzazione e, di fatto, il codice della DAO è una sorta di centralizzazione¹⁰. La tesi di Shermin è che nessuna DAO può essere veramente decentralizzata. Il termine "decentralizzato" si riferisce al fatto che la DAO non è gestita da un singolo individuo o organizzazione. Nonostante le organizzazioni decentralizzate e le organizzazioni virtuali esistano da tempo, una DAO è caratterizzata dalla presenza sia di decentralizzazione che di regole rigorose applicate automaticamente.

Tra decentralizzazione e centralizzazione esiste una gamma di possibili risultati. Pertanto, sebbene il concetto di decentralizzazione per una DAO possa includere la nozione che ogni detentore di token possa proporre una modifica delle regole o richiedere denaro e che tutti i detentori di token possano votare sulla modifica delle regole o sulla richiesta di finanziamenti, in realtà ciò potrebbe non funzionare come previsto.

Ad esempio, potrebbe esserci un numero eccessivo di proposte dannose che, se realizzate, causerebbero danni significativi alla DAO o addirittura ne provocherebbero il completo collasso.

Anche proposte del tutto innocue potrebbero causare problemi perché potrebbero introdurre codice difettoso. Di conseguenza, alcune organizzazioni hanno incluso aspetti di centralizzazione, come l'inserimento di un consiglio che delibera sulle decisioni, e spesso permettono ai titolari di token di delegare i propri voti ad altri membri. Nonostante il fatto che l'uso dei consigli sembri accentrare il potere, sono stati progettati dei meccanismi per garantire che il potere non sia centralizzato. Ad esempio, i membri dei DAO hanno la possibilità di rimuovere e sostituire i membri del consiglio a piacimento, ed è richiesto che i membri continuino a fare proposte e a votare su tali proposte.

Anche se un certo grado di decentralizzazione è necessario, la formazione di una DAO non segue sempre l'ideale di una comunità che lavora insieme per farla nascere.

Al contrario, quello che alla fine sarà conosciuto come DAO è spesso concepito e costruito da un team molto piccolo. L'organizzazione autonoma decentralizzata non nasce finché non viene consegnata alla rete. Ovvero, fino a quando l'individuo o l'organizzazione che sta dietro all'iniziativa non rende possibile la partecipazione di altri alla governance. In particolare, non è possibile per gli autori della DAO o per qualsiasi altra entità possedere un numero significativo di token per esercitare un'influenza sulle sue operazioni.

¹⁰ Shermin Voshmgir, 'Tokenized Networks: What is a DAO?', Blockchainhub. 2019

Regole che si controllano da sole

Gli smart contract che compongono la DAO fungono da regolamento dell'organizzazione e, di fatto, da costituzione. L'implementazione di contratti intelligenti, che includono regole che si applicano automaticamente, garantisce che le regole di una DAO siano rigorose e che la governance non abbia altra scelta che rispettarle. Di conseguenza, i contratti intelligenti funzionano come dispositivi di pre-impegno.

Il modo in cui le regole vengono applicate nelle organizzazioni tradizionali e nelle organizzazioni autonome decentralizzate varia in modo significativo, e questa è una delle differenze più importanti. Nelle organizzazioni e istituzioni tradizionali, la presenza di regole, politiche e procedure non previene gli atti non autorizzati e, anche se il malfattore viene scoperto e punito, è di scarsa utilità per coloro che hanno subito un danno. In altre parole, la presenza di regole, politiche e procedure non previene gli atti non autorizzati. L'implementazione di contratti intelligenti all'interno di una DAO, di conseguenza, impone vincoli ex-ante e rappresenta un cambiamento rispetto alla costosa pratica del monitoraggio e dell'applicazione ex-post che è comune nelle istituzioni convenzionali. D'altra parte, le spese iniziali per la stesura di vincoli ex-ante potrebbero essere maggiori rispetto al prezzo della creazione di contratti standard.

Un altro aspetto delle regolamentazioni auto-applicative è che le restrizioni imposte da una DAO potrebbero non essere sempre limitate alle attività che si svolgono all'interno della DAO stessa. Ad esempio, i costi di transazione sostenuti dalle organizzazioni, in particolare quelle caritatevoli, nel processo di garantire che il denaro donato venga dato al destinatario appropriato, sono una sfida essenziale che occupa molte risorse alle organizzazioni. Una DAO potrebbe intervenire con una moneta programmabile, che avvalendosi dei contratti intelligenti, potrebbe, ad esempio, essere utile nel settore degli aiuti internazionali. Non solo per la durata del primo trasferimento, ma per qualsiasi periodo di tempo, un'organizzazione autonoma decentralizzata che distribuisce criptovaluta a un ente locale o a qualsiasi individuo può definire chi è autorizzato a ricevere la criptovaluta.

L'inflessibilità delle organizzazioni autonome decentralizzate potrebbe dare origine a un'ulteriore serie di sfide, che non si incontrano nelle organizzazioni convenzionali, poiché le DAO possono comportarsi solo in conformità al loro codice.

Una DAO corre il rischio di essere danneggiata o addirittura di terminare le sue operazioni se uno smart contract contiene un errore o non consente alla DAO di eseguire un'azione necessaria per la sua protezione. Tuttavia, le DAO sono costruite con la flessibilità di modificare le proprie regole. Per questo motivo, la governance da parte dei membri è una componente chiave di una DAO.

La governance

La capacità dei membri di amministrare una DAO, compresa la modifica delle sue regole, è fondamentale. La governance è più ampia di quella gerarchica. In quest'ultima, le scelte come chi assumere, quali appaltatori utilizzare e quanto pagarli sono operative e vengono fatte dalla direzione, mentre nella DAO i detentori di gettoni prendono decisioni operative e di governance, poiché una DAO non ha un management. La governance comporta quindi scelte operative.

Vitalik Buterin ritiene che il ruolo dei possessori di token nella gestione delle DAO sia simile a quello delle democrazie, in quanto i membri possono stabilire cosa fare e realizzarlo.

Le DAO utilizzano una varietà di strumenti di governance per aggiornare le regole.

Ad esempio, possono impiegare la governance on-chain oppure possono combinare governance onchain e offchain. Secondo molti una vera DAO richiede il 100% di governance on-chain, mentre altri non sono d'accordo e affermano che in genere è necessario un mix. Si può affermare che non tutte le scelte vengono fatte on-chain a causa dell'inerzia e del ritardo; potrebbe risultare impegnativo anche prendere decisioni come l'acquisto di alcune graffette. Realisticamente, è necessaria una soglia. Una possibile soluzione potrebbe essere individuare percorsi di proposta e di voto separati a seconda della proposta per costruire la governance e ridurre i tempi, i costi e gli sprechi delle piccole scelte sulla catena.

Se stai richiedendo fino a un ETH, puoi farlo in un giorno, non in una settimana, se invece stessi richiedendo un budget maggiore, come 10 ETH, vorresti più tempo per la discussione. Data la crescita delle strutture di governance e della tecnologia delle DAO, non è attualmente possibile classificare esclusivamente le DAO che impiegano una governance puramente on-chain.

L'uso del software open-source e delle sue norme influisce anche sulla governance delle DAO, perché Chiunque può eseguire il fork del codice, creando una nuova DAO.

Il fork è un meccanismo di governance che può verificarsi quando i membri non sono soddisfatti della governance del DAO.

Le DAO possono anche controllare e salvaguardare beni tangibili per i membri e i beni comuni.

le DAO non si limitano a riprodurre le tipiche organizzazioni gerarchiche, come alcuni avevano previsto, ma puntano anche alla controversa protezione delle risorse comuni. Garrett Hardin sostiene che se una risorsa, come un pascolo per gli animali, fosse libera di essere usata e consumata da tutti, verrebbe saccheggiata e di conseguenza tutti sarebbero più poveri.

Ogni agricoltore dovrebbe continuare ad aggiungere bestiame per raccogliere tutto il valore, l'eccesso di pascolo ridurrebbe il rendimento dell'agricoltore e il bestiame non si svilupperebbe con

la stessa velocità o peso. Hardin pensa che gli agricoltori continuerebbero ad aggiungere bestiame fino a quando il pascolo non sarà in grado di sostenerlo, portando distruzione a tutti. Hardin nel suo articolo “The Tragedy of the Commons (1968)” suggerisce che sia un attore centrale a governare i beni comuni e a regolare il consumo delle risorse¹¹.

Elinor Ostrom, studiosa premio nobel nel 2009, la pensava diversamente; Il lavoro della Ostrom fornisce una confutazione anche empirica, delle convinzioni ampiamente diffuse sulla "tragedia dei beni comuni". L'autrice ha studiato il processo attraverso il quale le comunità in molti luoghi diversi del mondo trovano strategie per regolare i beni comuni al fine di garantirne l'esistenza per i loro bisogni e per quelli delle generazioni future, trovando 8 punti comuni tra le strategie vincenti¹².

8 principi guida per l'amministrazione dei beni comuni

1. Stabilire in modo chiaro i confini del gruppo.
2. Adattare le norme che regolano l'uso dei beni comuni ai requisiti e alle circostanze specifiche dell'area.
3. Fare in modo che gli individui la cui vita è influenzata dalle regole abbiano voce in capitolo sull'evoluzione di tali regole.
4. Garantire il rispetto dei diritti dei membri della comunità a partecipare alla creazione delle regole da parte delle autorità esterne.
5. Creare un metodo di monitoraggio della condotta dei membri della comunità che sia svolto da membri della comunità stessa.
6. Implementare punizioni graduali per coloro che infrangono le regole.
7. Rendere i processi di risoluzione dei conflitti facilmente accessibili e convenienti.
8. Creare responsabilità per la regolamentazione della risorsa condivisa a livelli nidificati, partendo dal livello più elementare e arrivando fino al sistema collegato più complesso.

Le DAO adeguatamente costruite che amministrano i beni comuni possono soddisfare tutti i criteri di progettazione della Ostrom.

¹¹ Garrett Hardin, “the tragedy of the commons”, 1968

¹² Jeremy Williams. “Elinor Ostrom’s 8 rules for managing the commons”. Accessible: <https://earthbound.report/2018/01/15/elinor-ostroms-8-rules-for-managing-the-commons/>. 2018

In primo luogo, le DAO possono avere dei confini. In secondo luogo, possono essere prese in considerazione le esigenze locali. I membri possono modificare le regole e le autorità esterne possono riconoscere l'autogoverno dei membri. I contratti intelligenti rendono più facile il monitoraggio e l'applicazione delle regole della DAO e la trasparenza delle azioni può promuovere la responsabilità e il monitoraggio peer-to-peer; gli smart contract possono essere utilizzati per governare e promuovere la trasparenza e ridurre le violazioni delle regole; la trasparenza dei contratti intelligenti e l'auto-applicazione contribuiranno a risolvere i problemi e le terze parti potranno offrire una risoluzione delle controversie a basso costo.

