POLITECNICO DI TORINO

Corso di Laurea Magistrale

Computer and Communication Networks Engineering

Il Metaverso

Un' applicazione innovativa della tecnologia Blockchain

Relatori

Prof. Danilo Bazzanella

……..

Candidato

Antonio Intagliata

……..

Indice

Capitolo 1 - La tecnologia Blockchain

In questo capitolo sarà presentata una panoramica sulle componenti principali che caratterizzano la tecnologia Blockchain. Vedremo come la Distributed Ledger Technology, o DLT, ha permesso di estendere i concetti di architettura distribuita delle basi di dati - su cui la Blockchain basa i propri sviluppi - e si presenteranno alcuni cenni di crittografia maggiormente utilizzati in ambito Blockchain per garantire l'integrità e la sicurezza delle informazioni distribuite.

Sarà possibile capire come questa nuova tecnologia distribuita rafforza il concetto di fiducia (*trust*) che spesso affidiamo (inconsciamente o per necessità) a servizi che utilizzano architetture centralizzate. Nel momento in cui deleghiamo la responsabilità del salvataggio o della gestione in generale delle nostre informazioni ad una terza parte, ci chiediamo mai se questo servizio è realmente in grado di fornire delle garanzie riguardo la giusta protezione contro furti, manomissioni o distruzioni dei nostri dati? Possiamo dire che il servizio è quindi affidabile per le nostre applicazioni solo perchè risolve una parte delle nostre necessità?

Per fare un esempio reale non c'è bisogno di andare molto indietro nel tempo, ma basterebbe tornare alla notte del giorno 10 Marzo 2021 quando nei Data Center del Provider OVH situati a Strasburgo, in Francia, divampa un incendio che coinvolge il settore identificato con *Sbg2*, dove migliaia di clienti - la maggior parte Europei - vedono i propri servizi web interrompersi improvvisamente[1]. Molti utenti sulle pagine social del Provider non comprendono molto bene la gravità dell'accaduto, fiduciosi di un immediato intervento di ripristino dei backup sfruttando la ridondanza dei sistemi come punto di forza del Provider, peccato però che i sistemi di backup si trovavano all'interno dello stesso settore dove è divampato l'incendio; non solo, per mettere in sicurezza gli altri settori dall'evento straordinario che è accaduto, è stata rimossa l'alimentazione anche al settore identificato con *Sbg4*, coinvolgendo nel disservizio un'altra grande parte della clientela del Provider non direttamente correlata al disastro. Aziende che non avevano previsto delle procedure di recovery plan (magari accettando una parziale perdita di informazioni) si sono trovate ad affrontare una situazione che avrebbe potuto danneggiare, o ha danneggiato seriamente, le proprie attività basate sul web, dal semplice servizio email alle piattaforme e-commerce e… ai servizi di backup.

[1] https://www.wired.it/internet/web/2021/03/10/incendio-data-center-ovh-strasburgo/

Per questi motivi la tecnologia Blockchain può essere un ottimo punto di partenza se si vuole ripensare l'architettura delle proprie applicazioni senza dipendere da servizi per i quali non possiamo valutare realmente la loro affidabilità.

1.1. La Distributed Ledger Technology (DLT)

Molte applicazioni, che si sono evolute nel tempo fino alla loro completa digitalizzazione, hanno costantemente avuto la necessità di salvare e rendere permanenti le informazioni della propria attività su registri dedicati (una base di dati che poteva essere cartacea - si pensi al Libro Mastro per le registrazioni contabili - o digitale). Questo registro, indipendentemente dal suo livello di tecnologia digitale che lo supporta, può essere più o meno sensibile ad alcuni fattori che ne possono compromettere la sua integrità, in particolare:

- **furto (leak):** le informazioni entrano in possesso di entità non autorizzate alla loro conoscenza/comprensione;

- **manomissione (volontaria / involontaria):** la gravità di questo fattore può variare dal semplice errore umano in fase di registrazione, fino alla volontaria attività di alterazione delle informazioni al suo interno per scopi illeciti;

- **distruzione e impossibilità di recupero delle informazioni:** la distruzione delle informazioni per cause involontarie o eventi naturali che ne compromettono l'integrità del registro stesso devono essere sempre tenute in considerazione durante il ciclo di vita di un'applicazione.

Tralasciando momentaneamente il primo fattore (dato che prenderemo in considerazione registri pubblicamente consultabili), risulta evidente che senza opportune metodologie di recovery plan o monitoraggio delle azioni - che si tramutano spesso in altissimi costi di prevenzione per le Aziende - l'integrità delle informazioni o la vita stessa dei registri è messa costantemente a rischio. Nasce dunque la necessità di realizzare un registro sul quale le informazioni permanenti in esso contenute, identificate da ora in poi con il termine ***transazioni***, possano essere:

- **distribuite**: i nodi dell'applicazione possiedono una copia della base di dati principale e qualsiasi nuova transazione viene registrata tramite un consenso collettivo;

- **trasparenti**: i dati del registro vengono resi fruibili ai nodi dell'applicazione che può interrogarli in qualsiasi momento;

- **immutabili**: non viene consentita la modifica del dato successivamente alla transazione o, se previsto dalle applicazioni basate ad esempio su Blockchain, tale modifica viene sempre registrata come una nuova transazione

I vantaggi sopra elencati diventano dei punti di forza per tutte quelle applicazioni basate su registri distribuiti, in quanto un attacco che tenti di violare l'integrità dei dati, seppur possibile, richiede costi e tempi elevati[2].

La **Distributed Ledger Technology (DLT)** è un tipo di tecnologia che sposta la centralità di un registro - e le sue responsabilità - a livello di tutti i nodi dell'applicazione (peers), che sono coinvolti a mantenere integri e immutabili i dati del registro stesso. Infatti ogni peer possiede una copia del database e ha la possibilità di operare su di esso in maniera indipendente dalle attività degli altri utenti, partecipando collettivamente - attraverso protocolli di consenso che vedremo più avanti - al mantenimento di un' unica immagine aggiornata contenente le nuove transazioni provenienti dai diversi utenti.

La **Blockchain** è un tipo specifico di DLT che rafforza l'integrità dei propri dati riducendo le operazioni che in generale una DLT può effettuare. Infatti le uniche operazioni consentite ai peers in una Blockchain sono la **creazione** di nuovi blocchi e la loro **lettura**. Una modifica quindi nella catena del registro è sempre tradotta in un'operazione di creazione di un nuovo blocco, nel paragrafo successivo vedremo la struttura dei blocchi di una Blockchain.

[2] https://www.toolbox.com/it-security/data-governance/articles/distributed-ledger-technology-cyber-threat/

1.2. Struttura dei blocchi

All'interno di una Blockchain il blocco (*block*) può essere considerato come l'unità indivisibile dell'architettura dove vengono salvate le informazioni di una transazione, ogni blocco è identificato univocamente attraverso un block ID (*BID*), che solitamente viene generato attraverso metodi crittografici. L'insieme dei blocchi che compongono la Blockchain, come il termine stesso suggerisce, sono organizzati attraverso una catena nel quale ogni blocco contiene il *BID* del blocco precedente.
I dati della transazione vengono conservati all'interno del blocco e possono essere consultati in chiaro dagli attori che partecipano all'applicazione.

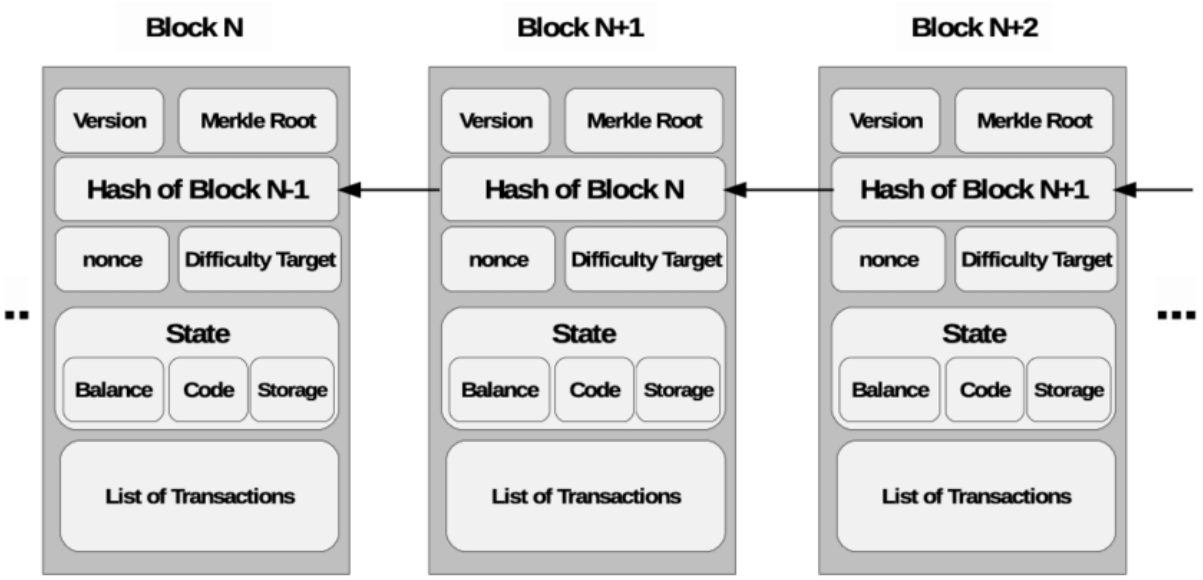


Immagine di esempio che rappresenta la struttura dei blocchi di una Blockchain[3]

Altri importanti campi che possiamo trovare in una generica Blockchain all'interno di un blocco sono:

- **Index Number:** identifica il numero del blocco all'interno della catena, è un identificativo sequenziale incrementale che il creatore di un nuovo blocco deve rispettare in fase di creazione.

[3] *IoT Security: Review, Blockchain Solutions, and Open Challenges, November 2017, Future Generation Computer Systems 82*

- **Version Number:** questo numero, nelle architetture Blockchain più complesse, identifica la versione stessa della Blockchain che potrebbe variare le sue policy nel tempo e quindi sviluppa la propria catena in un nuovo ramo (fork), è utile in fase di consultazione dei blocchi precedenti per capire con quale versione della catena è stata registrata la transazione.

- **Timestamp:** rappresenta il momento esatto in cui il blocco è stato creato ed è responsabilità del peer compilarlo. Questo campo in realtà acquisisce vitale importanza in tutte quelle Blockchain che sono appunto definite *timestamp-based*, dove la definizione del momento specifico in cui avviene la transazione è fondamentale per la valutazione della qualità della chain, si pensi ad esempio alle Supply chains, ai servizi di logistica o alle catene di servizi per garantire l'effettiva proprietà di un bene dopo il suo acquisto.

- **Nonce**: abbreviazione di "number that can only be used once". Il processo di generazione del nonce può avvenire in modo casuale fino a quando non si trova un valore nonce diverso da quelli utilizzati nei blocchi precedenti. Alternativamente, può essere generato attraverso metodi crittografici che, in relazione alla lunghezza della stringa iniziale, rendono estremamente improbabile trovare una stringa identica a quelle dei blocchi precedenti. All'interno di una blockchain viene solitamente utilizzato insieme all'ID del blocco per verificare l'effettiva partecipazione del peer alla catena (Proof of Work, come vedremo più avanti) oppure per verificare la validità dei blocchi.

1.3. Cenni di crittografia applicata alle Blockchain

1.3.1. Crittografia Simmetrica / Asimmetrica

Una Blockchain, data la sua natura distribuita, necessita di fondamentali metodi crittografici per poter garantire l'integrità dei propri dati e concedere le autorizzazioni necessarie a tutti i/parte dei peers coinvolti in una transazione.

La crittografia, in generale, può essere suddivisa in due macro-categorie: sulla base delle loro proprietà matematiche e della correlazione tra le chiavi che le entità devono utilizzare per cifrare/decifrare i messaggi, queste sono la crittografia **simmetrica e asimmetrica.** La principale differenza tra i due tipi di crittografia deriva dal fatto che nella simmetrica la cifratura di un messaggio tra due o più entità, a parità di algoritmo utilizzato, avviene attraverso una *chiave K* che deve essere necessariamente conosciuta da chi vuole scambiare i messaggi.