A causa dell'abilità delle persone nell'aggirare le normative, Ostrom sostiene la necessità di una governance adattiva. La governance adattiva è fondamentale per le organizzazioni convenzionali e per le DAO per due motivi. In primo luogo, una DAO può eseguire solo ciò che è scritto; perché sono possibili errori nei contratti intelligenti. Nell'attacco a The DAO, una falla e l'impossibilità di modificare i regolamenti hanno permesso a qualcuno di rubare milioni di dollari e causarne la caduta. In secondo luogo, le DAO cambiano rapidamente e l'evoluzione delle regole è fondamentale. Se modificare le regole di una DAO fosse oneroso e richiedesse troppo tempo, i membri potrebbero abbandonarla e creare una DAO rivale.

2.4.1 La trasformazione della gig economy in comunità creative

Lo sviluppo dell'economia flessibile DAO combina gli aspetti più vantaggiosi della creator economy e della gig economy (ossia il modello economico basato sul lavoro occasionale e a chiamata), entrambe basate sul concetto di lavoro flessibile e freelance. Siti Web 2.0 come Fiverr hanno reso possibile l'accesso rapido a una forza lavoro qualificata di collaboratori indipendenti. Questo, tuttavia, ha comportato un notevole danno alle strutture occupazionali già esistenti, e spesso i freelance sono stati sottopagati o sottovalutati per l'impegno di tempo che si sono assunti.

Lo sviluppo successivo è stata la comparsa di siti online per il crowdsourcing, come Patreon. Grazie a questo sviluppo, i creativi non solo hanno potuto essere pagati, ma sono anche potuti entrare in contatto con i loro seguaci e costruire una comunità significativa intorno al loro lavoro creativo. In realtà di questi ecosistemi non ne beneficiano tutti i partecipanti allo stesso modo. Inoltre, la crescente rivalità per l'attenzione potrebbe essere stancante per la persona responsabile del progetto o per l'artista che vuole concentrarsi su ciò che gli piace di più.

I DAO stanno cercando di realizzare un cambiamento di paradigma sviluppando un ambiente che ricompensi contemporaneamente coloro che avviano i progetti e coloro che vi partecipano come membri della comunità. Grazie a questo concetto, ognuno è in grado di diventare un membro prezioso all'interno di un ecosistema che si basa su un argomento di cui è molto entusiasta.

Biconomy si è posto l'ambizioso obiettivo di creare questo tipo di piattaforma e punta a portare quante più persone possibili sulla sua piattaforma. Ha avviato un programma di sovvenzioni con un budget di 2 milioni di dollari per contribuire a portare avanti questo obiettivo. Il DAO fornirà ai membri della comunità sovvenzioni e premi per aiutarli a sviluppare applicazioni decentralizzate (dApp), educare il pubblico, migliorare l'infrastruttura di Web3 e incentivare nuovi utenti.

Secondo Ahmed Al-Balaghi, il creatore di Biconomy DAO, occorre affrontare due criticità principali per creare un ecosistema decentralizzato autonomo di successo. Il primo passo è quello di incoraggiare la partecipazione dei membri della comunità preesistente, illustrando i molti modi in cui possono dare il loro contributo. Il secondo passo consiste nell'avviare il processo di crescente decentralizzazione, ad esempio dando alla comunità il potere di scegliere come distribuire una sovvenzione di due milioni di dollari. Le persone potranno far sentire la propria voce attraverso l'uso del DAO di Biconomy¹³.

2.5 Web 3.0

Dalla nascita di internet l'innovazione applicata su questa tecnologia non si è mai fermata, quasi senza accorgercene siamo passati da pagine web statiche (Web 1.0), a social media e a siti web più dinamici e interattivi (Web 2.0), queste innovazioni hanno portato anche ad un maggiore grado di centralizzazione, ed all'impossibilità di mettere al sicuro i propri dati e la propria privacy. Da queste esigenze è nato il web 3.0.

Anche chiamato Web3, per il Web 3.0 non esiste una definizione unica, ma possiamo sicuramente dire che è l'insieme delle nuove tecnologie internet che si affidano all'intelligenza artificiale (AI), alla blockchain e al machine learning; con lo scopo di creare siti web, applicazioni e perfino economie digitali aperte, interconnesse ed intelligenti.

Per capire meglio cosa aspettarci dalla terza generazione del web potrebbe essere utile affrontare l'evoluzione che c'è stata negli ultimi due decenni, partendo dalla nascita del world wide web:

¹³ Lisa Gibbons. "DAO shall not be alone! Ecosystem DAOs on the rise". 2022

- WEB 1.0- Internet ai tempi era un insieme di pagine HTML statiche, senza possibilità di interazione, l'unica possibilità di scambi sociali era attraverso le prime chat ed i forum.
- WEB 2.0- Alla fine degli anni 90' internet prende una svolta più dinamica, dando la capacità agli utenti di interagire con i siti web attraverso moduli, database ed elaborazioni lato server. Gli utenti erano quindi in grado di modificare i dati ed inserire i propri. La potenzialità di questa innovazione non è passata inosservata e nel decennio successivo sono nati i social network e i servizi basati sul cloud.
- WEB 3.0- la nuova generazione del web punta a ridare in mano degli utenti i propri dati, argomento essenziale per la comprensione del capitolo successivo, attraverso tecnologie quali blockchain, open source, internet of things, realtà virtuale e aumentata, AI e molto altro ancora. In questa tabella ho voluto riassumere il processo¹⁴.

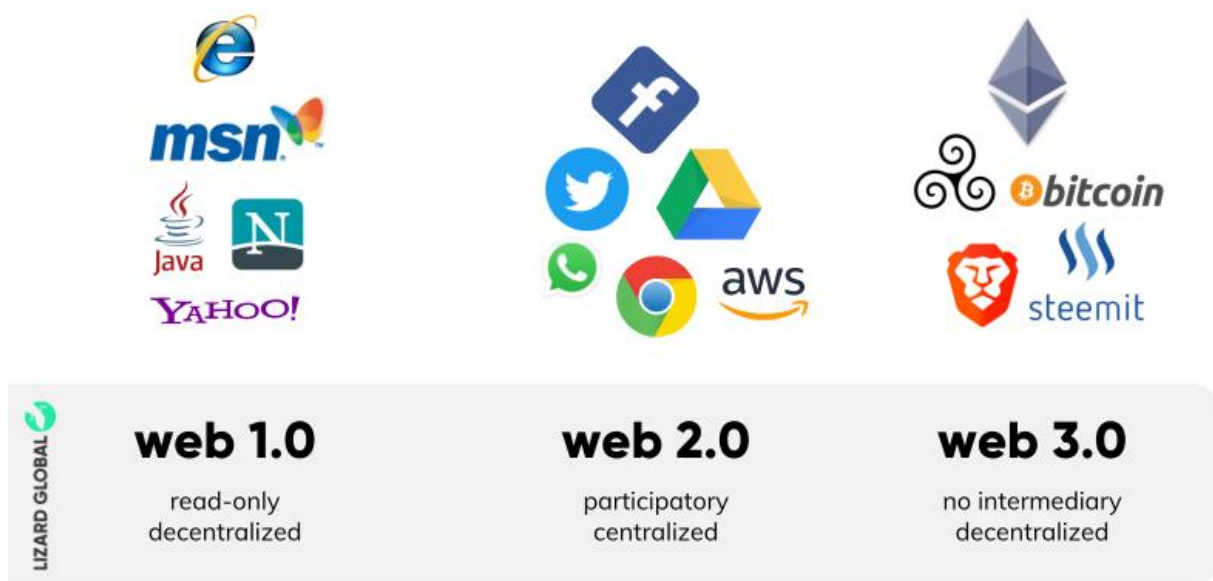


Figura 6: alcune dei players principali nelle tre generazioni (reperita da lizard.global)

	WEB 1.0	WEB 2.0	WEB 3.0
Contenuto	Interazione passiva	Community e creazioni degli utenti	I contenuti creati sono di proprietà dell'utente

¹⁴ Binance academy. Accessible: <https://academy.binance.com/it/articles/the-evolution-of-the-internet-web-3-0-explained>

tecnologie	HTML	HTML dinamico e javascript	Blockchain, AI, machine learning
Ambienti virtuali	mai	3D di base	3D, realtà aumentata e realtà virtuale
Archiviazione dati	Sui server dei singoli siti	Proprietà delle big tech	Distribuiti tra gli utenti
pubblicità	invasiva	interattiva	Targettizzata, basata sui comportamenti
pubblico	Utenti individuali	Community di utenti	Utenti interconnessi su più piattaforme e dispositivi

Mi interessa focalizzarmi sul contributo che la Blockchain ha apportato a questa nuova generazione. Grazie alla blockchain siamo riusciti ad ottenere un livello di sicurezza sulla proprietà dei dati che era quasi impensabile. La blockchain ha “creato” la possibilità per chiunque di “tokenizzare” un asset. Neanche questa innovazione è passata inosservata e si è quindi sviluppato un mercato enorme attorno ai Non Fungible Tokens anche detti NFT.

Capitolo 3

Non Fungible Token

I Non-Fungible Token (NFT) sono una sorta di criptovaluta che deriva dagli smart contract di Ethereum. L'idea iniziale di NFT è stata presentata in Ethereum Improvement Proposals (EIP)-721 e successivamente ampliata in EIP-1155.

Le qualità intrinseche degli NFT li distinguono dalle criptovalute convenzionali come il Bitcoin. Perché tutti i Bitcoin sono identici e intercambiabili. L' NFT, invece, è distinto e non fungibile (cioè non intercambiabile o sostituibile), il che lo rende adatto a identificare in modo univoco qualcosa o qualcuno.

Per essere più precisi, un creatore può facilmente dimostrare l'esistenza e la proprietà di beni digitali sotto forma di film, fotografie, opere d'arte, biglietti per eventi e tanto altro, sfruttando gli NFT su smart contract (in Ethereum). Inoltre, l'autore ha diritto a royalties per ogni operazione redditizia effettuata su qualsiasi mercato NFT o attraverso il trading peer-to-peer. L'NFT è in grado di trasformarsi in una potenziale soluzione per la protezione della proprietà intellettuale grazie alla piena negoziabilità, alla grande liquidità e alla semplice interoperabilità. Sebbene gli NFT siano essenzialmente solo codici, questi hanno un valore per un acquirente se si tiene conto della loro relativa rarità come oggetto digitale. La soluzione garantisce effettivamente prezzi di vendita per questi prodotti legati alla proprietà intellettuale che per gli asset virtuali non fungibili potevano sembrare inimmaginabili.

L'idea alla base degli NFT è stata ispirata da uno standard per i token di Ethereum che cercava di identificare ogni token con un elemento distintivo. Gli identificatori distintivi di questi token possono essere collegati a proprietà virtuali o digitali. Tutte le proprietà designate possono essere liberamente scambiate con valori personalizzati basati sulla loro età, rarità, liquidità e altri fattori. Il mercato delle applicazioni decentralizzate (DApp) ne ha tratto un notevole impulso.

Le tecnologie NFT sono ancora in fase iniziale, pur avendo un potenziale impatto significativo sugli attuali mercati decentralizzati e sulle future opportunità economiche. Mentre alcuni possibili ostacoli devono essere affrontati adeguatamente, altri offrono prospettive brillanti che dovrebbero essere riconosciute. Inoltre, nonostante il pubblico abbia accesso a una grande

quantità di informazioni sugli NFT attraverso blog, wiki, forum, codici e altre fonti, manca uno studio sistematico. Questo studio cerca di richiamare l'attenzione su questi problemi e di concentrarsi sul mondo della “Crypto-Art” e della speculazione nata dietro questo contesto.

3.1 I token fungibili e non fungibili

Gli NFT sono unità di dati conservate in un libro mastro della blockchain che verificano la legittimità di un bene digitale e forniscono al titolare del bene un certificato di proprietà. Gli NFT sono rari perché sono singolari e hanno una sola identità. Per i consumatori e i produttori di contenuti digitali, l'idea di scarsità crea il mercato ideale. Gli NFT servono come prova dell'identità della proprietà garantita dal libro mastro digitale. Come possiamo trarre vantaggio dalla mania degli NFT? In questo caso, la considerazione della non fungibilità è rilevante. I valori negoziati in base ai tassi di cambio sono il mezzo per scambiare denaro fiat come USD e EUR ; è irrilevante quali banconote vengano scambiate, perché ogni banconota ha un tasso di cambio variabile e lo stesso valore di ciò che è stampato su di essa. Gli NFT, invece, sono distinti: una volta creati, vengono aggiunti al libro mastro digitale pubblico e ogni volta che un token viene spostato, la sua proprietà o impronta cambia. Il proprietario dell'NFT ne mantiene i diritti in quanto inventore, e ogni persona che lo commercia o lo possiede è il rispettivo proprietario che riceve incentivi ogni volta che c'è un trasferimento di proprietà. Questa è una considerazione cruciale per l'analisi del valore.

Il modo in cui valutiamo le cose nel mondo reale è cambiato grazie alla nozione di token. Sono token anche documenti come carte d'identità, patenti di guida e biglietti aerei, che sono utilizzati nella nostra vita quotidiana e possono essere di diversi tipi, alcuni transitori e altri permanenti. Ognuno di essi ha un attributo, che viene registrato sul libro mastro globale basato sulla blockchain, ad esempio. Quando si considerano i vari tipi di token, come i token di accesso, i token di sicurezza, i token di criptovaluta, i token di identità e così via, è importante tenere presente che possono spaziare dalla concessione di diritti di accesso, a una semplice opera d'arte digitale visiva che ne attesta l'autenticità fino a consentire agli utenti di accedere a un caso commerciale specifico, come un biglietto aereo. Il vantaggio di un biglietto aereo è che ci permette di utilizzare i servizi della compagnia; tuttavia, una volta completata l'operazione, il biglietto è inutile. La stessa filosofia si applica agli NFT, ma di tipo digitale.

Un NFT viene emesso con un certificato di autenticità sulla blockchain, dimostrando al mondo che non esistono altri token simili. Di conseguenza, questi gettoni sono rari e unici nel loro genere. ogni NFT è salvato su una blockchain pubblica e aperta al pubblico controllo (spesso quella di Ethereum). Di conseguenza, i token non fungibili (NFT) presentano alti gradi di verificabilità, resistenza alla manomissione, usabilità e tracciabilità.

È difficile stimare il valore reale degli NFT approfittando dell'attuale frenesia che Internet sta vivendo. Con lo sviluppo di CryptoKitties, CryptoPunks e altri innumerevoli progetti che emergono ogni giorno, l'ossessione per l'arte digitale è aumentata. Tuttavia, la validità o la prova della proprietà di questi beni digitali è semplicemente un certificato fornito al proprietario del bene. Per i consumatori e i produttori di contenuti digitali, l'idea di scarsità crea il mercato ideale. Di conseguenza, gli NFT fungono da identificazione estetica sul libro mastro della blockchain che trasmette un diritto di proprietà. Con l'intreccio dei suoi marketplace e lo sviluppo in altri domini come il gaming, il metaverso e l'industria creativa, i casi d'uso significativi degli NFT stanno aumentando. Gli NFT sono vulnerabili a due fattori principali: in primo luogo, l'idea di autenticità percepita associata all'oggetto fisico e, in secondo luogo, l'accumulo di valore basato sulla proprietà. Le carte collezionabili sono state a lungo una forma comune di scambio e raccolta di valore nella nostra società. La loro unicità ne ha aumentato il valore. Da quando, nel XIX secolo, il baseball e la fotografia sono stati combinati per creare le carte da baseball, il carattere fisico delle carte da gioco ha permesso al grande pubblico di influenzare la formazione della comunità.

La rarità, il valore futuro previsto e la provenienza degli NFT sono gli elementi che li rendono preziosi. La provenienza è data dalla storia della proprietà e dal certificato di proprietà. Un'illustrazione emblematica di ciò è il dipinto della Monna Lisa, che ha il diritto di essere prezioso perché è stato in possesso di importanti re. Non solo è un'opera d'arte fantastica, e lo è indiscutibilmente, ma i proprietari hanno attestato la sua autenticità e la proprietà è passata di mano in mano nel corso della storia. Gli NFT sono token costruiti sulla blockchain che riflettono la proprietà di contenuti che hanno valore per molte persone. Sebbene rappresentino solo una piccola parte del potenziale della blockchain, ci sono modi importanti in cui questa tecnologia potrebbe rilanciare i cambiamenti della società.

Teoricamente, la contestualizzazione della produzione di valore attraverso la proprietà può essere considerata tra i ruoli e i diritti di una persona (o più persone) che implicano un controllo

irrevocabile sulle risorse; storicamente, questa proprietà assegnata sui beni modella gli individui coinvolti nella creazione di valore. La proprietà è stata considerata dagli esperti del settore come un motore del valore economico. L'acquisizione di diritti di proprietà dà la possibilità di utilizzare le risorse in vari modi, dall'acquisto e dall'investimento, alla vendita con l'obiettivo finale di massimizzare la generazione di valore.

Tuttavia, la questione della proprietà sollevata riguarda il valore materiale o immateriale che l'NFT possiede in termini di tokenizzazione. Essere il proprietario di qualcosa dovrebbe, in teoria, dare il controllo totale su di esso e sul modo in cui lo si utilizza.

Gli NFT si stanno evolvendo in una "macchina del valore di tutto" o in un meccanismo per trasformare digitalmente qualsiasi cosa in gettoni in questo momento di transizione. Secondo le previsioni di Qin Wang, studioso esperto di blockchain, gli NFT collegheranno entità fisiche e digitali, creando un ponte tra il mondo reale e quello virtuale e facilitando gli scambi di valore. L'emergere di questo parallelismo è un argomento intrigante da studiare, poiché cambierebbe il modo in cui viene percepito il valore di massa se il mondo reale e quello virtuale fossero collegati. Nel mondo digitale, quando la proprietà cambia, il valore percepito è molto alto; tuttavia, quando la proprietà cambia nel mondo fisico, cambiano anche le strutture di proprietà associate, che sono molto difficili da accertare¹⁵.

3.2 mercati

Il mercato dei token non fungibili (NFT) dovrebbe registrare una notevole crescita di popolarità nel 2021. Il totale delle vendite giornaliere sul mercato degli NFT è passato da circa 183.121 dollari nel 2020 a una media di 38 milioni di dollari nel 2021 (statistiche ottenute dal sito nonfungible.com). Tra i casi di NFT si possono citare la vendita dell'artista Beeple, che ha venduto un'opera d'arte digitale per 69 milioni di dollari, e la vendita del primo Tweet pubblicato dal CEO di Twitter Jack Dorsey per 2,9 milioni di dollari. Entrambe le transazioni sono avvenute nel 2018. CryptoPunks e Decentraland sono altri due token non fungibili (NFT) di spicco. Le vendite totali della collezione CryptoPunks, introdotta per la prima volta da Larva Labs nel 2017, hanno superato il miliardo di dollari nel 2021. Dopo l'annuncio di Facebook di voler cambiare il proprio nome in Meta, il valore di MANA, il token nativo di Decentraland, una piattaforma di metaverso su cui gli utenti possono acquistare e vendere proprietà virtuali, è

¹⁵ Wang, Q., Li, R., Wang, Q. & Chen, S., 2021. "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. arXiv e-prints".

salito alle stelle del 400% e ha raggiunto il massimo storico di capitalizzazione di mercato di oltre 6 miliardi di dollari.

Gli NFT possono essere acquistati tramite mercati specializzati come Rarible, OpenSea e Axie Marketplace, tra gli altri. Su queste piattaforme gli investitori hanno la possibilità di negoziare il diritto di proprietà sull'asset sottostante l'NFT.

Secondo il report del sito <https://nonfungible.com/reports/2022/en/q2-quarterly-nft-market-report>; per quanto riguarda il mercato degli NFT si è visto un calo nel 2022 rispetto all'anno precedente. Nella tabella i dati a confronto:

	Q1 2021	Q2 2022
Volume totale di dollari scambiati	10.734.200	8.070.349
Volume delle vendite	12.639.781	10.105.697
Acquirenti	1.571.566	1.172.235
venditori	903.771	579.513
Wallet attivi	1.864.820	1.247.083
Prezzo medio	849	798

Inoltre, sempre con dati ricavati dal sito nonfungible.com, è interessante notare come il mercato sia frazionato tra le diverse tipologie di NFT esistenti:



3.3 Opportunità

I potenziali vantaggi degli NFT sono discussi in questa sezione, in particolare esamineremo varie aree che potrebbero potenzialmente beneficiare degli NFT.

Potenziamento dell'industria del gaming: Nel settore dei giochi, gli NFT offrono un grande potenziale non sfruttato. Esistono già diversi giochi che sfruttano le criptovalute, come CryptoKitties¹⁶, Cryptocats¹⁷, CryptoPunks¹⁸, Meebits¹⁹, Axie Infinity²⁰, Gods Unchained²¹ e TradeStars²². Gli utenti spesso hanno la possibilità di acquistare all'interno del gioco beni virtuali in edizione limitata o non comune, che possono poi rivendere con profitto. Anche grazie a questo incentivo un gran numero di investitori partecipa ai giochi, contribuendo all'aumento di popolarità degli NFT. L'NFT ha una serie di caratteristiche interessanti, una delle quali è la fornitura di registri di proprietà dei beni trovati all'interno dei giochi. Inoltre, supporta la marcatura economica della posizione all'interno dell'ecosistema, a vantaggio sia dei giocatori che dei creatori. In particolare, i creatori di giochi e di NFT sono anche gli editor dei “gadget”

¹⁶ Cryptokitties. Project Accessible: <https://www.cryptokitties.co>

¹⁷ Cryptocats. Project Accessible: <https://cryptocats.thetwentysix.io>

¹⁸ Cryptopunks. Accessible: <https://www.larvalabs.com/cryptopunks>

¹⁹ Meebits. Project Accessible: <https://meebits.larvalabs.com>

²⁰ Axie infinity. Project Accessible: <https://axieinfinity.com>

²¹ Gods unchanged. Project Accessible: <https://godsunchained.com>

²² Tradestars. Project Accessible: <https://tradestars.app>

(ad esempio, armi e skin) e possono ricevere royalties ogni volta che i loro oggetti vengono (ri)venduti sul mercato aperto. Si tratta di una situazione vantaggiosa per tutte le parti coinvolte. I giocatori hanno la possibilità di acquistare oggetti di gioco che sono personali ed esclusivi. Questo porterà alla creazione di un modello di business favorevole sia ai giocatori che agli sviluppatori, in cui entrambe le parti beneficiano del mercato secondario. Le prospettive per il futuro sono ottime e le comunità blockchain puntano a diffondere l'uso degli NFT in misura significativa, in modo da includere una varietà di diversi tipi di beni digitali.