Se volessimo fare un esempio immaginiamo due entità, *A(lice)* e *B(ob)* che vogliono scambiare un testo privato di cui solo loro vogliono conoscerne il contenuto. Alice possiede il testo in chiaro, applica l'algoritmo di cifratura (encryption) con la chiave K e ottiene un testo cifrato, apparentemente privo di senso per qualunque attaccante che riesca ad intercettarlo durante la comunicazione verso Bob. A questo punto Bob, una volta ricevuto il messaggio, applica l'algoritmo di de-cifratura (decryption) passando in input il testo cifrato ricevuto da Alice e la stessa chiave K utilizzata per cifrarlo. Qualsiasi altra chiave diversa da K non ha alcuna possibilità di recuperare il testo originale contenuto nel messaggio.

Schema del flusso di un messaggio cifrato con crittografia asimmetrica.

Ciò che sta alla base della cifratura simmetrica ed evidenza gli svantaggi nel suo utilizzo consiste nel fatto che, per avere la garanzia che il messaggio sia stato cifrato dal mittente, la chiave K deve essere condivisa esclusivamente tra due soggetti, qualsiasi altra comunicazione che Alice dovrà cifrare verso altri utenti diversi da Bob sarà effettuata con un'altra chiave diversa da K.

Ciò significa che in una rete composta da ***n*** utenti - in cui ciascuno di essi dovrà possedere ***n*** chiavi - il **numero totale di chiavi** all'interno della rete coincide con il totale delle coppie che si possono comporre con ***n*** elementi, secondo la formula:

$$\binom{n}{2} = \frac{n!}{2 \times (n-2)!} = \frac{n \times (n-1)}{2} \simeq \frac{n^2}{2}$$

La **crittografia asimmetrica**, permette di superare questa complessa gestione, utilizzando una coppia di chiavi tra loro correlate matematicamente, dette rispettivamente:

- **chiave pubblica (P):** viene messa a disposizione pubblicamente e può essere utilizzata dalle altre entità per cifrare i messaggi diretti verso il possessore di questa chiave, per verificare che la ricezione del messaggio sia arrivata senza manomissioni (***integrità***) dal possessore e/o per verificare che il possessore della chiave abbia realmente mandato il messaggio (***non ripudio***).

- **chiave privata (K):** questa chiave deve essere trattata come una password e deve sempre essere messa in sicurezza dal possessore, viene utilizzata per decifrare i messaggi ricevuti dall'altra entità che ha cifrato il messaggio con la chiave pubblica P.

Schema del flusso di un messaggio cifrato con crittografia asimmetrica.

La tecnologia Blockchain sfrutta la crittografia asimmetrica con chiave pubblica/privata, agendo ad esempio durante la cifratura delle transazioni tra i peers e la loro verifica in qualsiasi momento successivo all'aggiunta del blocco nel registro.

1.3.2. Cenni sugli Algoritmi irreversibili e funzioni di Hash

Un'altra importante categoria di algoritmi di cifratura delle informazioni è rappresentata dagli algoritmi ***irreversibili*****,** cioè quegli algoritmi per i quali viene applicata una manipolazione del messaggio da cifrare attraverso tecniche che ne garantiscono l'impossibilità (in termini temporali) di essere decifrati attraverso processi a ritroso.
Questi algoritmi di solito sono maggiormente rappresentati in termini operativi dalle ***funzioni di Hash****,* delle funzioni che godono di particolari proprietà:

- Indipendentemente dalla lunghezza dell'input, restituiscono un output sempre della stessa lunghezza;
- A variazioni minime della stringa in input, corrispondono variazioni drastiche della stringa di output;
- La possibilità di collisione - due stringhe di input della stessa lunghezza ma di contenuto diverso che generano lo stesso codice hash - tende a zero all'aumentare della lunghezza del risultato in output.

Per queste proprietà le funzioni di Hash vengono utilizzate in particolare per:

- Creazione di dizionari e di indici, il cui codice Hash di un elemento rappresenta la chiave che identifica l'elemento stesso
- Salvataggio in database di dati cifrati (si pensi al salvataggio delle password degli utenti di un sistema, che per policy GDPR non possono più essere conservate in chiaro)
- Generazione di una checksum (rilasciata solitamente dal distributore della risorsa) per verificare l'integrità del file o del testo che è stato trasferito ed essere certi che si sta trattando dell'entità originale.

Per essere sicuri che il messaggio cifrato corrisponda al messaggio in chiaro, l'unico modo possibile con questo tipo di funzioni è conoscere il messaggio iniziale, ri-applicare l'algoritmo di

cifratura utilizzato e confrontare il risultato con il messaggio cifrato che il mittente ci ha fornito insieme all'originale. Da ciò si deduce che gli algoritmi irreversibili sono un ottimo metodo per garantire l'originalità di un messaggio ed escludere la presenza di manomissioni durante il percorso verso la destinazione.

Un'altra applicazione delle funzioni di hash la ritroviamo anche in tutti quei flussi dove deve essere garantita non solo l'integrità del messaggio, ma anche la non ripudiabilità (ovvero il mittente non può negare di non aver inviato il messaggio), e questo accade ad esempio nelle Firme Digitali in cui viene utilizzata la combinazione delle funzioni di hash con altri algoritmi di cifratura asimmetrica visti in precedenza. Con il termine ***Firma Digitale*** si intende un procedimento crittografico con l'obiettivo di garantire l'autenticità, l'integrità e la non ripudiabilità dei messaggi o dei documenti digitali gestiti dall'utente firmatario nella fase di comunicazione con gli altri utenti. Esso può essere composto da diverse fasi e di seguito si presenta un esempio di come potrebbe avvenire la firma di un messaggio che Alice vuole inviare a Bob:

- Alice converte il suo messaggio in chiaro **T** attraverso una Funzione di Hash **H(T)** ed effettua la cifratura dell'output con la sua chiave privata, il tutto può riassumersi con la seguente formula:

$$X_T = C(H(T) , PRIVKEY_{Alice})$$

- Il messaggio **T** viene dunque inviato a Bob insieme al suo valore $\mathbf{X_T}$ ottenuto in precedenza.

- Bob a sua volta genera lato suo il valore di Hash **H(T)** conoscendo il testo in chiaro e recupera il valore **H(T)** di Alice decifrando il messaggio $\mathbf{X_T}$ con la chiave pubblica di Alice:

$$H(T) = D(X_T , PUBKEY_{Alice})$$

- Bob confronta il valore **H(T)** da lui calcolato con il valore **H(T)** calcolato da Alice, se i due valori corrispondono allora Bob può essere certo che il messaggio non solo è stato

inviato da Alice, ma non ha subito manipolazioni durante il percorso verso la destinazione.

Sebbene le funzioni di Hash e dei loro principali algoritmi maggiormente utilizzati nelle applicazioni (MD5, SHA-1, SHA-256, ecc..) garantiscano una maggior sicurezza nella conservazione delle informazioni cifrate senza conservare il testo in chiaro, trattandosi di metodi dipendenti esclusivamente da risorse computazionali, esse diventano obsolete con il passare del tempo e con l'aumentare della potenza computazionale che si ha a disposizione rendendoli vulnerabili ad attacchi sempre più sofisticati, per cui è molto importante mantenere aggiornati i propri applicativi con i metodi di hashing più recenti o, ad esempio, prevedere la reiterazione dello stesso algoritmo di hashing un numero svariato di volte sullo stesso input.

1.4. I protocolli di consenso

Di seguito vengono presentati i più comuni protocolli di consenso che sono sufficienti per capire la loro importanza all'interno di una blockchain. Per una lista più esaustiva dei progetti blockchain e del tipo di proof utilizzato si rimanda all'Appendice.

1.4.1. Proof of Work (PoW)

L'idea principale alla base della Proof of Work consiste nel compiere un lavoro - in termini di consumo delle proprie risorse computazionali - per dimostrare l'impegno che un peer ha con la rete, ricevendo quindi una ricompensa per il lavoro svolto. Solitamente questa operazione viene espressa con il nome *mining*, e chi compie il lavoro prende il nome di *miner*, poiché la si assimila all'estrazione mineraria il cui lavoro porta ad una ricompensa.

L'algoritmo Proof of Work utilizzato in Bitcoin si basa sulla risoluzione di un problema crittografico che dovranno effettuare i miners per creare un nuovo blocco valido nel registro della blockchain. I miners utilizzano come input per l'algoritmo di hash SHA-256 le informazioni presenti nell'header del blocco di transazioni precedente, un numero casuale chiamato "nonce" e un timestamp: riprendendo gli stessi concetti degli algoritmi Hashcash si pone l'obiettivo di "*trovare degli hash con politica SHA-256 tali che che i primi 32 bit su 256 siano 0"*. La modifica di un parametro di input, ad esempio l'incremento del nonce, cambierà l'output successivo in uno completamente diverso e il miner dovrà ripetere la funzione di hash affinché le condizioni dell'algoritmo non saranno soddisfatte. Si noti che il numero di hash da trovare e la condizione che sul valore dei bit iniziali dell'hash trovato sono dei parametri che possono variare nel tempo all'interno della rete e definiscono la *difficoltà di mining*: essa varia sulla base dell'intera potenza di calcolo messa a disposizione nella rete da tutti i peer, in modo da garantire una stabilità del tempo medio di necessario per creare un nuovo blocco della catena.

La Proof of Work viene utilizzata al giorno d'oggi all'interno delle blockchain perché fornisce maggiore sicurezza alla catena: è molto complesso infatti modificare i vecchi blocchi a causa del fatto che la catena valida, per la stragrande maggioranza dei nodi, è quella più lunga, cioè la catena con maggiore potenza di calcolo accumulata. Questa proprietà garantisce che i dati presenti nei vecchi blocchi, per essere modificati, richiederebbero un duro lavoro di calcolo da

parte del peer malevolo per generare autonomamente una blockchain più lunga di quella condivisa con il resto della rete.

Nonostante la prova del lavoro sembri fornire la giusta sicura in una blockchain, ci sono alcuni inconvenienti che dovrebbero essere presi in considerazione:

- **Crescente complessità di estrazione**: la complessità dell'estrazione di un blocco aumenta nel tempo. Questo può essere visto come un punto di forza del protocollo, perché protegge la rete contro il nuovo hardware, ma non lo è. Con l'aumentare della complessità, esistono davvero poche mining industries capaci di spendere abbastanza soldi per ottenere nuovi hardware specifici per estrarre una criptovaluta. Questo potrebbe portare a fare una centralizzazione del potere minerario, che è contraria all'idea di decentramento della blockchain.

- **Utilizzo di energia**: con l'aumento della complessità di estrazione di un blocco, è necessaria sempre più potenza di hashing, che si traduce in un consumo di energia sempre più elevato. Sebbene questo viene definito come il principale problema da risolvere sulle blockchain di tipo PoW in favore di altri tipi di algoritmi più sostenibili, il *troppo consumo* è sempre preferibile che venga rapportato ad altri tipi di fonti di utilizzo, uno studio della Ark Investment nel 2020 approfondisce questo tema e spiega che l'energia richiesta per tenere attiva l'economia di bitcoin è di ordini di grandezza inferiore a scenari di utilizzo per l'estrazione dell'oro o dei sistemi bancari[4].

- **Protezione da attività fraudolente**: Satoshi Nakamoto nel suo whitepaper ha osservato che la struttura della blockchain è funzionale - nel senso che può essere considerata una struttura che opera in maniera decentralizzata - solo se la maggioranza dei nodi è composta da nodi onesti, ciò impedirebbe di effettuare e registrare nei blocchi transazioni fraudolente all'interno della catena: in questo caso si parla di attacco del 51%. Più di recente sono stati ideati degli attacchi che, sotto alcune ipotesi, rischiano di far soccombere la rete ad attacchi anche di percentuali inferiori al 51%: ad esempio il lavoro di I.Eyal e E.Sirer si concentra sul problema che un gruppo con almeno il 34% del potere

[4] https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/ARKInvest_031220_Whitepaper_BitcoinMining.pdf

di mining di hash sulla rete[5] possa essere in grado di modificare la catena e quindi rendere insicura l'intera blockchain.

- **Modalità di distribuzione dei compensi:** l'algoritmo PoW utilizzato all'interno della blockchain di Bitcoin premia soltanto il peer che è riuscito ad estrarre correttamente un nuovo blocco, per questo motivo la varianza della distribuzione dei compensi è molto alta e questo disincentiva il mining diffuso. Per questi motivi sono state proposte varie modifiche al protocollo di Bitcoin per garantire una maggiore fairness sulla distribuzione delle ricompense[6].

1.4.2. Proof of Stake (PoS)

Nei meccanismi della *Proof of Stake*, i validatori dei blocchi vengono scelti in base alla loro disponibilità di bloccare (mettere in "stake") parte delle proprie criptomonete per guadagnare la possibilità di inserire un nuovo blocco nella catena: la distribuzione della probabilità che un peer sia scelto non è quindi uniforme, dipende infatti dall'ammontare di *stake* che ha un peer all'interno della catena. Questo fornisce sicuramente un primo vantaggio che non è possibile raggiungere con la Proof of Work, e cioè che il tempo computazionale per la generazione di un blocco si riduce notevolmente fornendo maggiore velocità (*rate*) alla crescita della catena con un consumo di risorse, in termini energetici, molto alto. Queste sono le principali ragioni che hanno spinto molti investitori a finanziare progetti basati su blockchain di tipo PoS e a ripensare e re-ingegnerizzare le blockchain di tipo PoW con soluzioni più sostenibili nel tempo (si veda il caso di Ethereum e il passaggio alla Beacon Chain[7]).

La Proof of Stake viene al momento utilizzata nei progetti basati su blockchain, il cui valore degli utenti è regolato dal possesso di una criptovaluta (si veda paragrafo dedicato alle Criptovalute). In generale se un utente vuole entrare a far parte della blockchain con PoS e vuole essere coinvolto nella generazione dei blocchi della catena, deve acquistare/possedere un certo

[5]Ittay Eyal and Emin Gün Sirer, Majority is not enough: bitcoin mining is vulnerable, Communications of the ACM - Volume 61, Issue 7, July 2018 pp 95-102, https://doi.org/10.1145/3212998.

[6] Bazzanella, D., Gangemi, A. Bitcoin: a new proof-of-work system with reduced variance. Financ Innov 9, 91 (2023). https://doi.org/10.1186/s40854-023-00505-2

[7] https://ethereum.org/en/upgrades/beacon-chain/

importo della valuta, e “bloccare” parte di esso come risorsa crittografica che indicherà la disponibilità dell’utente a generare nuovi blocchi. La blockchain ricompenserà gli utenti che generano nuovi blocchi con un ammontare della stessa cripto-valuta.

Molti servizi di exchange forniscono i cosiddetti **Staking Pools**, ovvero l’exchange stesso diventa un utente vero e proprio della catena: un utente che acquista la moneta della blockchain all’interno dell’exchange non fa altro che mettere a disposizione un ammontare della valuta in un portafoglio comune gestito dall’exchange aumentando così il proprio potere di staking e aumentare le probabilità di essere scelti per la generazione di nuovi blocchi. L’exchange successivamente distribuirà la ricompensa ai propri utenti.

Anche in una blockchain PoS però non bisogna sottovalutare alcuni aspetti che sono fondamentali per la vita della blockchain stessa:

- **Monopolio**: il principale svantaggio degli algoritmi PoS è che potrebbe essere possibile un potenziale monopolio da parte dei principali stakeholders della rete. Questa possibilità mette quegli algoritmi allo stesso livello di PoW, situazione che dovrebbe essere evitata per garantire una migliore distribuzione della ricompensa tra i vari peers. In ogni caso il problema può essere facilmente risolto ad esempio definendo una rotazione tra gli utenti “più ricchi” che partecipano alla generazione del blocco, o temporizzando lo stake di questi utenti in modo che maggiore è la posta in gioco messa a disposizione, più stretto è il tempo in cui l’ammontare viene bloccato per lo stake.

- **Niente in gioco**: per quanto riguarda qualsiasi blockchain proof-of-work, di fronte a un attacco double-spend o in un chain fork, i nodi avranno tre opzioni tra cui scegliere:
    - Segui la catena 1 e probabilmente trarrai vantaggio se la catena 1 vince.
    - Segui la catena 2 e probabilmente ottieni vantaggio se la catena 2 vince.
    - Non fare nulla e non ottenere alcun beneficio. È possibile scegliere solo una di queste tre opzioni, altrimenti si sprecherebbe energia nell'estrazione mineraria sulla catena sbagliata, costando un sacco di soldi in termini di elettricità. Usando il protocollo proof of stake, questa situazione cambia.

Tenendo presente il piccolo costo dell'energia per la creazione di un blocco in un ambiente PoS, potresti facilmente seguire le due catene create utilizzando meno energia rispetto a un minatore

blockchain proof-of-work. Se si verifica questa situazione, la blockchain non avrà ordine e quindi sarà un caos. Inoltre, se viene seguita più di una catena unica, è probabile che ci siano più fork, il che potrebbe causare più caos.

1.4.3. Proof of Authority (PoA)

La Proof of Authority (PoA) è un algoritmo di consenso basato sulla reputazione che introduce una soluzione pratica ed efficiente per i network blockchain (soprattutto quelli privati). Il termine è stato proposto nel 2017 dal co-fondatore ed ex-CTO di Ethereum Gavin Wood. L'algoritmo di consenso PoA fa uso del **valore delle identità**: significa che i convalidatori dei blocchi mettono in stake la propria reputazione al posto delle monete. Di conseguenza, le blockchain PoA sono protette dai nodi di convalida che vengono selezionati arbitrariamente come entità affidabili. Il modello Proof of Authority si basa su un numero limitato di convalidatori, fattore che lo rende un sistema altamente scalabile. I blocchi e le transazioni sono verificati da partecipanti pre-approvati, che fungono da moderatori del sistema.

PoA consente alle imprese di mantenere la propria privacy e allo stesso tempo avvalersi dei vantaggi della tecnologia blockchain. Microsoft Azure è un altro esempio di compagnia che applica la PoA. In poche parole, la piattaforma Azure fornisce soluzioni per network privati, con un sistema che non richiede una valuta nativa come il 'gas' di ether, dato che il network non ha bisogno di mining. L'algoritmo di consenso PoA può essere applicato in un gran numero di scenari ed è considerato un'opzione valida per le applicazioni logistiche: nelle catene di fornitura (supply chain), ad esempio, la PoA è ritenuta una soluzione efficace e adeguata.

Proof of Authority vs Proof of Stake

Alcuni considerano la PoA come una versione modificata della PoS, che fa uso dell'identità invece delle monete. A causa della natura decentralizzata di gran parte dei network blockchain, a volte la PoS non è adatta per certe attività e imprese. Al contrario, i sistemi PoA possono rappresentare una soluzione migliore per le blockchain private viste le prestazioni notevolmente migliori.

Sebbene le condizioni per il Consenso Proof of Authority possano variare da sistema a sistema, l'algoritmo di consenso PoA dipende solitamente da:

- identità valide e affidabili: i convalidatori devono confermare le proprie identità reali.

- difficoltà nel diventare un convalidatore: un candidato deve essere disposto a investire denaro e mettere in gioco la propria reputazione. Un processo rigoroso riduce il rischio di selezionare convalidatori dubbi e incentiva un impegno a lungo termine.

- uno standard per l'approvazione dei convalidatori: il metodo per selezionare convalidatori deve essere uguale per tutti i candidati.

Il senso del meccanismo di reputazione è la certezza dell'identità di un convalidatore. Il processo non può essere facile, né può essere abbandonato facilmente: deve in pratica riuscire a sbarazzarsi dei malintenzionati. Infine, fare in modo che tutti i convalidatori vengano sottoposti alla stessa procedura garantisce l'integrità e l'affidabilità dell'intero sistema.

Limiti della PoA

L'impressione del meccanismo PoA è che rinuncia alla decentralizzazione. Si potrebbe quindi dire che il modello introdotto da questo algoritmo di consenso è solo uno sforzo per rendere più efficienti i sistemi centralizzati. Sebbene questo renda la PoA una soluzione attraente per le grandi aziende con esigenze logistiche, suscita una certa esitazione - soprattutto nell'ambito delle criptovalute. I sistemi PoA offrono un'elevata capacità di elaborazione, ma la possibilità di censura e blacklisting mettono in dubbio la loro immutabilità.

Un'altra critica frequente riguarda le identità dei convalidatori PoA, le quali sono visibili a chiunque. La risposta a questo argomento è che solo individui stabiliti in grado di occupare questa posizione cercherebbero di diventare convalidatori (come partecipante noto al pubblico). Nonostante questo, conoscere le identità dei convalidatori potrebbe potenzialmente portare a manipolazione da parte di terzi. Per esempio, se un competitore vuole ostacolare un network basato sulla PoA, potrebbe influenzare convalidatori noti per farli agire in modo disonesto e compromettere il sistema dall'interno.

PoW, PoS, o PoA hanno tutti i propri vantaggi e svantaggi unici. E' risaputo che la decentralizzazione ha un enorme valore nella comunità delle criptovalute e la PoA, come meccanismo di consenso, la sacrifica per raggiungere alte prestazioni e scalabilità. Le funzionalità inerenti ai sistemi PoA sono in netto contrasto con i network blockchain utilizzati finora. Nonostante ciò, la PoA presenta un interessante approccio e non può essere trascurata come soluzione blockchain emergente, adatta soprattutto a applicazioni blockchain private.

1.5. Ottimizzare la Blockchain: Merkle Tree

Dato che l'efficienza di una blockchain è correlata al numero di blocchi che essa possiede, e quindi alla sua dimensione, è necessario trovare un metodo molto performante per garantire la navigazione della catena, la ricerca di transazioni all'interno di essa, la validazione di nuovi blocchi e soprattutto fare in modo che la modifica o la compromissione di un blocco venga intercettato e annullato con rapidità. Gli utenti che partecipano alla blockchain sono le stesse entità che si occupano di validare i blocchi presenti all'interno della catena, devono necessariamente avere a disposizione l'intera base di dati, dal primo nodo fino all'ultimo, il che si traduce in un consumo di banda molto elevato e soprattutto ci si affida alla disponibilità dell'utente di conservare i dati della catena che possono raggiungere anche dimensioni superiori ai 100GB[8].

Un contributo molto importante è stato dato da Ralph Merkle che, nel 1979, ha ideato una soluzione molto efficiente per i processi di verifica di grandi quantità di dati, che è possibile applicare a strutture come le blockchain.

Questa nuova applicazione prende il nome di **Merkle Tree** e le sue caratteristiche possono essere riassunti nei seguenti punti:

- Le informazioni vengono conservate per mezzo di una struttura ad albero.
- La loro struttura permette di adattarsi facilmente non solo alle blockchain ma a diversi tipi di architetture informatiche, dalle basi di dati alle applicazioni di reti peer-to-peer in generale

[8] https://101blockchains.com/blockchain-size/

- Verificano rapidamente l'integrità di un blocco della catena utilizzando funzioni di hashing, che sono computazionalmente efficienti per i propri processi di verifica.
- Velocizzano la ricerca di singoli elementi (transazioni) all'interno della blockchain.
- Favoriscono il recupero dei blocchi dell'intera catena o parte di essa, diminuendo la quantità di dati da trasmettere, e quindi migliorando la banda necessaria al trasferimento, dando la possibilità di conservare la blockchain anche su dispositivi con memoria più limitata come i dispositivi mobile.

Il Merkle Tree è stato con successo implementato su Blockchain come Bitcoin. Se volessimo generalizzare l'applicazione del Merkle Tree su una Blockchain possiamo tenere in considerazione le seguenti proprietà del grafo da applicare ad ogni singolo blocco della catena:

- Il blocco contiene una lista di transazioni, ogni transazione ha un proprio identificativo. Si può immaginare ogni transazione come un nodo foglia del Merkle Tree: due o più nodi vengono considerati per il calcolo del valore di hash del nodo padre. Si prendano ad esempio due transazioni identificate da un valore di hash $\mathbf{T_1}$ e $\mathbf{T_2}$:

  $$\mathbf{H_X} = \boldsymbol{H}\ (\mathbf{T_1} \,||\, \mathbf{T_2})$$

  Applicando quindi una funzione di hash ***H()*** alla concatenazione dei valori di hash dei suoi nodi figli, si ottiene un nuovo valore $\mathbf{H_p}$ che sarà assegnato al nodo padre.