Eventi virtuali che stanno prosperando: Gli eventi online tradizionali dipendono da enti di natura centralizzata che forniscono sia la tecnologia che la fiducia necessaria per partecipare. Gli usi della tecnologia blockchain sono ancora limitati a un campo ristretto di attività, nonostante la tecnologia abbia già assunto una serie di compiti, come il processo di raccolta di capitali (attraverso ICO, IFO, IEO, ecc.). Gli NFT sono in grado di ampliare significativamente lo spettro di utilizzo della tecnologia blockchain grazie alle qualità aggiuntive che possiedono (unicità, proprietà, liquidità). Per questo motivo, è possibile per ogni persona legarsi a un particolare evento, esattamente come avviene nella vita di tutti i giorni. A titolo esemplificativo, possiamo pensare alla vendita di biglietti per eventi. Quando si acquistano i biglietti in un tipico mercato di biglietti per eventi, i clienti devono riporre la loro fiducia in una terza parte. Di conseguenza, esiste la possibilità che un cliente acquisti biglietti fraudolenti o non validi, che possono essere contraffatti o che sono stati annullati. È possibile recuperare lo stesso biglietto estraendone le informazioni dopo che è stato venduto più volte come, in una circostanza estrema, potrebbe avvenire per fotografie pubblicate online. Il termine "biglietto basato su NFT" si riferisce a un biglietto che è stato emesso dalla blockchain e serve come prova del diritto di accesso a un qualsiasi evento, sia esso di natura culturale o sportiva. Al portatore di un biglietto basato su NFT è vietato rivendere l'oggetto dopo che è stato acquistato, poiché il biglietto è unico nel suo genere e in offerta limitata. Il contratto intelligente costruito sulla tecnologia blockchain consente un mercato trasparente per la compravendita di biglietti per eventi, a vantaggio di tutte le parti coinvolte, compresi il cliente e l'organizzatore dell'evento. Invece di affidarsi a terze parti, i clienti possono transare direttamente con lo smart contract per acquistare e vendere biglietti in criptovaluta in modo efficiente e affidabile.

Motivare la creazione del Metaverso: Il Metaverso è un luogo online comune e condiviso che supporta e facilita un'ampia varietà di attività digitali. In generale, si riferisce a un insieme di

metodi per creare un ambiente virtuale, di cui alcuni esempi sono la realtà aumentata e Internet. L'idea risale a diversi decenni fa e ha fatto notevoli progressi grazie al rapido sviluppo della tecnologia blockchain. Il mondo virtuale che esiste online può trarre grandi vantaggi dalla capacità della blockchain di mantenere la sua natura decentralizzata. I partecipanti a questa realtà alternativa alimentata dalla blockchain possono avere un'ampia varietà di casi d'uso interessanti, come giocare, presentare opere d'arte autoprodotte, scambiare beni e proprietà virtuali (come opere d'arte, terreni, nomi, riprese video, oggetti indossabili e così via). Inoltre, gli utenti hanno la possibilità di guadagnare dall'economia virtuale attraverso varie opzioni, possono allevare creature non comuni e poi venderle per ottenere i premi, oppure possono affittare le strutture (ad esempio gli uffici) a persone per guadagnare.

I progetti Decentraland²³, Cryptovoxels²⁴, Somnium Space²⁵, MegaCryptoPolis²⁶ e Sandbox²⁷ sono i più importanti esempi di tecnologia blockchain in azione. In realtà, l'ecosistema del metaverso comprende tutte le applicazioni sopra descritte. Data la complessità della situazione e la continua evoluzione che sta avendo, ho deciso di menzionarla qui separatamente solo perché è ancora in fase iniziale.

Collezioni digitali: Carte collezionabili, vini, foto digitali, film, immobili virtuali, nomi di dominio, gioielli, francobolli crittografati e altri beni reali e intellettuali sono alcune delle forme di oggetti da collezione che si possono trovare nel regno degli oggetti da collezione digitali. In questa frangente useremo le arti creative come esempio.

Per cominciare, gli artisti che creano con metodi più convenzionali hanno pochissime opzioni per esporre le loro opere. Poiché non ricevono sufficiente attenzione, i prezzi non possono rappresentare con precisione il valore reale delle loro opere, quindi le piattaforme su cui è stato pubblicato il loro materiale e le pubblicità impongono tariffe intermedie.

²³ Decentraland (mana). Project accessible: <https://decentraland.org>

²⁴ Cryptovoxels. Project Accessible: <https://www.cryptovoxels.com>

²⁵ Somnium space. Project Accessible: <https://somniumspace.com>

²⁶ Megacryptopolis. Project Accessible: <https://mcp3d.com>

²⁷ Sandbox. Project accessible: <https://www.sandbox.game>

Questo lavoro è stato diffuso sui social network. Gli NFT sono responsabili della conversione delle opere in versioni digitali conferendogli un'identità. Non è necessario che gli artisti trasferiscano la proprietà delle loro opere o dei loro contenuti alle agenzie. Questo dà loro una spinta significativa sotto forma di molti guadagni. Esempi comuni sono REPLICATOR di Mad Dog Jones venduto per 4,1 milioni di dollari²⁸ (figura 7), l'opera di Grimes (venduta per un totale di circa 6 milioni di dollari) e altre opere di notevoli criptoartisti come Beeple e Trevor Jones.



Figura 7: Replicator di Mad Dog Jones

Inoltre, nella maggior parte delle situazioni non è possibile per gli artisti ottenere royalties dalle vendite successive delle loro opere. D'altra parte, i token non fungibili (NFT) possono essere costruiti in modo tale che l'artista guadagni una quota fissa di royalty ogni volta che la sua opera d'arte digitale viene scambiata sul mercato (ad esempio, SuperRare, MakersPlace, Rare Art Lab e VIV3). Le opere d'arte digitali possono essere gestite e salvaguardate in modo efficace con questo metodo. Inoltre, alcune piattaforme, come Mintbase e Mintable, hanno sviluppato strumenti che consentono alle persone normali di generare facilmente le proprie opere NFT.

3.4 relazione tra NFT e criptovalute

²⁸ Mad dog jones. Accessible: <https://www.phillips.com/detail/mad-dog-jones/1>

Gli NFT e le criptovalute sono stati indissolubilmente legati fin dall'inizio delle rispettive epoche. La seconda è spesso necessaria per acquistare la prima, e gli stessi portafogli digitali possono essere utilizzati per detenere entrambe. La maggior parte delle persone che detengono NFT sono anche investitori in criptovalute, poiché i valori degli NFT sono espressi in denominazioni di criptovalute. Lo sviluppo delle crypto rende possibile l'esistenza degli NFT; dopo tutto, la legittimità e la proprietà di entrambi i tipi di attività devono essere verificate tramite transazioni blockchain.

A causa di tutte queste analogie, è logico supporre che le variazioni di valore delle criptovalute si ripercuotano sul valore degli NFT, e questo è esattamente ciò che accade. Tuttavia, cercando una chiara relazione di causa ed effetto tra la volatilità del mercato delle criptovalute e le fluttuazioni del prezzo dei NFT, scopriremo che tale relazione sta diventando sempre più difficile da trovare.

3.4.1 l'inverno delle criptovalute

Il termine "inverno delle criptovalute" viene spesso utilizzato per descrivere un periodo in cui il mercato delle criptovalute sta andando male. La situazione è analoga a una flessione del mercato azionario nota come bear market. Un inverno delle criptovalute è caratterizzato da un sentimento di mercato pessimistico e da un calo dei prezzi degli asset in media su un'ampia gamma di valute digitali.

La ricerca indica che gli inverni delle criptovalute hanno un effetto significativo sull'atteggiamento degli investitori. Osservando la storia dei prezzi delle criptovalute, a volte è semplice identificare un inverno delle criptovalute. Ciò è dovuto al fatto che un mercato ribassista può essere accompagnato da un calo percentuale dei valori delle criptovalute a due cifre. I modelli seguiti dai mercati delle criptovalute potrebbero seguire schemi paragonabili a quelli dei mercati azionari, con cicli di rialzo e ribasso.

Poiché le criptovalute sono ancora una classe di asset relativamente nuova, è possibile che i loro valori non tornino mai al punto in cui erano prima di un criptoinverno.

Ci sono stati altri casi di inverno delle criptovalute negli anni passati. Ad esempio, a partire dalla fine del 2017 e fino a dicembre 2020, il prezzo delle criptovalute ha continuato la sua

tendenza al ribasso ed è rimasto ben al di sotto dei massimi precedenti. Tuttavia, nel dicembre 2020, i prezzi sono schizzati ai massimi storici nel bel mezzo di un forte bull market.

Non esistono regole formali comunemente riconosciute che specifichino fino a che punto i valori delle criptovalute debbano scendere perché si possa parlare di criptoinverno. Tuttavia, i leader del settore e le persone influenti hanno la tendenza a riconoscere apertamente l'inizio di un inverno delle criptovalute, come è avvenuto all'inizio del 2022.

Preoccupazioni per i prossimi inverni delle criptovalute

A differenza del mercato azionario, che ha mostrato un andamento altalenante nel corso della sua esistenza, la storia delle criptovalute risale a poco più di un decennio fa. Qualsiasi inverno delle crypto può potenzialmente durare per un periodo di tempo infinito. Lo scenario peggiore per gli investitori sarebbe un inverno prolungato, che porterebbe i prezzi degli asset a diminuire costantemente fino a raggiungere lo zero.

L'uso e il commercio delle criptovalute sono regolati da un numero limitato di norme finanziarie. Anche se molte imprese che operano in questo mondo sono finite nel mirino delle autorità di regolamentazione, la stragrande maggioranza di esse continua a operare con pochissima supervisione. Ciò apre la strada a frodi e truffe, di cui i clienti devono essere sempre consapevoli, compresa la possibilità di subire perdite conservando le criptovalute per un periodo di tempo prolungato.

Le forze del mercato sono in ultima analisi responsabili della determinazione dei prezzi delle azioni e gli investitori dipendono dagli strumenti di ricerca fondamentale e tecnica per stabilire gli obiettivi di prezzo. Lo sviluppo di modelli di valutazione per le criptovalute è ancora agli inizi. Per questo motivo, esiste un rischio significativo che si crei un divario tra i prezzi delle azioni e quelli delle criptovalute.

Tutte le criptovalute saranno colpite dal Crypto Winter? L'inverno delle criptovalute ha in genere un effetto sulla maggior parte delle criptovalute. Durante questo periodo, gli investitori dovrebbero prepararsi a un calo generale dei prezzi di mercato, anche se è possibile che si verifichino alcune eccezioni.