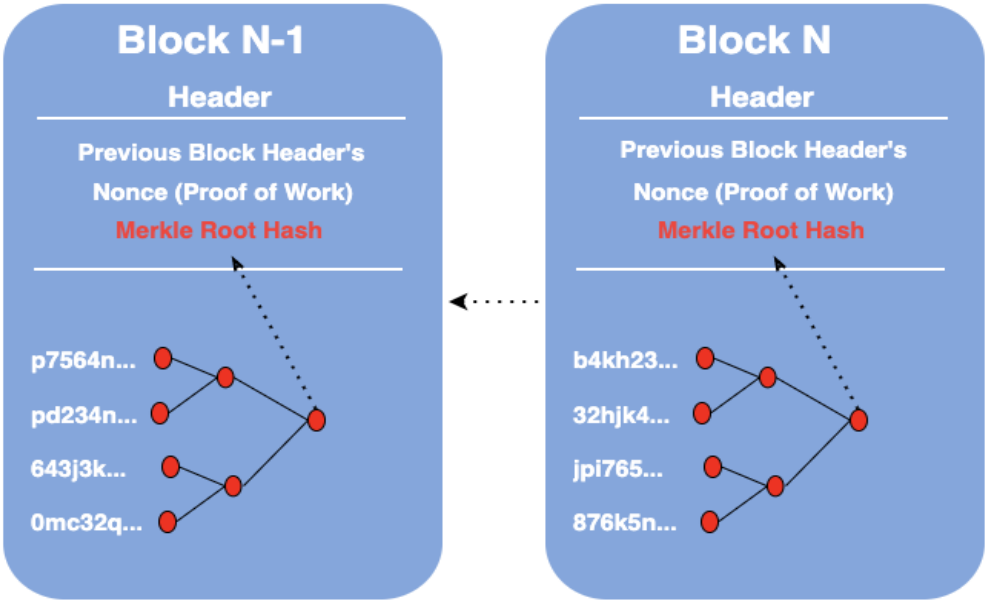
- L'algoritmo si ripete generando un nuovo livello superiore di nodi, i cui figli corrispondono ai nodi padre precedentemente creati, e il cui nuovo valore di hash è dato proprio dalla funzione ***H()*** applicata alla concatenazione dei valori di hash dei suoi nodi figli:

  $$\mathbf{H_P} = \boldsymbol{H}\ (\mathbf{H_{X1}} \,||\, \mathbf{H_{X2}})$$

- L'algoritmo termina dopo la generazione del nodo radice - che prende il nome di **Merkle Root** - e del suo valore di hash. Questo valore viene poi salvato come proprietà del blocco stesso.

- Quando una nuova transazione viene convalidata e aggiunta nel blocco, tutti i valori di hash dei nodi dell'albero vengono ricalcolati fino al Merkle Root: si osservi che se la

transazione non aggiunge nuovi nodi padri, il calcolo può essere ottimizzato considerando solo i nodi del ramo della nuova transazione. Il nuovo valore del Merkle Root viene distribuito a tutti i nodi, in questo modo il blocco può considerarsi aggiornato.



Presenza del valore del Merkle Root all'interno di un blocco.

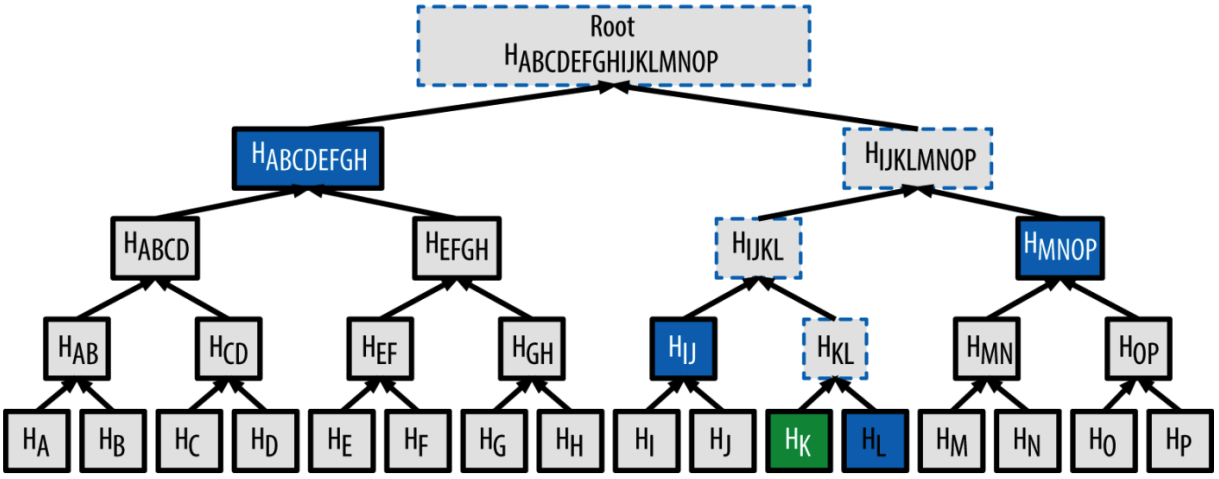
Verifica della presenza di una transazione

Il Merkle Root può considerarsi come il valore di checksum di ogni singolo blocco, un utente della blockchain infatti potrebbe conoscere i singoli blocchi nella loro totalità delle transazioni che li compongono - questi utenti sono chiamati *Full Node*s - oppure possedere solo una parte dei blocchi, questi utenti prendono appunto il nome di Light Nodes. Questi utenti infatti pur avendo una conoscenza parziale della blockchain possono comunque far parte del processo di validazione della presenza/integrità di una transazione all'interno di un blocco attraverso la cosiddetta **Merkle Proof:** essa consiste nel ricalcolare il Merkle Root del blocco secondo il seguente algoritmo:

- Se H(X) è la transazione da verificare, si prende in considerazione la transazione vicina $H_S(X)$ tramite la quale era stato creato l'hash del loro nodo padre dell'albero H_P.

- A questo punto ripeti il procedimento considerando il nodo allo stesso livello del nodo padre di cui era stato calcolato l'hash e sali di livello nel ricalcolo fino al nodo radice.

Questo significa che per una lista di transazioni che creano un Merkle Tree di profondità N, il ricalcolo del Merkle Root ha una complessità computazionale pari a *O(N)*. Questa procedura è più comunemente nota come ***Verifica semplificata del pagamento (SPV)*** ed è stata descritta da Satoshi Nakamoto nel Whitepaper di Bitcoin (si veda il Cap. 1.7.1).



Merkle Proof, si noti come per calcolare la corretta appartenenza della transazione H_K al blocco è sufficiente applicare il calcolo dell'hash solo in relazione ai blocchi evidenziati in blu.

1.6. Automatizzare la Blockchain: gli Smart Contracts

Se volessimo dare una definizione di Smart Contract sarebbe opportuno riprendere quella data da Gideon Greenspan[9]: "Un contratto smart è un pezzo di codice che viene memorizzato su una blockchain, attivato da transazioni su blockchain e che legge e scrive i dati nel database di quella blockchain". In effetti si tratta proprio di un software che, per volontà degli individui coinvolti nell'accordo, collegano il verificarsi di alcune condizioni applicative a degli esiti che per natura stessa del contratto sono vincolanti. Sono stati teorizzati da Nick Szabo nel 1994[10]. A differenza di altri tipi di contratti che possono essere digitali o meno, una delle peculiarità è il fatto che il contratto non può essere bloccato da interventi manuali una volta che è stato attivato, non esiste quindi un'entità che può modificarne l'esecuzione o bloccarne la sua validità: ovviamente questo giustifica il fatto che lo smart contract deve risiedere all'interno di una blockchain dove possono essere garantiti i concetti di decentralizzazione e irrevocabilità della transazione.

Gli Smart Contracts possono essere sviluppati nei linguaggi di programmazione maggiormente conosciuti (C++, Javascript, Python, Go) sulla base del linguaggio previsto dalla blockchain, ma si stanno via via delineando dei linguaggi dedicati sempre più sofisticati, che permettono di rappresentare anche in maniera più "parlante" le attività da lanciare in un contratto. Si prenda ad esempio i linguaggi **Solidity** e **Vyper** utilizzati da Ethereum[11]. Si veda nell'immagine un esempio di contratto scritto in linguaggio Solidity per gestire il trasferimento di una somma di coins da un pagatore ad un ricevente.

La realizzazione di uno smart contract, prendendo come esempio la blockchain di Ethereum (che sarà descritto nei prossimi paragrafi), può essere riassunta in un processo attraverso i seguenti punti:

- L'utente della blockchain apre un Digital Wallet (come ad esempio MetaMask) e deposita degli ETH sul wallet creato.
- Per scrivere uno smart contract utilizza il servizio web remix.ethereum.org, un IDE di sviluppo che permette di testare i contratti che si stanno creando.

[9] http://www.gidgreen.com/

[10] https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[11] https://ethereum.org/en/developers/docs/smart-contracts/languages/

- Dopo aver distribuito lo smart contracts sempre dalla piattaforma precedente, l'utente può visitare il sito **https://etherscan.io/contractsVerified**, un servizio che permette di vedere gli smart contracts caricati e validati in piattaforma Ethereum e può selezionarlo.

Gli Smart Contracts possono essere anche di diversi tipi. Alcuni ad esempio possono essere contratti di Token presenti sul mercato, altri invece potrebbero servire per approvare i vari processi della blockchain come lo staking, il farming e il liquidity mining.

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >= 0.7.0;

contract Coin {
    // The keyword "public" makes variables
    // accessible from other contracts
    address public minter;
    mapping (address => uint) public balances;

    // Events allow clients to react to specific
    // contract changes you declare
    event Sent(address from, address to, uint amount);

    // Constructor code is only run when the contract
    // is created
    constructor() {
        minter = msg.sender;
    }

    // Sends an amount of newly created coins to an address
    // Can only be called by the contract creator
    function mint(address receiver, uint amount) public {
        require(msg.sender == minter);
        require(amount < 1e60);
        balances[receiver] += amount;
    }