Non è possibile fare una previsione esatta sull'inizio o sulla fine di un inverno delle criptovalute. Seguire le ultime notizie e monitorare l'attività dei forum su piattaforme di social media come

Twitter, Reddit e Discord può fornire indicazioni preziose sulla mentalità degli investitori e sugli investimenti che hanno pianificato.

La vendita dell'NFT CryptoPunk #4464 ha avuto luogo il 12 luglio e sono stati scambiati 2.500 ETH. Si è trattato della più grande vendita di NFT nei trenta giorni precedenti, e non di trenta giorni qualsiasi, bensì dell'inverno delle criptovalute che sarà registrato per sempre come quello dell'estate del 2022.

Tra il massimo storico del 2021 e la metà di luglio di quest'anno (2022), il valore delle criptovalute è sceso di 2.000 miliardi di dollari. La svalutazione è stata alimentata in parte dal fallimento della stablecoin nota come terraUSD [Appendice], oltre che dalla bancarotta di Three Arrows Capital e dal calo del settanta per cento del valore del Bitcoin, la criptovaluta di maggior valore al mondo.

Anche se l'inverno delle criptovalute è stato il più “freddo” di sempre, è stato possibile ottenere un prezzo record per una delle collezioni di NFT più ricercate e per uno degli NFT più rari di quella collezione. Tuttavia, cosa implica esattamente?

La transazione CryptoPunk #4464 (figura 8) è ora al quarto posto con altre due vendite come la più alta vendita di NFT CryptoPunk nella storia della piattaforma ossia 2.500 ETH. Successivamente, CryptoPunk #4156 (figura 9) è stato venduto per 2.500 ETH nel dicembre del 2021. Nel febbraio del 2022, anche il CryptoPunk #5577 (figura 10) è stato acquistato al prezzo di 2.500 ETH.

Poiché la maggior parte degli NFT è registrata sulla blockchain di Ethereum, la maggior parte dei valori degli NFT è visualizzata in tagli di criptovaluta di ETH. Questo è il punto in cui il legame tra i prezzi delle criptovalute e i valori degli NFT è evidente. A causa della nota volatilità del mercato delle criptovalute, un legame tra tre diversi NFT non è affatto un legame.

Quando il mercato delle criptovalute era nella sua corsa al rialzo pre-invernale, si è verificata la transazione del CryptoPunk (CP) #4156. All'epoca, 2.500 ETH avevano un valore di 10,25 milioni di dollari. Dopo due mesi, il prezzo dei 2.500 ETH pagati per il numero #5577 della stessa collezione era sceso a 7,7 milioni di dollari. La transazione più recente, del CP #4464, avvenuta il 12 luglio, aveva un valore di soli 2,6 milioni di dollari, sempre per il corrispettivo di 2500 ETH.

Pertanto, tre investitori diversi hanno pagato un totale di 2.500 ETH per ciascuno dei tre NFT acquistati a pochi mesi di distanza l'uno dall'altro. Tuttavia, a causa delle variazioni di prezzo delle criptovalute, il "pareggio" risulta in una differenza di valore di 7,65 milioni di dollari tra il primo e il terzo posto.

CoinDesk ha proposto un paragone creativo per spiegare il legame tra criptovalute e NFT. Secondo questa analogia, le criptovalute sono il padre, mentre gli NFT sono i figli. Sebbene non sia esatta, semplifica una connessione finanziaria difficile e la rende più facile da comprendere. Quando il mercato degli NFT è nato, si trattava di una nicchia relativamente poco sviluppata che dipendeva dal mercato delle criptovalute per la direzione dei prezzi. Gli NFT sono poi maturati fino a diventare esseri grandi e potenti che desideravano la loro libertà.

Gli NFT si sono “ribellati” e hanno registrato un'impennata proprio quando i valori delle criptovalute stavano crollando, in modo simile al comportamento degli adolescenti ribelli che sopravvalutano la loro preparazione al mondo. Poi, dopo che il mercato degli NFT ha raggiunto la sua maturità e ha visto alcune delle dure realtà del mondo esterno, è tornato alle sue radici per ristabilire relazioni finanziarie con i suoi antenati crittografici.

Gli NFT sono destinati a essere integrati in piattaforme come eBay e Instagram, e l'attesissimo marketplace NFT di Coinbase dovrebbe consentire agli utenti di acquistare NFT utilizzando carte di credito e valute convenzionali. I progressi che si profilano all'orizzonte potrebbero quindi dissociare i token non fungibili (NFT) dalle criptovalute; ma, fino ad allora, gli NFT continueranno a rimanere vicini al nido anche se sono entità indipendenti.

Quindi Il prezzo delle criptovalute ha un effetto sul valore degli NFT? L'unica risposta affidabile è dipende dalla persona a cui lo si chiede. Secondo le statistiche presentate da Coinbase, c'è poca associazione tra NFT e criptovalute in termini di volume di vendite e di prezzi. Dall'altro lato, esiste una relazione causale tra il recente panico sul mercato delle criptovalute e il calo del prezzo degli NFT.

Per concludere, i token non fungibili a volte rispecchiano il movimento delle criptovalute a cui sono agganciati, ma non sempre. Ci sono alcuni fattori su cui la maggior parte degli esperti concordano che potrebbero spiegare il divario, e sono i seguenti:

- i mercati sono recenti.
- Ancora più di recente, e non ancora conclusa, è avvenuta la divisione dei due mercati.
- Entrambi stanno attraversando il loro primo bear market prolungato insieme.

In definitiva, il legame tra i prezzi delle criptovalute e i valori di NFT è oscuro, ma il quadro diventerà probabilmente più chiaro quando l'attuale inverno delle criptovalute sarà terminato.



Figura 8: CryptoPunk #4464

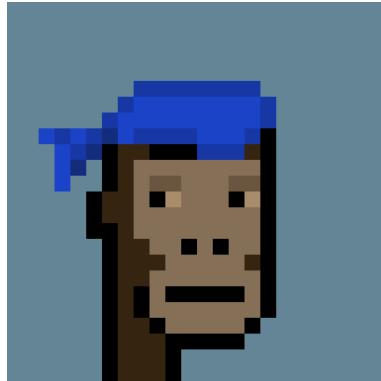


Figura 9: CryptoPunk #4156

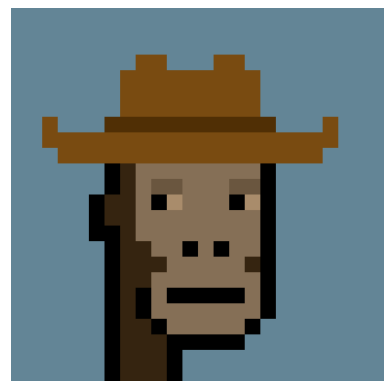


Figura 10: CryptoPunk #5577

Capitolo 4

Crypto-Art

Il concetto di bellezza viene talvolta confuso con quello di arte, eppure si tratta di un termine che, nella migliore delle ipotesi, è ambiguo. È necessario riconoscere che la realizzazione della bellezza come categoria estetica è storicamente specifica, essendo soggetta a convenzioni e mode, ed è anche necessario riconoscere che la realizzazione della bellezza non è sempre l'obiettivo dell'artista. Entrambi questi punti devono essere riconosciuti. Un obiettivo alternativo potrebbe essere quello di educare o illuminare lo spettatore su un argomento o una questione che riguarda la società, la politica o il discorso stesso dell'arte. Questo potrebbe assumere la forma di dibattiti intellettuali sull'astrazione, sui suoi sistemi di rappresentazione o sulle determinanti istituzionali del valore economico o qualitativo, per esempio.

In effetti, fin dall'inizio del XX secolo, un gran numero di artisti si è interessato a indagare varie questioni relative al valore, sia esso monetario o morale. Andy Warhol è l'artista più noto, secondo Oliver Roeder, il cui lavoro si è comportato in modi paragonabili alla cripto-arte. Secondo la spiegazione di Roeder nell'articolo "*The Blockchain Is Just Another Way To Make Art All About Money*"²⁹, Warhol ha espresso pubblicamente il suo desiderio di avere successo commerciale e di guadagnare molto denaro. Lo faceva perché voleva far conoscere le sue opere e il suo marchio al maggior numero di persone possibile. Si potrebbe scrivere molto sulle somiglianze e le differenze tra la pop art e la criptoarte, ma in questo documento vorrei soffermarmi solo sul paradigma che combina la creazione di opere d'arte con le transazioni monetarie. Per comprendere questo nuovo tipo di attività, si può fare riferimento alla storia dell'arte digitale (nota anche come "software art" dagli anni '60 e "Internet art" dagli anni '90).

Se paragonata all'arte tradizionale o convenzionale, la criptoarte viene talvolta presentata come una svolta rivoluzionaria; tuttavia, quando ne esaminiamo la forma, scopriamo che tende ad aderire alla logica un po' accademica dell'immagine bidimensionale e rettangolare (come un dipinto o un disegno). Poiché l'opera d'arte è progettata per essere vista attraverso uno schermo, come quello di un computer, di un telefono o di un tablet, la maggior parte della criptoarte ha colori vivaci e un'immagine enorme e accattivante che è al centro dell'opera. Per quanto ne sappiamo, sono pochi i casi in cui i professionisti dell'arte crittografica si sono confrontati con il sistema di valori impliciti

²⁹ O. Roeder. *The blockchain is just another way to make art all about money*. Accessibile: <https://fivethirtyeight.com/features/blockchain-is-just-another-way-make-art-all-about-money/>, 2018

delle blockchain. Una notevole eccezione a questa regola è la creazione di Plantoid nel 2015 da parte di Primavera De Filippi, che è anche la creatrice del gruppo artistico Okhaos.

Plantoid è un NFT in grado di "vivere" e "riprodursi" grazie all'uso di micropagamenti in Bitcoin, come ha sottolineato Aaron Franck nell'articolo *“This Bitcoin-Eating Plant Robot Hires Artists to Make Its Babies”*³⁰:

“Plantoid is an attempt at using art to illustrate what I consider to be one of the most innovative and disruptive aspects of the blockchain—the ability to create autonomous entities which are completely independent and self-sufficient,”

Ogni Plantoid è dotato di un proprio portafoglio Bitcoin. Gli spettatori possono effettuare un pagamento per l'oggetto utilizzando la criptovaluta scansionando un codice QR. In risposta, il dispositivo mostrerà "colori e suoni". Quando ha accumulato abbastanza Bitcoin, la pianta commissiona, tramite contratti intelligenti, a un altro artista o gruppo di artisti la costruzione di un'altra pianta sulla blockchain di Ethereum, utilizzando i Bitcoin accumulati per finanziare la produzione. Questo lavoro è un tentativo di automatizzare il mecenatismo e di estetizzare la blockchain come mezzo in sé. Abbiamo grandi speranze che le modalità e i limiti della blockchain per la creazione di cryptoarte vengano spinti ancora più lontano in futuro.