    // Sends an amount of existing coins
    // from any caller to an address
    function send(address receiver, uint amount) public {
        require(amount <= balances[msg.sender], "Insufficient balance.");
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        emit Sent(msg.sender, receiver, amount);
    }
}
```

Esempio di Smart Contract implementato in linguaggio Solidity. Si noti la somiglianza del linguaggio a quelli più comuni Object Oriented.

1.7. Applicazioni della Blockchain

Dopo aver fornito una panoramica generale delle caratteristiche tecniche di un sistema basato su Blockchain, vengono adesso presentati dei progetti che hanno applicato realmente una blockchain: principalmente questi progetti sono nati nel settore economico/finanziario, e si darà risalto al primo vero progetto in ambito blockchain ovvero Bitcoin, che ha permesso di capire le vere potenzialità di un sistema decentralizzato, governato da una criptomoneta. Cercando di descrivere Bitcoin sottolineando la distinzione che esiste tra il progetto e la criptovaluta che regola le ricompense del suo sistema - infatti per chi si approccia per la prima volta ai temi delle blockchain e delle criptovalute cade facilmente in questo errore - saranno presentate successivamente alcune piattaforme come Ethereum e Cardano che inglobano progetti di natura e scopi diversi, con la realizzazione di nuovi elementi digitali che regolano le transazioni di questi sistemi, ma basati tutti su una struttura comune, proprio la blockchain. Si fornirà qualche cenno sui ***Non Fungible Token (NFT)***, un nuovo elemento di scambio/valore per oggetti fisici o virtuali che ha senso solo se di base c'è una struttura blockchain a regolare le transazioni. Alla fine si presenteranno alcuni progetti che si distaccano dal settore finanziario, come le supply chain, e si forniranno degli spunti sui quali la blockchain potrebbe, in futuro non molto lontano, prendere il sopravvento.

1.7.1. Bitcoin (BTC) e il mondo delle Criptovalute

La storia del progetto Bitcoin è tanto avvincente e misteriosa quanto i suoi creatori, sempre se chi si cela sotto il nome di Satoshi Nakamoto non sia un solo sviluppatore o un gruppo di persone che utilizzano questo pseudonimo. Ciò che si sa è che Satoshi Nakamoto non corrisponde a nessuna persona reale, ma vi sono state molte speculazioni a riguardo. Tutto inizia Bitcoin nel 2008, quando "Satoshi Nakamoto" pubblicò un White Paper intitolato *"Bitcoin: A Peer-to-Peer Electronic Cash System"* [12]: questo documento descrive una nuova valuta completamente digitale che utilizza la crittografia per garantire la sicurezza e la privacy delle transazioni senza la necessità che fosse presente all'interno di questo mercato un'entità regolatore. Nakamoto il 3 Gennaio del 2009, basando lo sviluppo del progetto su un ledger distribuito con l'architettura blockchain, ha sviluppato il software per Bitcoin e ha creato il primo

[12] https://bitcoinwhitepaper.co/

blocco di transazioni, noto come *"Genesis Block"*. Questo ha dato il via al sistema Bitcoin, in cui i blocchi di transazioni sono creati e aggiunti alla blockchain tramite un processo noto come ***mining***. Il processo di mining è un sistema computazionale intensivo che utilizza i concetti della Proof of Work (PoW) - descritti nel Capitolo precedente - e richiede la partecipazione degli utenti della blockchain a risolvere un complesso problema matematico mettendo a disposizione le proprie risorse di calcolo: lo scopo è quello di *estrarre* l'identificativo del blocco successivo della blockchain, verificarlo facilmente ed accettarlo solo se un certo lavoro è stato fatto per ottenere questo risultato, impedendo così la creazione arbitraria di nuovi blocchi da parte di chiunque. Il lavoro computazionale compiuto dagli utenti che riescono ad estrarre un nuovo blocco del ledger viene ricompensato in BTC, la criptovaluta del sistema, e questo invoglia i partecipanti della blockchain a investire notevoli somme di denaro sull'acquisto di hardware specializzato, come processori grafici (GPU) o circuiti integrati specifici per l'applicazione (ASIC), in quanto il lavoro richiesto è troppo complesso per i comuni computer, un investimento che viene notevolmente ricompensato al crescere della blockchain, in quanto la probabilità di estrazione, per il tipo di problema matematico da risolvere, diventa sempre più bassa alla scoperta di un nuovo blocco.

L'operazione che deve essere eseguita per il mining consiste nel trovare una stringa il cui valore di hash, applicando l'algoritmo SHA-256, contenga un certo numero di zeri iniziali. A causa dell'irreversibilità della funzione di hash, l'unico modo per poter ricercare un valore che soddisfi questo risultato è effettuare numerosi tentativi con input sempre diversi, affinché non si arrivi ad una soluzione. Dato che la complessità computazionale della risoluzione della challenge è proporzionale esclusivamente al numero di "0" iniziali nell'hash, questo valore variabile prende il nome di *"target di difficoltà",* ed è proprio il valore che il sistema Bitcoin regola automaticamente ogni 2016 blocchi, in modo da mantenere il tempo medio di creazione di un blocco a circa 10 minuti.

Bitcoin è diventato rapidamente popolare tra gli appassionati di criptovalute e gli investitori, con il prezzo che è aumentato notevolmente nel corso degli anni. Nel 2010, il valore di un singolo Bitcoin era di pochi centesimi, ma nel 2021 ha raggiunto un massimo storico di quasi $69.000. Nonostante l'anonimato di Nakamoto, il suo lavoro su Bitcoin ha avuto un impatto significativo sulla tecnologia delle criptovalute e sulla finanza globale in generale: ha aperto la strada ad altre criptovalute, che hanno la possibilità di rivoluzionare il modo in cui le persone pensano al denaro e alle transazioni finanziarie ed è stato importante per aprire la strada a nuovi sviluppi

tecnologici sulle strutture di database decentralizzate. Ad oggi esisterebbe una lista di cento e più progetti blockchain regolati da criptovaluta, ma che hanno aggiunto elementi di interesse rispetto a Bitcoin più sensibili ai temi del consumo energetico utilizzando soluzioni diverse e più performanti del PoW, e che hanno reso il mercato delle criptovalute un asset finanziario a tutti gli effetti con valide alternative a BTC su cui investire.

1.7.2. Non-Fungible Token

Il termine NFT sta per "Non-fungible Token" e può essere descritto come un'entità crittografica che certifica qualcosa di unico e non riproducibile, come ad esempio la proprietà di un oggetto digitale, l'autenticità di un bene: gli eventi degli ultimi anni che hanno visto esplodere l'utilizzo degli NFT hanno dimostrato che essi possono essere applicati anche come mezzo per la protezione della proprietà intellettuale (*IP*).

Vedono la loro prima applicazione nella piattaforma Ethereum (che descriveremo nel paragrafo successivo). Quando si parla di NFT si commette facilmente l'errore di paragonarli alle criptovalute, in realtà la distinzione è molto netta perchè la criptovaluta può essere paragonata ad una moneta reale di un unico taglio ed un suo valore, e tutte le monete della stessa valuta possiedono dunque lo stesso valore: per cui le criptovalute perdono il concetto di irriproducibilità. Gli NFT invece, essendo oggetti unici tra di loro, possiedono anche un valore intrinseco diverso sulla base di cosa essi stessi rappresentano. La criptovaluta potrebbe invece essere un mezzo di scambio per trasferire ad esempio il possesso o l'acquisto di un NFT applicato ad un'opera d'arte digitale dal creatore all'acquirente, o dall'attuale possessore ad un altro. È possibile classificare gli NFT a seconda di proprietà chiave come quelle che seguono [13]:

- ***Verifiability***: l'NFT e i dati a esso correlati, come la sua proprietà, può essere verificata pubblicamente consultando la blockchain a cui esso appartiene.

- ***Transparent Execution***: le attività degli NFT, incluse la creazione, la vendita e l'acquisto sono accessibili a tutti in maniera trasparente.

[13] Qin Wang, Rujia Li, Qi Wang, Shiping Chen, Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges (Tech Report)

- ***Availability***: il sistema NFT non crolla mai, non ha periodi di down come succede alle piattaforme più diffuse (come Whatsapp), bensì tutti i token e gli NFT emessi sono sempre disponibili per la vendita e per l'acquisto, resilienza garantita dalla blockchain. L'unica instabilità può riguardare il prezzo, ma ciò deriva dalla domanda e dalla richiesta del mercato e non dalla tecnologia in sé.

- ***Tamper-resistance***: grazie alla blockchain, i dati e le informazioni relative alle transazioni vengono archiviati in modo persistente e non possono essere modificati una volta che lo scambio viene confermato.

- ***Usability***: ogni NFT contiene le informazioni più aggiornate, rendendoli al passo con i tempi, facilmente accessibili e utilizzabili.

- ***Atomicity***: il trading e la compravendita degli NFT può essere completato in un'unica transazione chiamata ACID (acronimo di Atomic, Consistent, Isolated e Durable). Se dovesse fallire uno dei processi previsti per il completamento della transazione, l'intero processo esegue un rollback e le proprietà degli assets digitali tornano ai rispettivi possessori prima della transazione.

- ***Tradability***: ogni NFT e ogni oggetto corrispondente può essere venduto e scambiato in maniera arbitraria. La possibilità e la volontà di scambio dell'asset digitale dipendono esclusivamente dagli attori che vogliono portare a termine la transazione.

1.7.3. Ethereum (ETH)

Ethereum è una piattaforma digitale open source basata sulla tecnologia blockchain. Ideata da Vitalik Buterin, è la piattaforma nel quale circola la criptovaluta ***Ether (ETH)*** e raggruppa moltissimi progetti e applicazioni distribuite. Nel 2013, Buterin si avvicina alla tecnologia blockchain quando viene coinvolto nel progetto di Bitcoin come programmatore e co-fondatore della rivista Bitcoin Magazine, egli inizia però ad accorgersi delle limitazioni offerte da Bitcoin e per questo motivo decide di realizzare una piattaforma decentralizzata basata sempre sulla filosofia che i processi non devono necessitare di intermediari e che le applicazioni di una

blockchain non dovessero soltanto essere rivolte all'ambito finanziario, ma grazie agli Smart Contract e alle Decentralized Apps (*DApps*) le possibilità di utilizzo diventano praticamente infinite. A differenza di Bitcoin, Buterin inserisce anche il concetto di utente ***permissionless*** (come Bitcoin) - che non ha alcun limite nella validazione delle transazioni all'interno della blockchain - e di utente ***permissioned,*** limitato invece alla validazione.

L'architettura della blockchain di Ethereum è composta da due parti principali: la blockchain come distributed ledger technology, e la macchina virtuale Ethereum (***Ethereum Virtual Machine***, o più comunemente rappresentata dal suo acronimo ***EVM***). La EVM è una macchina virtuale intesa come un software che gira su uno strato applicativo posto sopra la blockchain, che consente l'esecuzione di logiche sviluppate in codice di programmazione, distribuite, e validate dagli utenti che fanno parte della blockchain: queste logiche sono appunto gli Smart Contracts di cui abbiamo parlato nel Capitolo precedente. Un'applicazione decentralizzata o (DApp) sviluppata su piattaforma Ethereum si caratterizza proprio dal codice che gira sulla sua Virtual Machine.

Ethereum, come Bitcoin, viene sviluppato utilizzando Proof of Work come protocollo di consenso per validare le transazioni e garantire la sicurezza della rete, ma ovviamente questa scelta è stata sempre sensibile alle limitazioni che il protocollo comporta soprattutto quando, oltre al consumo di risorse computazionali, il sistema deve garantire un'efficienza sul numero di transazioni per intervallo di tempo, che rispetto a Bitcoin tendono ad ordini di grandezza superiori. Per questo Buterin ha sempre ritenuto che, finchè Ethereum si basa su PoW, non potrà mai mostrare le sue vere potenzialità e per questo motivo decide di dare inizio ad un progetto, chiamato **Ethereum 2 (ETH2)**, che invece è basato sul protocollo di consenso Proof of Stake[14] ed è stato attivato nel Settembre del 2022 tramite un evento che la community di Ethereum ha chiamato "The Merge", il nome infatti fa riferimento alla fusione della precedente blockchain Beacon Chain basata su PoS - usata come banco di prova per la migrazione - che poi è diventata la nuova Ethereum 2.