Figura 11: <https://plantoid.org/#gallery>

³⁰ Aaron Franck. *This Bitcoin-Eating Plant Robot Hires Artists to Make Its Babies*. Accessibile: <https://singularityhub.com/2016/12/21/this-bitcoin-eating-plant-robot-hires-artists-to-make-its-babies/>, 2016

Inoltre, nonostante la concentrazione del mondo crypto sull'anonimato possa rendere possibile una critica radicale - ad esempio, alla dipendenza del sistema dell'arte da "artisti di marca" - può anche alimentare una riluttanza ad assumersi la responsabilità di una particolare azione o decisione. Un artista o un critico deve prendere una posizione, e poi essere responsabile di quella posizione, per poter partecipare a una discussione, che è esattamente ciò che l'arte in generale è. È quindi possibile che la criptoarte diventi solo una moda passeggera se non viene sottoposta a un esame storico e critico.

4.1 introduzione

Prima di analizzare il rapporto tra il mondo fisico dell'arte tradizionale e il mondo digitale della Crypto Art e degli NFT, di quest'ultimo è necessario comprendere le sue dinamiche e gli attori che hanno contribuito a crearlo. Ciò consentirà di comprendere meglio la relazione tra i due mondi "fisici". L'ascesa vertiginosa degli exchange di valute nel 2021 è diventata un fenomeno di assoluto interesse e di notevole impatto economico, che è stato collegato all'inarrestabile ascesa delle criptovalute, tra cui l'aumento del 570% della valutazione del Bitcoin da circa 8.000 dollari a oltre 50.000 dollari nell'arco di un solo anno nel 2021, per un mercato che, secondo CoinMarketCap, ha raggiunto un valore di oltre 2.000 miliardi di dollari.

Lo stretto legame con il mondo degli investitori in criptovalute è indubbio; questi investitori sono gli early adopters che hanno sperimentato, in tempi non sospetti, l'uso e l'associazione degli NFT con le opere d'arte - o presunte tali - e più in generale con gli oggetti da collezione, che sono oggi le più diverse tipologie di asset digitali.

Questi "nuovi" oggetti da collezione hanno accumulato, prima di altri, quelli che oggi sono diventati ingenti capitali in criptovalute come Bitcoin, Ethereum e molte altre valute virtuali, nate negli anni passati quando il loro valore era di pochi centesimi di dollaro e oggi, in alcuni casi, diverse migliaia.

Gli investitori che detengono enormi percentuali di criptovalute e sono in grado di manovrare facilmente il mercato vendendo improvvisamente grandi quantità di valuta virtuale e di NFT sono conosciuti in gergo tecnico come le "balene".

Sono stati loro i primi a iniziare a raccogliere NFT; erano appassionati di tecnologia Blockchain e specialisti del settore. Gli investitori e i trader hanno presto seguito le loro orme. Lo hanno fatto insieme, e in piccola parte anche per divertimento: hanno sostenuto imprese visionarie e

pionieristiche incoraggiando l'espansione della sperimentazione con la tecnologia dei token non fungibili.

Il mondo degli NFT, proprio come quello delle criptovalute e delle scelte dei loro collezionisti, è caratterizzato e influenzato da una grande volatilità. Questa volatilità si manifesta con variazioni di valore esagerate e imprevedibili, che contribuiscono all'alto grado di instabilità del mercato e, di conseguenza, al suo alto rischio.

Per questo motivo, le prime produzioni di opere NFT, così come la loro esposizione e vendita, sono coordinate all'interno della comunità crittografica. Questi eventi seguono dinamiche, valori e quantificazioni peculiari, spesso completamente diversi da quelli del mondo dell'arte convenzionale. La selezione degli artisti, delle opere, la loro quotazione e il loro trasferimento, così come il modello di valorizzazione e fruizione, continuano a rimanere, in qualche misura, più vicini alle tecniche, di marketing e finanziarie, che caratterizzano la comunità delle criptovalute.

È un mondo in cui la comunità gioca un ruolo significativo, in cui le relazioni dirette tra collezionisti e artisti avvengono su social network come Twitter, Telegram o Discord, e in cui l'acquisto di opere NFT è più simile a una transazione economico-finanziaria. Le piattaforme valutano e classificano gli artisti e i collezionisti in base a ciò che hanno venduto o acquistato, e gli artisti possono guadagnare reputazione in base alle loro vendite e ai loro acquisti.

Tuttavia, dopo che la casa d'aste Christie's ha venduto un NFT per 69 milioni di dollari, il sistema ha subito un rapido cambiamento. Il vecchio mondo dell'arte ha improvvisamente preso coscienza di questo nuovo mercato e di questa nuova ecologia e ha cercato non solo di farne parte, ma anche di prescrivere le proprie norme per evitare di esserne escluso.

Tenendo conto di ciò, la prima risposta dell'industria dell'arte è stata quella di tentare di applicare ideali, modelli e comportamenti in qualche caso paragonabili a quelli dell'arte fisica convenzionale e dell'arte digitale. In realtà, il tentativo ha subito rivelato diverse discrepanze e molte difficoltà nell'interferire con un "fenomeno" che, quotidianamente, si espande a ritmi incredibili e stabilisce nuovi record di vendita.

Il mondo dell'arte è in continua evoluzione e di conseguenza, nuovi artisti, designer, animatori, illustratori e specialisti dell'Intelligenza Artificiale e dell'Arte Generativa hanno trovato una visibilità mai vista prima. Questo vale anche per i collezionisti che si nascondono dietro pseudonimi fittizi e diventano star indiscusse con vendite e acquisti che possono raggiungere diversi milioni di dollari, spesso senza aver mai messo piede in un museo d'arte in tutta la loro vita.

Lontani da ogni dinamica del sistema canonico, molti artisti si sono ritrovati sulle pagine delle maggiori riviste mondiali e ricercati da gallerie e musei. Allo stesso tempo, i crypto-collezionisti hanno iniziato a dettare legge, condizionando il mercato a suon di acquisizioni, suscitando un interesse assoluto anche nel mondo dell'arte tradizionale. Uno scenario in cui le dinamiche si sono ribaltate: abbiamo assistito ad artisti del mondo crypto che ottengono quotazioni a sei zeri per opere NFT, mentre in passato le loro opere fisiche non suscitavano l'interesse di quasi nessuna galleria; e viceversa, artisti prestigiosi del mondo fisico con quotazioni milionarie, per i quali molti collezionisti hanno trovato conveniente acquistare i primi esperimenti digitali venduti a prezzi che possono essere considerati "abbordabili."

Un vero e proprio cortocircuito del sistema dell'arte, noto per la sua diffidenza e indisponibilità al cambiamento, che, con qualche difficoltà, ha dovuto far fronte a uno scenario nervoso con artisti che volevano vendere NFT, collezionisti tradizionali che aspiravano a buttarsi a capofitto nel digitale, con potenti case d'asta che iniziavano a gestire vendite in stretto rapporto con i cryptoartisti, mentre gallerie e operatori del settore rimanevano e rimangono ancora in attesa di capire meglio come approcciare questo nuovo mercato. Un vero e proprio cortocircuito del sistema dell'arte.

Nel frattempo, i grandi collezionisti di criptovalute stanno conquistando la ribalta indossando sempre più spesso i panni degli imprenditori digitali. Ciò ha portato alla nascita di nuove piattaforme e mercati di token non fungibili con caratteristiche distinte che si avvicinano ai valori detenuti dai grandi collezionisti di criptovalute e a quelli detenuti nel mondo reale.

Superati i primi mesi di grande clamore e fervore del mercato NFT, favorito anche dal declino delle criptovalute, oggi si va verso una stabilizzazione, la ricerca di nuovi equilibri e di una maggiore consapevolezza, insieme alla ricerca della qualità nella scelta delle opere. Sono tutte cose che si stanno facendo nel tentativo di trovare un equilibrio migliore.

Oggi i due mondi cominciano a comunicare tra loro. Lo dimostra la maggiore attenzione che viene posta sulla selezione degli artisti, sulla loro esposizione, sulla valutazione e sull'inserimento nel Sistema dell'Arte. Osserviamo collezionisti tradizionali che, per acquistare opere, spesso denominate in Ether, scambiando le loro valute, sono diventati di fatto dei cryptoinvestitori. È probabile che aspetti come la curatela, la critica e la sostenibilità ambientale diventino più rilevanti. Nel frattempo, l'esperienza dell'utente e l'alfabetizzazione digitale, economica e finanziaria saranno le basi di un futuro che vedrà l'arte e gli NFT sempre più vicini, nella speranza che possa essere più solida, meno volatile e sostenibile.

4.2 Crypto arte in senso pratico

Come punto di partenza per la nostra discussione sul sistema della criptoarte, esamineremo l'importante mercato online noto come SuperRare.com. Ogni volta che un artista carica una nuova opera sulla galleria di SuperRare, viene aggiunta una transazione alla blockchain di Ethereum. Questa transazione genera un token non fungibile (NFT), che è indissolubilmente legato all'opera d'arte, e poi invia il token al portafoglio digitale dell'artista. Per fornire una prova definitiva dell'originalità dell'opera, l'artista applica una crittografia alla transazione e poi la firma digitale. Il token è indissolubilmente legato all'opera d'arte ed è un bene unico che serve a rappresentare la proprietà e la genuinità dell'opera d'arte sottostante. Il file dell'opera d'arte viene distribuito dalla galleria sui nodi della rete peer-to-peer InterPlanetary File System (IPFS). La rete IPFS assegna all'immagine un nome utilizzando un codice che corrisponde esattamente al contenuto dell'immagine. Questo implica che la stessa immagine, anche se dispersa su numerosi nodi della rete, avrà sempre lo stesso nome e sarà concettualmente riconosciuta come un'unica risorsa. Questo è dovuto al modo in cui funzionano le reti distribuite.

La vita dell'opera digitale inizia ora sulla blockchain, dove può essere acquistata da un collezionista o da un appassionato e dove può essere successivamente trasferita, venduta o conservata dai collezionisti come qualsiasi altra reliquia unica. Le aste sono il metodo più comune per la vendita di opere d'arte. Durante un'asta, i potenziali acquirenti presentano offerte e l'attuale proprietario del bene ha la possibilità di accettare una delle offerte. Quando un bene viene venduto, il portafoglio dell'acquirente riceve il token corrispondente all'oggetto e il portafoglio del venditore riceve il prezzo corrispondente in Ether.

Dopo l'acquisto, l'opera d'arte può ancora essere scambiata sul mercato secondario e, in alcuni casi, l'artista originale riceve un compenso per ogni vendita successiva (ad esempio, il 10% del prezzo di vendita su SuperRare). Ogni transazione è crittografata e peer to peer grazie alla tecnologia blockchain e IPFS, ciò significa che né il denaro né il bene sono mai conservati dalla galleria o da terzi.

Per rendere il concetto più chiaro prenderò in esempio un'opera iconica nel mondo degli NFT, ossia "Everydays: The First 5000 Days" dell'artista Beeple battuta all'asta l'11 marzo 2021 per \$69,346,250³¹.

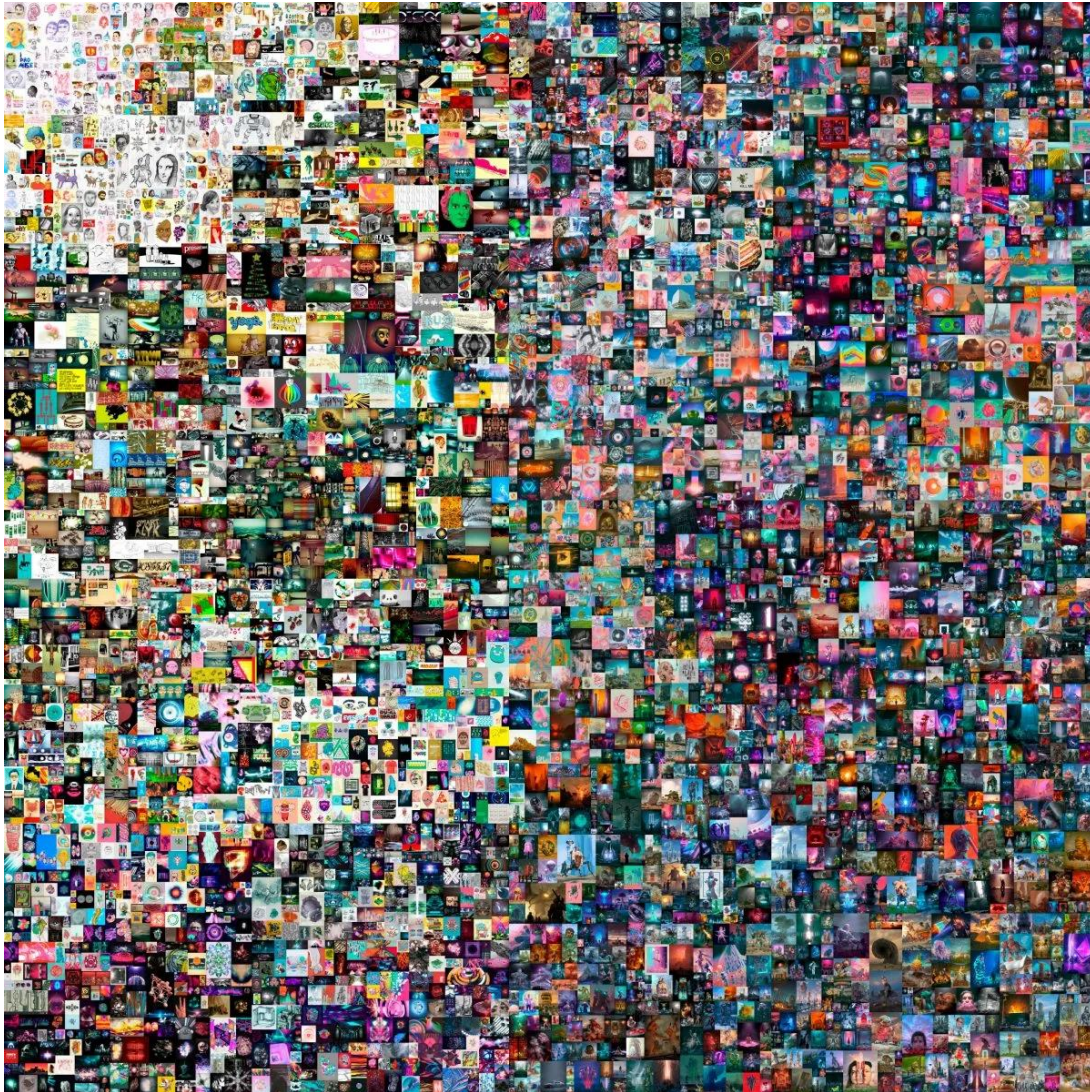


Figura 12: Beeple, *Everydays: The First 5000 Days*

Alla famosa casa d'aste Christie's è spettato il compito di bandire l'opera che ad oggi, agosto 2022, è ancora l'NFT di maggior valore mai venduto; è stata presentata in questo modo:

"Beeple (b. 1981)

EVERYDAYS: THE FIRST 5000 DAYS

token ID: 40913

wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807

smart contract address: 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756

non-fungible token (jpg)

21,069 x 21,069 pixels (319,168,313 bytes)

³¹Pagina web sul sito Christie's riguardo l'opera di Beeple. 2021. Accessibile: <https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924>

*Minted on 16 February 2021.
This work is unique.”*

Da questa descrizione possiamo trarre tutte le informazioni necessarie sull’NFT, vale a dire: L’NFT del file in formato jpeg dell’opera *Everydays: The First 5000 Days*, dal peso di 319 Mbytes, ha come numero identificativo 40913, ed è stato creato dall’indirizzo del portafoglio

0xc6b0562605D35eE710138402B878ffe6F2E23807,

Quando Beeple ha sviluppato il token per la prima volta, lo ha fatto con l’assistenza di uno smart contract che specifica le linee guida per l’utilizzo del token.

Il contratto riporta il seguente indirizzo:

0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756.

Grazie a piattaforme come Etherscan.io riusciremo, inserendo l’indirizzo pubblico del portafoglio, che nel nostro caso è dell’artista, a vedere tutte le transazioni poste in essere dal portafoglio.

The screenshot displays the Etherscan.io interface for a specific wallet. The top section, titled 'Overview', shows the wallet's balance as 117.45368202681235475 Ether, with an Ether value of \$175,022.43 (at \$1,490.14/ETH) and a token balance of \$942,757.60. The 'More Info' section indicates that the name tag is not available. Below this, the 'Transactions' section is active, showing a list of the latest 25 transactions out of a total of 391. The table includes columns for Txn Hash, Method, Block, Age, From, To, Value, and Txn Fee. The transactions listed are primarily 'Safe Transfer From' operations, with values of 0 Ether and fees ranging from 0.00064404 to 0.00073819.

Txn Hash	Method	Block	Age	From	To	Value	Txn Fee
0x7bc798a2261b482de8...	Approve	15416225	23 hrs 24 mins ago	Beeple	OUT Wrapped Ether	0 Ether	0.00131933
0x122b0548e29abc3a6a...	Transfer	15405861	2 days 15 hrs ago	0x395e640104a9bd9568...	IN Beeple	0 Ether	0.000525
0xd627be32370b2e793d...	Transfer	15405861	2 days 15 hrs ago	0x395e640104a9bd9568...	IN Beeple	0 Ether	0.000525
0x115e30e2b18503bae...	Transfer	15405859	2 days 15 hrs ago	0x395e640104a9bd9568...	IN Beeple	0 Ether	0.000525
0xfe6d55d91643f1b3469...	Safe Transfer Fr...	15367012	8 days 18 hrs ago	Beeple	OUT 0x44541d1ff5e8a1ed225...	0 Ether	0.00073819
0x29aa75e24f2c39f8085...	Safe Transfer Fr...	15367008	8 days 18 hrs ago	Beeple	OUT 0x44541d1ff5e8a1ed225...	0 Ether	0.00073585
0xc1430fe7f9698b3b8ec...	Safe Transfer Fr...	15367002	8 days 19 hrs ago	Beeple	OUT 0x44541d1ff5e8a1ed225...	0 Ether	0.00064404
0x00da21a03d9dd541d9...	Safe Transfer Fr...	15366990	8 days 19 hrs ago	Beeple	OUT 0x44541d1ff5e8a1ed225...	0 Ether	0.00066403

Figura 13: cronologia, sul sito etherscan.io, di acquisti/vendite del portafoglio che ha venduto l’opera

Possiamo dire con sicurezza che il portafoglio appartiene a Beeple perché sono visibili tutte le opere da lui create, attraverso gli hash identificativi.

Ad esempio l'opera battuta per 69 milioni di dollari è identificata dall'hash:

0x84760768c527794ede901f97973385bfc1bf2e297f7ed16f523f75412ae772b3,

e la ritroviamo nello storico dell'indirizzo.

Ci terrei a riassumere i passaggi attraversati dall'artista

- Beeple ha creato il file.
- Ha creato un hash che non poteva essere decifrato dagli hacker e che era completamente unico.
- Ha creato un file di metadati che includeva l'hash dell'opera d'arte e lo ha inserito nel file.
- Ha creato un hash al file di metadati che aveva preparato.
- Entrambi i file, le informazioni e le opere d'arte, sono stati pubblicati sul servizio di condivisione di file decentralizzato IPFS sulla darknet.
- Sulla blockchain di Ethereum ha sviluppato o "coniato" un token controllato da uno smart contract. Christie's ha poi organizzato un'asta per questo token.
- Il pagamento, effettuato sotto forma di criptovaluta Ether e pari a 69 milioni di dollari, ha permesso di concludere l'asta con successo. C'è da dire che nessuno è stato in grado di identificare questo pagamento sulla blockchain di Ethereum; è quindi probabile che il denaro sia stato spostato attraverso qualche metodo privato.
- Il token è stato trasferito da Beeple al vincitore, che lo ha poi trasferito nuovamente nel suo portafoglio privato.

Bibliografia e sitografia

1. Gian Luca Comandini. *“Da zero alla luna, quando come perché la Blockchain sta cambiando il mondo”*. 2020
2. Haber S, Stornetta W.S. *“How to time-stamp a digital document”*. *Journal of Cryptology* , Issue 3, 99–111, 1991.
3. Bayer, Dave & Haber, Stuart & Stornetta, W. *“Improving the Efficiency and Reliability of Digital Time-Stamping”*, 1999.
4. Lamport, Leslie & Shostak, Robert & Pease, Marshall. *“The Byzantine Generals Problem”*, 2002.
5. Vitalik Buterin. 2015. Accesibile: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
6. Sito ufficiale Ethereum, ultimo aggiornamento settembre 2015. Accesibile: <https://ethereum.org/it/what-is-ethereum/>
7. Szabo N. *“Smart Contracts: Building Blocks for Digital Markets”*, 1996.
8. *Ethereum Classic Website*, (2016). Accesibile: <https://ethereumclassic.github.io/>
9. Jentsch, C. (2016a). *The History of the DAO and Lessons Learned*. Medium. Accesibile: <https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5>, 22 October 2016.
10. Shermin Voshmgir, *“Tokenized Networks: What is a DAO?”*, Blockchainhub. July 2021
11. Garrett Hardin. *“The tragedy of the commons”*, 1968

12. *Jeremy Williams. "Elinor Ostrom's 8 rules for managing the commons". <https://earthbound.report/2018/01/15/elinor-ostroms-8-rules-for-managing-the-commons/>. 2018*
13. *Lisa Gibbons. "DAO shall not be alone! Ecosystem DAOs on the rise". 2022.*
14. *Binance academy. Accessible: <https://academy.binance.com/it/articles/the-evolution-of-the-internet-web-3-0-explained>*
15. *Wang, Q., Li, R., Wang, Q. & Chen, S., 2021. "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. arXiv e-prints".*
16. *Cryptokitties. Project Accessible: <https://www.cryptokitties.co/> (2021)*
17. *Cryptocats. Project Accessible: <https://cryptocats.thetwentysix.io/> (2021)*
18. *Cryptopunks. Accessible: <https://www.larvalabs.com/cryptopunks> (2021)*
19. *Meebits. Project Accessible: <https://meebits.larvalabs.com/> (2021)*
20. *Axie infinity. Project Accessible: <https://axieinfinity.com/> (2021)*
21. *Gods unchanged. Project Accessible: <https://godsunchained.com/> (2021)*
22. *Tradestars. Project Accessible: <https://tradestars.app/> (2021)*
23. *Decentraland (mana). Project accessible: <https://decentraland.org/> (2020)*
24. *Cryptovoxels. Project Accessible: <https://www.cryptovoxels.com/> (2021)*
25. *Somnium space. Project Accessible: <https://somniumspace.com/> (2021)*
26. *Megacryptopolis. Project Accessible: <https://mcp3d.com/> (2021)*