[14] https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/

Gas

Il termine *"Gas"* sta ad indicare l'unità di misura utilizzata per rappresentare il costo computazionale delle operazioni del protocollo Ethereum. Per capire meglio il suo significato è necessario dare un introduzione alla Ethereum Virtual Machine (EVM), ovvero l'ambiente applicativo all'interno del quale gli smart contracts sono eseguiti sulla blockchain attraverso una serie di operazioni. Ciascuna di queste operazioni consuma una serie di risorse per essere eseguita, e quindi utilizzano quello che più generalmente si intende come energia, o lavoro. Poiché i miners, durante le attività di estrazione di nuovi blocchi nella blockchain, devono utilizzare molta energia, si è reso necessario introdurre un'unità di misura per quantificare il loro lavoro svolto (e quindi l'energia consumata) dalle loro operazioni. La quantificazione del lavoro svolto nella blockchain permette di offrire una ricompensa ai miners proporzionale alle operazioni di esecuzione degli smart contracts o delle transazioni. Si parla di Gas soltanto quando si fa riferimento al lavoro compiuto sulla piattaforma Ethereum.

È importante notare che il Gas, sebbene il suo valore sia dato dalla criptovaluta ETH come ricompensa di un lavoro, non è in alcun modo rappresentabile con un Token. Infatti se ad esempio c'è bisogno di eseguire uno smart contract e questo consuma in termini computazionali 10 Gas, indipendentemente da chi eseguirà il contratto il costo computazionale sarà sempre lo stesso (circa 0.0004 ETH), ma in termini economici il suo valore in Euro dipende esclusivamente dal rapporto tra la criptovaluta ETH e la valuta di confronto. Questa distinzione è necessaria proprio per tenere separato il costo intrinseco di esecuzione in termini di energia consumata, dal valore della criptovaluta usata come ricompensa.

Token ERC-20

Ethereum permette la creazione di Non Fungible Token attraverso dei protocolli standard definiti dalla blockchain, essi sono identificati con il prefisso ***ERC (Ethereum Request for Comment)*** e un numero di versione, sulla base della quale ogni Token di Ethereum evolve alcune caratteristiche di interoperabilità nel contesto della blockchain.

ERC-20[15] è un protocollo, creato nel 2015 da Fabian Vogelsteller, che definisce uno standard delle API per poter creare NFT all'interno di uno Smart Contract. Di seguito si elencano alcuni dei principali metodi che è possibile utilizzare con questo Token:

- *name()* : campo opzionale, identifica il nome del Token
- *symbol()* : campo opzionale, identifica il symbol del Token
- *decimals()* : campo opzionale, indica le cifre decimali del Token
- *totalSupply()* : indica il numero totale dei Token esistenti
- *balanceOf()* : indica il numero totale di Token posseduti da un particolare account
- *transfer()* : trasferisce un numero di Token dall'account del mittente all'indirizzo specificato
- *transferFrom()* : così come il metodo transfer(), ma specifica l'indirizzo dal quale effettuare il trasferimento
- *allowance()* : indica il numero di Token che un utente può spendere per conto del proprietario attraverso il metodo transferFrom()
- *approve()* : Indica il numero di Token che un utente può spendere.

Il Token ERC-20 specifica anche dei trigger, cioè delle azioni che possono scattare al verificarsi di un particolare evento, questi sono:

- *Transfer()* : trigger che scatta quando i token sono trasferiti
- *Approved()* : trigger che scatta ogni volta che il metodo approve() viene eseguito con successo.

Il Token ERC-20 è utilizzato con successo in famosi progetti basati su blockchain come ad esempio **USDC**[16], una stablecoin lanciata dalla società Circle di valore pari al Dollaro Americano (USD) che è possibile acquistare nei principali exchange di criptovalute e che può essere considerata la rispettiva moneta virtuale del Dollaro. Un altro esempio in cui è stato utilizzato questo token è la criptovaluta UNI correlata al progetto **UniSwap**[17], il cui ecosistema permette di creare dei pozzi di liquidità rappresentati dalla criptovaluta stessa che viene utilizzata per facilitare gli scambi tra criptomonete/Token ERC-20 di natura completamente diversa. Infatti questo Token è uno dei più utilizzati in ambito trading proprio per le sue capacità di adattarsi molto bene agli scambi di monete virtuali.

[15] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md
[16] https://www.circle.com/en/usdc
[17] https://uniswap.org/

Token ERC-721

ERC-721[18] è stato creato nel 2018 da Dieter Shirley, jacob Evans, Natassia Sachs e William Entriken e rappresenta un altro standard per la creazione di NFT.
Così come ERC-20 esso possiede dei metodi molto simili che permettono di gestire le transazioni per gli acquisti/scambi di digital assets, e si differenzia per alcuni metodi come ad esempio:

- *balanceOf()* : indica il numero di token che un account possiede
- *ownerOf()* : il Token ID del proprietario
- *safeTransferFrom()* : trasferisce in maniera sicura i token da un account di un proprietario ad un altro account.
- *setApprovalForAll()* : da la possibilità ad un operatore di chiamare il metodo safeTransferFrom() o transferFrom() su ogni token posseduto dall'account chiamante
- *isApprovedForAll()* : controlla se un operatore può gestire tutti gli asset del proprietario.

Anche la gestione dei trigger all'avvenuto trasferimento o approvazione è previsto in questo Token. A partire da ERC-721 sono state sviluppate molte estensioni tra differenti tipi di smart contracts, tra i più comuni possiamo citare ad esempio ***ERC721Enumerable***, che supporta dei metodi aggiuntivi per enumerare i token di un proprietario (anche se queste soluzioni vengono poco utilizzati per i costi di gestione all'interno della blockchain) , oppure il più recente ***ERC721A*** che implementa diversi metodi per ridurre le fee sulle transazioni permettendo agli utenti di coniare più NFT e raggrupparli in un' unica transazione.

Token ERC-1155

ERC-1155[19] nasce con l'obiettivo di risolvere alcune limitazioni dei Token precedenti, in particolare ERC-721 e i tentativi successivi del protocollo per gestire gruppi di transazioni con meno carico computazionale, ottimizzando i consumi della blockchain.
Il Token vede la sua nascita attorno al progetto Enjin[20], una piattaforma basata su Ethereum che permette di creare, archiviare, distribuire e commerciare asset digitali attraverso i Token.

[18] https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md
[19] https://eips.ethereum.org/EIPS/eip-1155
[20] https://enjin.io/

L'aspetto più rilevante è che la differenza tra ERC 1155 e ERC 721 si concentra principalmente sul supporto per i trasferimenti in batch. ERC-1155 permette di includere più asset in un unico contratto smart, consentendo così il loro trasferimento con una congestione di rete limitata e costi di transazione inferiori. Un ulteriore punto di forza dello standard dei token ERC 1155 è il supporto di Token, non fungibili e fungibili, con la possibilità di supportare più stati su un singolo contratto e indirizzo.

Lo standard ERC-1155 si distingue tra ERC 1155 e ERC 721 per la capacità di creare anche Token semi-fungibili: essi servono fondamentalmente come gettoni fungibili durante la negoziazione, e solo successivamente diventeranno NFT quando saranno riscattati. Un altro aspetto degno di nota dello standard dei token ERC-1155 è la possibilità di applicare operazioni di rollback sulle transazioni per annullare i trasferimenti di Token.

1.7.4. Il Progetto Cardano (ADA)

Dovendo presentare in questo elaborato i principali progetti basati su blockchain, si vuole dedicare uno spazio anche al Progetto Cardano: il motivo non risiede tanto nel valore economico della sua criptomoneta ADA - infatti non la si può collocare sui livelli raggiunti da Bitcoin ed Ethereum - che la farebbero sembrare una tra le tante criptovalute in circolazione, ma è importante comprendere gli obiettivi futuri che il Progetto si pone di raggiungere in termini di scalabilità e sicurezza. Cardano utilizza un approccio tecnico / scientifico all'applicazione della blockchain, partecipa attivamente allo sviluppo di nuove soluzioni e nuovi algoritmi per regolare i sistemi decentralizzati: esso può essere visto infatti come una piattaforma tecnologica - o anche come un contenitore di progetti blockchain-based - proponendo un'***architettura a strati*** (layers) dove le applicazioni decentralizzate rappresentano il livello più esterno, mentre la blockchain rappresenta il livello più profondo di questo sistema tecnologico. Questa configurazione porta moltissimi vantaggi nella gestione dei progetti, in quanto la manutenzione degli stessi può avvenire in maniera molto più organizzata ed efficiente, ma soprattutto permette di gestire con maggiore controllo tutte le operazioni di soft-fork che possono avvenire a livello di blockchain (ad esempio un cambio di protocollo o di policy) senza che gli strati superiori dell'applicativo

vengano direttamente coinvolti in queste operazioni, traducendosi spesso in disservizio lunghi tempi di manutenzione.

Charles Hoskinson, il fondatore di Cardano, ha voluto realizzare questo progetto in quanto essendo stato co-fondatore di Ethereum, ha potuto valutare in prima persona tutte le difficoltà che un fork di una blockchain causa verso tutti i servizi che si basano su di essa. Hoskinson definisce Ethereum una blockchain di seconda generazione, e vista l'impossibilità di evolvere in maniera agile questa struttura ha voluto realizzare da zero un progetto di terza generazione che si fondasse sui principi della filosofia scientifica e della ricerca accademica peer-reviewed.

Possiamo dire che Cardano si basa su tre requisiti fondamentali, che caratterizzano anche l'idea con cui ogni singola riga di codice è scritta dagli sviluppatori affinché vengano sempre soddisfatti:

- **Scalabilità**, grazie ad un meccanismo di consenso basato sull'algoritmo proof-of-stake Ouroboros e utilizzando nuove topologie di rete per incrementare il numero di transazioni possibili all'interno delle blockchain.

- **Interoperabilità**: utilizzare un approccio che mira a creare una sorta di "Internet delle blockchain", utilizzando le cosiddette sidechain.

- **Sostenibilità**: attraverso Patrocini e ICO.

Il team di Cardano è pienamente consapevole che applicare i concetti della decentralizzazione su sistemi economici che attualmente regolano la finanza a livello mondiale è praticamente impossibile, per questo preferisce sviluppare nuove soluzioni che possano in qualche modo "affiancarsi" alle economie attuali, ad esempio favorire dei sistemi di scambio valuta con delle fee minime sulle transazioni oppure applicare dei sistemi bancari più snelli per i paesi in via di sviluppo.

1.7.5. Supply chains e garanzia di qualità dei prodotti

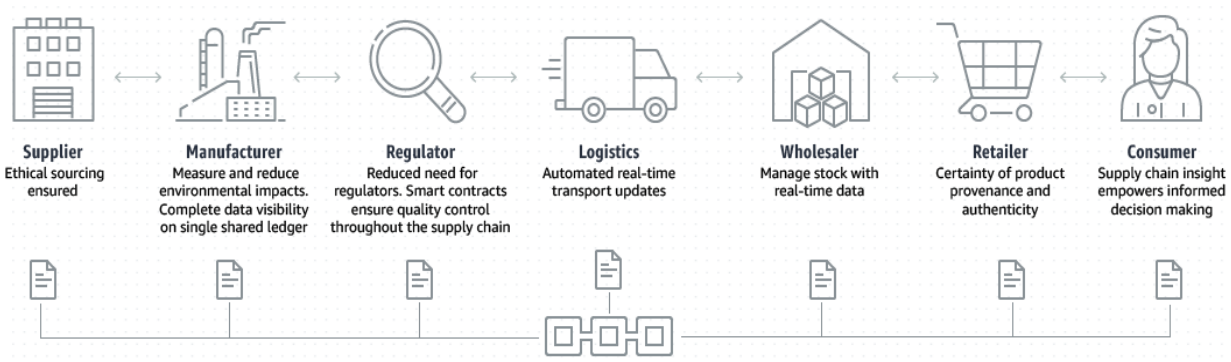
Uno dei primi progetti in cui è stata utilizzata la tecnologia Blockchain è stato sicuramente l'ambito delle Supply Chain, ovvero tutta la catena di Aziende e attori che sono coinvolti dalla realizzazione di un prodotto fino alla consegna al cliente finale. I peer di questa blockchain possono disporre di un DLT dove vengono aggiornate in tempo reale le varie transazioni e le movimentazioni della merce in modo che ogni singolo passo nella produzione e nella vendita sia tracciabile, verificabile e recuperabile nel tempo: inoltre la blockchain non fa altro che accordare la fiducia tra tutti gli attori coinvolti nel processo. Come abbiamo già avuto modo di evidenziare in altri contesti, i peer della blockchain non sono identificati solo nelle Aziende o in attori fisicamente riconducibili ad essi, ma è una cooperazione fra diverse entità tecnologiche sia fisiche che virtuali - come gli Smart Contracts, dispositivi IoT per il tracking, software di Data mining per l'analisi dell'efficienza dei processi - che contribuiscono al funzionamento dell'intera filiera. Di seguito si elencano alcuni casi di successo relative all'applicazione della blockchain in una filiera:

- Nel 2019 il Gruppo Carrefour ha pubblicizzato un progetto relativo alla tracciabilità dei polli attraverso la realizzazione della sua Food Blockchain[21]

- Google nel 2022 ha utilizzato i suoi servizi per la tracciabilità delle estrazioni minerarie[22] e ha proposto due nuove soluzioni che prendono il nome di **Supply Chain Twin** e **Pulse**[23] tra i suoi servizi web di Google Cloud Platform, i quali permettono di integrare, oltre ai dati necessari allo scambio delle transazioni tra le filiere, il recupero dei dati semi-privati degli utenti (ad esempio nel settore automotive) al fine di analizzarli e prendere nuove decisioni sulle ottimizzazioni del servizio.

- Amazon tra i suoi servizi web AWS propone il servizio Track and Trace[24] e mette a disposizione una blockchain completamente gestita per unire più reti pubbliche oppure permette di creare e gestire reti private scalabili con i framework Open Source Hyperledger Fabric o Ethereum.

[21] https://www.carrefour.com/en/group/food-transition/food-blockchain
[22] https://sustainability.google/progress/projects/blockchain/
[23] https://cloud.google.com/solutions/supply-chain-twin
[24] https://aws.amazon.com/it/blockchain/blockchain-for-supply-chain-track-and-trace/



La blockchain come base di tutte le informazioni sul percorso che porta il prodotto dalla produzione al cliente. L'immagine fa riferimento al servizio AWS Track and Trace di Amazon.

Capitolo 2 - Il Metaverso

Sebbene si è sentito parlare più frequentemente di Metaverso solo negli ultimi anni, il termine "Metaverso" è stato coniato per la prima volta da Neal Stephenson in uno dei suoi più famosi racconti del genere cyberpunk, ***Snow Crash***, pubblicato nel 1992. All'interno del romanzo il Metaverso viene descritto come un mondo non fisico raggiungibile attraverso la rete di fibre ottiche sparse per il mondo. Il protagonista Hiro, un hacker freelance in serie difficoltà economiche, si trova costretto a sbarcare il lunario effettuando consegne per *CosaNostra Pizza*, un franchise della Mafia che nel mondo del racconto è descritta come una delle più grosse corporazioni multinazionali che regolano l'economia del mondo distopico in cui è ambientato il racconto. L'attuale condizione di Hiro viene però riscattata dal suo avatar nel ***Metaverso*** - di cui egli stesso è stato uno sviluppatore del progetto - uno spazio dove vengono proiettate in maniera virtuale città, palazzi, rappresentazioni del mondo reale e dove è possibile interagire con altri esseri umani utilizzando un *headset* (visore). Stephenson nella sua opera non solo esalta gli aspetti positivi del Metaverso, ma esplora anche i lati più oscuri di questo mondo, utilizzato per le attività illecite delle organizzazioni del cybercrimine, lasciando sorgere al lettore la curiosità di vivere in un mondo virtuale correlato di grandezza e pericoli (non sembra una visione molto lontana dall'attuale World Wide Web).

Il successo di Snow Crash e dell'intero genere post-cyberpunk sta influenzando molto le idee del Metaverso come è stato concepito negli ultimi anni, a tal punto che si parla di ***iperstizione***, la tendenza che possiedono i generi letterari ad influenzare il progresso in una direzione che va verso la realizzazione di tecnologie riconducibili ai mondi rappresentati nei racconti. In ogni caso si parla sempre di spazi virtuali come una sorta di "rifugio" dal mondo distopico in cui degenerano i governi in un futuro non molto lontano. Fortunatamente l'attuale Ordine Mondiale, seppur con le grosse difficoltà e i conflitti che tengono sempre il fiato sospeso su possibili escalation che non si percepivano dalla Guerra Fredda, non ci proietta verso questo futuro molto pessimistico, e il Metaverso viene prima di tutto immaginato come uno spazio di supporto alla vita reale, con nuovi livelli di interazione tra gli esseri umani fisicamente distanti, ma virtualmente presenti (e consapevoli di esserlo).

Tra le principali aziende del settore informatico spicca ***Meta (ex Facebook inc.)*** che a partire dal 2020 ha totalmente rivoluzionato i suoi progetti aziendali in direzione dello sviluppo di un Metaverso, ma anche le altre Big Tech stanno portando avanti notevoli investimenti per la creazione di uno spazio virtuale, accessibile a tutti, nel quale sarà possibile proiettare non solo se stessi, ma anche le attività - di intrattenimento o professionali - che caratterizzano le decisioni del mondo di tutti i giorni. La sede dove si certificherà un matrimonio potrà essere una località virtuale, oppure sarà possibile acquistare un lotto di terreno virtuale dove costruire la propria residenza, oppure immaginare che si lavorerà per essere ricompensati in una valuta virtuale che ci permetterà di acquistare la proprietà di un quadro digitale, sono tutti esempi per capire cosa è possibile fare al giorno d'oggi in un "Metaverso" ancora tutto da definire e poter valutare gli impatti nel nostro mondo reale.

Se volessimo trovare un'analogia tra le tecnologie che caratterizzano oggi la nostra realtà e che hanno maggiori affinità nel Metaverso descritto nella letteratura, è evidente che Internet e il Web in generale sono le chiavi di accesso per comprendere questo nuovo mondo. Quello dello spazio cibernetico - o ***Cyberspazio*** come lo abbiamo già definito - al di là della connotazione letteraria da cui è nato è un concetto relativamente nuovo che rafforza la sua presenza con l'evoluzione tecnologica dei sistemi virtuali e di interscambio di informazioni. Originariamente ***Internet*** nacque come un progetto della Advanced Research Projects Agency (ARPA) in piena Guerra Fredda: il sistema avrebbe dovuto garantire la continuità delle operazioni tra le varie basi militari anche in caso di guerra nucleare e per questo era necessario possedere più protocolli di comunicazione che potessero lavorare in modo distribuito tra le diverse entità della rete. Si consideri che i protocolli che stanno alla base di Internet sono gli stessi, a meno di alcune ottimizzazioni, che regolavano le prime reti distribuite dell'ARPA. Il prodotto nato come un progetto di ricerca commissionato dal Dipartimento di Difesa Americano (DoD), ha fortemente rivoluzionato l'intero sistema delle relazioni sociali, sia tra Stati sia tra privati cittadini, incidendo in modo significativo soprattutto sui costi dei sistemi di comunicazione.

La rete Arpanet, dunque, si basa su un sistema di protocolli, denominati TCP/IP (Transmission Control Protocol/Internet Protocol), ancora oggi utilizzati per rendere possibile lo scambio di dati tra sistemi collegati. Una volta definiti e regolamentati i protocolli di connessione e scambio di informazioni tra due o più sistemi, risulta evidente che si può pensare adesso ad un nuovo ambiente virtuale, o spazio cibernetico, nel quale i soggetti possono interagire anche se distanti fisicamente migliaia di chilometri.

William Gibson nel suo racconto ***"Neuromancer"*** - che può essere definito come il prodotto letterario che ha dato origine al movimento cyberpunk - il Cyberspazio viene definito un' *"allucinazione consensuale…una rappresentazione grafica di dati ottenuti dai database di ogni computer nel sistema umano"*. Questa visione non si è poi distaccata molto da quello spazio che conosciamo oggi come Web, visto dal semplice punto di vista di un utente fino alle grosse corporazioni internazionali, e che potremo definire *"il sistema nervoso del paese…composto da centinaia di migliaia di computer, server, routers e fibre ottiche tra loro interconnesse e che permettono alle infrastrutture critiche di essere operative"*, così come lo ha descritto la Casa Bianca nel 2003 in un documento intitolato "National Strategy to Secure Cyberspace".

Dare una definizione e di conseguenza una regolamentazione di un qualsiasi spazio tra sistemi digitali è diventato strettamente vitale dal momento in cui, su questo dominio, avviene lo scambio di informazioni che possono essere definite critiche per tutto quello che riguarda la sicurezza e che dovrebbe essere considerato allo stesso livello dei domini "fisici" (aria, terra, mare e spazio) sui quali devono concentrarsi le difese, si pensi ad esempio ai cosiddetti SCADA (Sistemi di Controllo e Acquisizione Dati), ovvero strumenti che permettono il dialogo remoto tra le varie macchine che permettono di gestire sistemi per il controllo di impianti energetici, centrali nucleari, oleodotti che attraversano paesi geopoliticamente instabili. Anche le Nazioni Unite, infatti, hanno considerato necessario riconoscere il dominio cibernetico come *"il terreno fisico e non fisico creato da e/o composto da alcune o tutte delle seguenti proprietà: computer, sistemi di computer, network ed i relativi programmi informatici, dati di contenuto, dati di traffico e utenti"*.

2.1. Le tecnologie del Metaverso

Sviluppare concretamente un Metaverso deve far fronte non solo a delle difficoltà tecnologiche durante la fase della sua ideazione e creazione, ma deve in un certo senso prevedere il supporto alle nuove future tecnologie che caratterizzeranno il mercato nei prossimi decenni e che saranno la spina dorsale del Metaverso stesso, senza le quali l'accesso a questo mondo si ridurrebbe ad un'esperienza virtuale come tante altre che si possono benissimo provare ai giorni nostri. "Entrare" nel Metaverso potrebbe significare vivere un'esperienza dove tutti i sensi che

caratterizzano la nostra percezione del mondo reale vengono coinvolti, nasce quindi l'esigenza di sviluppare dei dispositivi sempre più immersivi, che possano replicare i nostri movimenti e che siano sempre più flessibili, leggeri e adattabili al nostro corpo. Un'altra sfida sicuramente da affrontare è relativa alla presenza sempre più crescente del numero di utenti che popoleranno il Metaverso, e per far questo le reti attuali - urbane, suburbane, professionali e domestiche - dovranno prevedere la gestione contemporanea di tipi di traffico sempre più eterogeneo, proveniente da un'utenza sempre più esigente.

Entra anche in gioco il concetto di **Digital Twin (DT)**, o Gemello Virtuale: esso non fa riferimento esclusivamente alle persone, come il nome potrebbe far pensare. Un DT è una replica digitale di una persona, di un oggetto, di un processo o di un sistema fisico, che può essere utilizzata per simulare e analizzare le caratteristiche, i comportamenti e le interazioni nel mondo reale. Può essere utilizzato per rappresentare un'ampia gamma di beni fisici, come macchine, edifici, città e persino intere catene di fornitura. Il Digital Twin viene creato utilizzando i dati dei sensori, i dati storici e altre informazioni sull'oggetto fisico e viene utilizzato per creare un modello virtuale dell'oggetto che può essere analizzato e manipolato. Esso può essere utilizzato per prevedere il comportamento dell'oggetto fisico in diverse condizioni che potrebbero non essere facilmente replicabili realmente, con l'obiettivo di identificare potenziali problemi prima che si verifichino. Può anche essere sfruttato per ottimizzare le prestazioni stesse dell'oggetto fisico, testando diverse configurazioni e scenari per migliorare efficienza e sicurezza: simulando l'oggetto fisico in un ambiente virtuale, è possibile identificare e risolvere i problemi prima che si verifichino e prendere decisioni più informate sul funzionamento e la manutenzione dell'oggetto fisico. Trattandosi di un sistema completamente digitale esso può avere moltissimi utilizzi indipendentemente dal tipo di tecnologia che si sta utilizzando, ad esempio potendo girare in tutte le direzioni, zoommare o scalare a piacimento un oggetto immersi in una realtà virtuale, o vedere in anteprima come potrebbe stare un oggetto di arredamento nella propria stanza sfruttando la realtà aumentata.

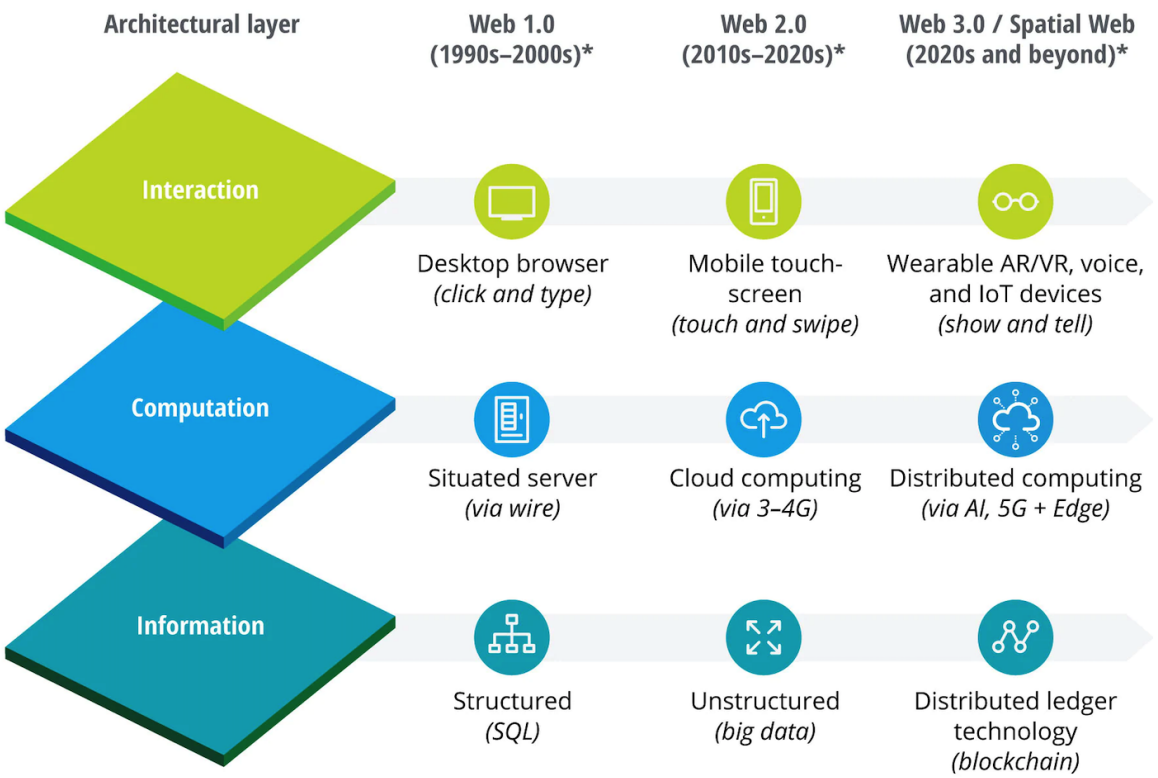
2.1.1. Web3

La terza generazione del Web (o ***Web3***), è un argomento che sta rivoluzionando il modo di concepire non solo lo sviluppo, ma anche il possesso di un sito web su Internet. Viene anche