27. *Sandbox*. Project accessible: <https://www.sandbox.game/en/> (2020)
28. *Mad dog jones*. Accessible: <https://www.phillips.com/detail/mad-dog-jones/NY090121/1>
29. O. Roeder. “The blockchain is just another way to make art all about money”. Accessible: <https://fivethirtyeight.com/features/blockchain-is-just-another-way-make-art-all-about-money/>, 2018.
30. Aaron Franck. “This Bitcoin-Eating Plant Robot Hires Artists to Make Its Babies”. Accessible: <https://singularityhub.com/2016/12/21/this-bitcoin-eating-plant-robot-hires-artists-to-make-its-babies/>, 2016.
31. Pagina web sul sito Christies riguardo l’opera di beeples. 2021. Accessible: <https://onlineonly.christies.com/s/beeples-first-5000-days/beeples-b-1981-1/112924>

APPENDICE

Il declino di TERRA LUNA

La comunità Terra ha introdotto Terra Luna, un token di criptovaluta, nel luglio 2019. Il token nativo della blockchain Terra, creata dalla società coreana Terraform Labs, è il token Terra Luna. Terra Luna Classic \$LUNC è il nuovo nome del token precedentemente noto come Terra Luna \$LUNA. L'asset è ormai noto per il crollo della criptovaluta avvenuto nel maggio 2022: il token, che un tempo veniva venduto a 80 dollari per \$LUNA su CoinMarketCap al 20 luglio 2022, è ora valutato a 0,0001074 dollari.

La piattaforma Terra è stata creata con l'obiettivo di fornire agli utenti la sicurezza del denaro fiat, utilizzando al contempo la tecnologia blockchain per facilitare i pagamenti più rapidi e meno costosi rispetto ai metodi di pagamento tradizionali. L'ampia accettazione del token Terra Luna può essere attribuita al fatto che è supportato da Terra Classic USD \$UST, il token algoritmico stablecoin di Terra Luna. Con oltre 20 miliardi di dollari investiti nella rete attraverso le sue applicazioni a dicembre 2021, Terra ha superato la smart chain BNB diventando il secondo protocollo DeFi per importanza. Prima del crollo di Terra Luna di maggio, che ha scosso il mondo delle criptovalute e ha lasciato molte persone con perdite finanziarie significative, \$LUNA era venduta a oltre 100 dollari.

A1 Il funzionamento di Terra Luna

Un gruppo di stablecoin algoritmiche destinate a mantenere i loro peg con il token LUNA sono alimentate dal protocollo Terra, che si basa sulla piattaforma Cosmos. Terra Classic USD, una di queste monete stable algoritmiche, mantiene il suo ancoraggio al dollaro USA attraverso una rete di investitori che acquistano il token Terra Luna Classic. Per il funzionamento è necessario generare alcuni LUNA prima di poter acquistare UST. I token LUNA vengono bruciati dopo aver pagato il tasso di cambio in \$LUNA. Quando la quantità di \$LUNA disponibili diminuisce, il prezzo aumenta. D'altra parte, si convertono i gettoni \$UST se si desidera coniugare LUNA. Bruciare le monete stabili aumenta il prezzo di \$UST.

Gli arbitraggisti della rete Terra traggono profitto dalle variazioni di prezzo del token Terra Luna Classic e del suo gemello, il Terra Classic USD. Terra Luna ha la funzione cruciale di essere il metodo di pagamento utilizzato per le commissioni di transazione nel sistema di gas della rete Terra, oltre a contribuire al mantenimento dell'ancoraggio di \$UST al dollaro USA. Di conseguenza, \$LUNA è ora un token di utilità dell'ecosistema Terra. Il token Terra Luna Classic può anche essere puntato per guadagnare denaro. Oltre al profitto che \$LUNA offre ai suoi possessori, dà loro anche la possibilità di redigere e votare su varie proposte che modificano il protocollo Terra. La domanda di stablecoin sostenuta dal token Terra Luna Classic è anche regolata dal token come meccanismo di regolamentazione.

A2 Il Crash

I siti di social media come Reddit e Twitter sono stati infiammati da commenti di investitori e analisti di criptovalute nel maggio 2022. Il prezzo del token Terra Luna Classic, noto anche come Terra Luna, è sceso da oltre 100 dollari per \$LUNA a meno di 1 dollaro. Fino a qualche tempo prima, tra l'11 e il 12 maggio 2022, il token Terra Luna aveva un considerevole market cap ed era considerato dai proprietari un saggio investimento. Inaspettatamente, \$LUNA è sceso da 120 a 0,02 dollari in sole 48 ore. Questa perdita ha stabilito un record significativo per il settore delle criptovalute. In seguito alla correzione del 99,9%, \$LUNA è scesa a 0,00000112 dollari contro BUSD, l'ultima coppia di scambio ad essere cancellata dalle borse di criptovalute.

Quando \$LUNA è crollata, il valore di \$UST, il suo token gemello, è sceso da un dollaro a pochi centesimi a causa del depegging. Binance Futures ha annunciato il delisting di \$LUNA e la liquidazione automatica dei contratti perpetui il 12 maggio 2022, alle 8:00 UTC. Inoltre, Binance Futures ha aggiornato i livelli di margine dei contratti LUNA con margine USDT e ha ridotto la leva massima a 8x. Anche il ritiro di \$LUNA e \$UST è stato temporaneamente sospeso sulla nota piattaforma di scambio. Do Kwon, l'amministratore delegato di Terraform Labs, ha presentato nei giorni successivi una proposta di soluzione per il ritiro di \$UST e la svalutazione di \$LUNA. L'offerta di UST sarebbe stata ridotta e il peg della stablecoin sarebbe stato ripristinato con un'operazione da 1 miliardo di dollari di \$UST. Terra Luna Classic sarebbe crollata di nuovo, ma questa volta con un impatto minore, poiché più persone hanno acquistato \$LUNA, in parte perché pensavano che il token potesse riprendersi e in parte per ridurre le loro perdite finanziarie. Do Kwon ha annunciato una nuova strategia dopo che il parziale successo del burn di \$UST nel riportare il token a \$1 si è rivelato insufficiente. La vecchia Terra Luna si sarebbe chiamata Terra Luna Classic (\$LUNC), mentre la

nuova Terra Luna si sarebbe chiamata Terra Luna 2.0 (\$LUNA). Inoltre, per premiare i detentori di lunga data, si è tenuto un airdrop di \$LUNA. Il 28 maggio 2022 Terra Luna 2.0 è stata rilasciata e nei giorni successivi il suo prezzo è sceso. Il prezzo di \$LUNA ha raggiunto un picco di 19,53 dollari prima di scendere a circa 4,39 dollari poche ore dopo. Il prezzo è risalito a 5,90 dollari a maggio, ma la reputazione di Terra Luna ne ha risentito. Da un picco di 4,50 dollari nel giugno 2022, Terra Luna ha subito un brusco calo a 3,30 dollari. Secondo CoinMarketCap, Terra Luna era valutata a 1,93 dollari per token al 22 luglio 2022. Per un token che in precedenza era scambiato a oltre 20 dollari, si tratta di una perdita sostanziale, ed è ovvio il motivo per cui Terra 2.0 è crollata. Gli investitori hanno venduto i loro airdrop, anche a prezzi bassi, dopo aver perso fiducia nella moneta. Ci sono state diverse voci legate al crash, che hanno reso gli investitori meno inclini a investire in \$LUNA e \$LUNC.

Ci sono molte teorie sul perché Terra Luna sia crollata, ma una importante è che ci sia stato un enorme sellout di Terra Classic \$UST. Secondo questa ipotesi, all'inizio di maggio si sono verificati alcuni consistenti ritiri di \$UST dall'ecosistema Terra. Questi ritiri hanno aumentato l'offerta di \$UST e fatto diminuire il prezzo. Gli investitori sono stati presi dal panico e hanno iniziato a vendere, mentre il prezzo di \$UST è sceso. Con la vendita di \$UST, è stato creato \$LUNA, che ha provocato un forte calo del prezzo del token. Per mantenere stabile il prezzo di \$UST, il Terraform Luna è stato generato continuamente; tuttavia, entrambi i token alla fine sono crollati.

Alcuni ritengono che i modelli Terra Luna e Terra Classic USD non possano durare. La stablecoin algoritmica Terra Classic USD \$UST si basa su \$LUNA per mantenere l'ancoraggio al dollaro USA. L'idea è che si possa scambiare 1 dollaro di \$LUNA con 1 dollaro di UST. Tuttavia, i crolli sono inevitabili quando i driver della volatilità del mercato sono presenti per le monete stabili algoritmiche. Questo perché le monete stabili come l'UST si affidano alle dinamiche della domanda e dell'offerta piuttosto che essere sostenute da criptovalute o valute fiat. Poiché il prezzo di \$LUNA era basato sul valore di \$UST, ciò ha avuto un impatto sul token.

A3 L'effetto del crollo

Il disastro di Terra Luna ha scosso il mercato delle criptovalute; molti investitori hanno perso i risparmi di una vita e la cronaca ha riportato addirittura diversi suicidi correlati alla faccenda. Nel giro di pochi giorni, gli investitori hanno visto il loro denaro passare da centinaia di dollari a pochi centesimi. Originariamente valutata oltre 40 miliardi di dollari, Terra Luna ha perso la fiducia e il valore degli investitori. La Securities and Exchange Commission statunitense ha avviato un'indagine

sulla situazione dopo che più di 2000 investitori hanno presentato una denuncia collettiva contro Do Kwon. In Corea del Sud, la sezione speciale per i crimini finanziari dell'ufficio del procuratore di Seoul è responsabile dell'inchiesta sul crollo di Terra Luna. Mentre queste indagini sono in corso, gli ex lavoratori dei Terraform Labs in Corea del Sud non possono lasciare il Paese.

La crisi di Terra Luna ha dimostrato senza ombra di dubbio che le criptovalute, in qualsiasi forma esse si presentino, saranno sempre volatili. Gli investitori che avevano fiducia nella capacità di \$UST di rimanere legata al dollaro USA hanno iniziato a perdere le speranze in \$UST e a mostrare maggiore scetticismo nei confronti di Tether \$USDT. La fiducia nelle stablecoin e nei token bitcoin è diminuita in generale, a causa della percezione che non tutte le stablecoin sono realmente sostenute da riserve. I critici del bitcoin si sono scatenati definendolo uno schema Ponzi in cui gli investitori sono stati ingannati due volte con il token. L'intero mercato delle criptovalute è crollato, perdendo investitori e oltre 400 miliardi di dollari di capitalizzazione di mercato.