definito in alcuni ambiti con il termine *Semantic Web*, poiché alla base di questa rivoluzionaria tecnologia c'è l'idea che qualsiasi documento presente nel web - sia esso una pagina HTML, un file di testo PDF, un'immagine o qualsiasi risorsa raggiungibile pubblicamente - venga arricchito da metadati, diventando l'input per i sempre più sofisticati algoritmi dell'intelligenza artificiale che ne permettano la ricerca, l'interpretazione e la classificazione. Ma questo non è certo l'elemento caratterizzante del nuovo scenario su cui vuole emergere questa nuova idea di Web.
Se volessimo trovare delle differenze sostanziali rispetto al web come lo conosciamo oggi e con il quale siamo quotidianamente alle prese, possiamo partire dal fatto che in Web3 i file e le risorse che lo compongono risiedono in una **struttura decentralizzata.**

Nel momento in cui si vuole pubblicare un'applicazione web - dal più semplice sito statico alle applicazioni più complesse che lavorano nei Cloud - le pagine, i dati, la logica applicativa risiedono tutti all'interno di servizi terzi verso i quali il proprietario del sito web dipende strettamente: il malfunzionamento di un servizio, o anche semplicemente il cambio di policy sulla gestione dei dati di un Datacenter per motivi geopolitici che può in qualche modo entrare in conflitto con le regole della propria organizzazione, rischiano di compromettere il funzionamento dell'applicazione e rendono necessarie delle contromisure non previste per tornare nuovamente "attivi" sul web. La soluzione di avere dei Server "in casa" inoltre, sebbene può sembrare per alcune realtà aziendali il miglior metodo per non dipendere da terzi, richiedono ingenti risorse di capitale, umano e non, per la gestione e la manutenzione delle infrastrutture così come l'organizzazione e la protezione dei dati sensibili.

Decentralizzare significa fare in modo che i componenti della propria applicazione web siano distribuiti tra i peer di una rete così che possa essere garantita la sua presenza e il suo raggiungimento in qualsiasi momento, e ovviamente alla base di questa struttura distribuita è proprio la Blockchain che può risolvere questo primo ostacolo.



Evoluzione del Web, sulla base dei 3 layers Informazione, Calcolo e Interazione. Sorgente: deloitte.com/insights

2.1.2. InterPlanetary File System (IPFS)

L'InterPlanetary File System (IPFS)[25] è un protocollo di archiviazione di file distribuito che consente agli host di archiviare e servire file come parte di una rete peer-to-peer. Nei contesti più comuni dove i Server dei siti web non hanno delle politiche di high availability (che richiedono costi molto elevati di progettazione/manutenzione), se il Server non è disponibile o si blocca, nel caso di HTTP, non saremo in grado di visualizzare le pagine web o effettuare richieste ai servizi web. Il protocollo IPFS ha lo scopo di superare queste limitazioni e i dati vengono copiati su diversi nodi della rete e sono accessibili quando necessario. IPFS può essere considerata **la spina dorsale del Web3.**

[25] https://ipfs.tech/

Così come nei più comuni protocolli peer-to-peer, se i file vengono caricati su IPFS vengono suddivisi in parti più piccole e distribuiti su più host della rete; IPFS assegna un hash alla risorsa, chiamata **Content ID (CID)** per consentire agli utenti di individuare il file. Piuttosto che indirizzare l'utente verso un luogo, i link di IPFS lo indirizzano verso il contenuto, che potrebbe essere memorizzato su un numero qualsiasi di nodi o computer in tutto il mondo. Tuttavia, finché le risorse sono ospitate da almeno un peer della rete, esse saranno sempre raggiungibili.

Il protocollo IPFS, a differenza delle risorse web attuali conservate sugli host, ha la possibilità di resistere in maniera molto più forte alle manomissioni e/o alle censure in quanto non gestisce mai la sovrascrittura delle risorse, ma ad una nuova versione del contenuto assegnerà un nuovo CID grazie alle proprietà delle funzioni di hash. Dato che le risorse vengono suddivise in blocchi più piccoli e distribuiti tra i peer, la sovrascrittura di una risorsa potrebbe ri-utilizzare i blocchi delle precedenti versioni che non hanno subito modifiche.

Anche se IFPS non è basato direttamente su blockchain, è considerato la spina dorsale del web3.

Si immagini di accedere al file dalla rete IPFS: il file, e tutti i suoi blocchi, sono identificati da un hash univoco del contenuto stesso. L'intero sistema si basa su un archivio di dati di tipo chiave-valore: è proprio questa caratteristica che consente l'indirizzamento dei contenuti, infatti chiunque può ospitare la chiave, indipendentemente dall'origine delle informazioni. Quindi, ci si connette allo sciame e si richiede alla rete quel file: per prima cosa si cercherà tra i peer più vicini all'utente, perché è probabile che abbiano una copia di quel file. Se invece non ce l'hanno, ci si connette al nodo che ha caricato originariamente il file, poiché è lui ad ospitarlo.

IPFS può essere visto come l'interazione di uno o più componenti[26], per i quali si danno alcuni dettagli:

- **IPNS (InterPlanetary Name System):** può essere paragonato in un certo senso al servizio DNS dell'attuale Internet, e come il nome fa intendere non è altro che il sistema che ha il compito di mappare un nome (*mutabile)* al nome di una risorsa (*immutabile)* dell'IPFS. In pratica i record dell'IPNS non sono altro che puntatori al puntatore del Content ID della risorsa che si vuole identificare. Questo permette di gestire in maniera più friendly i percorsi globali alla risorsa, e soprattutto è utile nel caso in cui si vuole

[26] https://docs.ipfs.tech/concepts/ipns/#how-ipns-works

puntare ad una risorsa che nel tempo avanza di versionamenti, in questo modo non è necessario aggiornare a livello applicativo tutti i percorsi che puntano a quella risorsa attraverso l'IPFS, ma sarà solo necessario cambiare il record IPNS all'ultima versione più recente. I nomi del record sono auto-certificanti: un record IPNS contiene tutte le informazioni necessarie a certificarne l'autenticità attraverso coppie di chiavi pubbliche e private: la natura auto-certificante dei record IPNS fa sì inoltre che i record non sono legati ad un protocollo di trasporto specifico, la maggior parte delle implementazioni IPFS si affida al DHT e a libp2p PubSub per pubblicare e risolvere i record IPNS.

- **Distributed Hash Tables (DHT):** corrisponde al componente di IPFS che gestisce il routing delle risorse. È un sistema di tipo chiave-valore e il suo compito è mappare ciò che l'utente sta ricercando con il rispettivo peer che ha memorizzato il contenuto. In DHT esistono tre tipi di record che possono essere conservati e vengono descritti nella tabella successiva.

Tipo	**Scopo**	**Usato da:**
Provider records	Mappa un identificatore di contenuti (ad esempio, un multihash) a un peer che ha annunciato di possedere quel contenuto e di essere disposto a fornirlo all'utente.	- IPFS per trovare i contenuti. - IPNS over PubSub per trovare altri membri pubsub
IPNS records	Mappa una chiave IPNS (per esempio l'hash di una chiave pubblica) ad un record IPNS (per esempio un puntatore firmato e verificato ad un percorso /ipfs/abcdefg...)	- IPNS
Peer records	Mappa un peer ID ad un insieme di indirizzi multipli che possono essere raggiunti dal Peer	- IPFS: quando si sa che il peer possiede contenuti, ma non conosciamo il suo indirizzo. - Connessioni manuali (per esempio ipfs swarm connect /p2p/Qmxyz...)

- **Bitswap**: è il modulo centrale di IPFS e definisce le regole per lo scambio dei blocchi delle risorse tra il peer richiedente, e i peer che possiedono le varie parti delle risorse.

Bitswap è un protocollo basato su messaggi in cui tutti i messaggi possono contenere due tipologie di informazioni:

  - liste di richieste dei contenuti (Want List)
  - contenuto dei blocchi da restituire al client richiedente

Una volta che sono stati identificati i peer che possiedono le risorse specificate nella Want List, questi peer inviano il blocco al client, nel caso in cui nessuno dei peer risponde per il mancato possesso del blocco radice (root block), Bitswap interroga la Distributed Hash Table (DHT) per ricercare i peer che sono in possesso di questa informazione e poter completare la richiesta.

- **DNSLink**: Un indirizzo DNSLink è simile a un indirizzo IPNS, ma utilizza un nome DNS al posto della chiave pubblica con hash. Proprio come i normali indirizzi IPFS, possono includere collegamenti ad altri file o ad altri tipi di risorse supportate da IPFS, come directory e symlink. Un esempio che potremmo trovare come record TXT di una zona DNS, in cui un sotto-dominio è mappato ad una risorsa dell'IPFS potrebbe essere il seguente:

_dnslink.docs.ipfs.tech.	*3600*	*IN*	*TXT*	*"dnslink=/ipfs/QmVMxjouRQCASA2HDGUBG"*

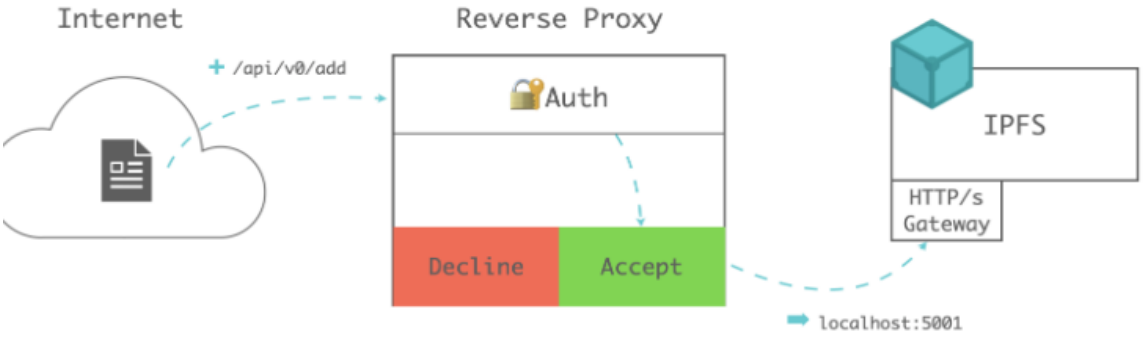
A questo punto se provassimo a raggiungere il dominio docs.ipfs.tech sarà restituito il contenuto della risorsa IPFS avente come Content ID: QmVMxjouRQCASA2HDGUBG. È proprio il protocollo IPFS a ricercare prima nel DNS dei record TXT che soddisfino la risoluzione del dominio in una risorsa IPFS o IPNS e restituire la corretta destinazione.

- **File systems**: Poiché i file in IPFS sono indirizzati al contenuto e per natura immutabili, la loro modifica può essere complicata. ***Mutable File System (MFS)*** è uno strumento incorporato in IPFS che consente di trattare i file come se fossero un normale file system basato sui nomi: è possibile aggiungere, rimuovere, spostare e modificare i file MFS e occuparsi dell'aggiornamento dei collegamenti e degli hash. **UnixFS**[27] invece è un formato basato su protocol-buffer per descrivere file, directory e collegamenti simbolici in IPFS. L'attuale implementazione di UnixFS è cresciuta organicamente e non ha un

[27] https://github.com/ipfs/specs/blob/main/UNIXFS.md

documento di specifica chiaro. Il lavoro di bozza e la discussione su una specifica per la prossima versione 2 del formato UnixFS sono attualmente in corso.

- **IPFS Gateway**: i gateway IPFS forniscono un servizio basato su HTTP che consente ai browser e agli strumenti che non conoscono - ancora - i protocolli IPFS di accedere al contenuto di IPFS, che altrimenti non sarebbe possibile recuperare. Possono essere visti a tutti gli effetti come dei Reverse Proxy, che si trovano davanti ai servizi IPFS per inoltrare loro le richieste sulla risorsa trovata. per questo motivo possono distinguersi, ad esempio, Gateway di tipo Read Only che impediscono altre operazioni diverse dal recupero (metodo GET) delle risorse, oppure Authenticated Gateways che forniscono gli accessi solo ad utenti che riescono ad autenticarsi prima al Proxy e rendere private le risorse all'interno dell'IPFS.



Schema che descrive un Authenticated Gateway, con accesso protetto alle risorse IPFS[28].

- **IPLD (InterPlanetaryLinkedData)**[29]**:** IPLD è una serie di standard e formati per descrivere i dati e rappresenta il Data Layer di IPFS. IPLD si basa su un concetto chiamato *Content Addressing*[30], che in realtà abbiamo già accennato agli inizi di questo paragrafo quando abbiamo enunciato che un documento in IPFS è identificato univocamente da un Content ID, e il Content Addressing non è altro che la capacità di risalire al documento dal suo ID. Oltre a garantire che i file non vadano persi in caso di spostamento, il Content Addressing assicura anche che gli utenti che intendono

[28] https://docs.ipfs.tech/concepts/ipfs-gateway/
[29] https://ipld.io/docs/intro/primer/
[30] https://web3.storage/docs/concepts/content-addressing/

recuperare una versione specifica di un file avranno la garanzia di poterla recuperare finché esisterà in qualsiasi punto della rete. IPLD utilizza un modello di dati sottostante che contiene forme come stringhe, booleani, ints, float, ecc. Per arrivare alla generazione di un CID, si utilizzano i **codec**: il CID include un indicatore chiamato *multicodec* per informare su quale codec utilizzare per il documento.

La maggior parte degli sviluppatori ha familiarità con sistemi di rappresentazione dei dati semplici come JSON o CBOR[31]: in entrambi i casi è possibile rappresentare e recuperare diverse strutture di dati utilizzando questi sistemi. Tuttavia, nessuno di questi semplici sistemi di rappresentazione dei dati mancano del supporto **ai collegamenti tra documenti diversi**: gli utenti attraverso IPLD possono memorizzare i dati utilizzando versioni estese di questi sistemi semplici. **DAG-JSON** consente di memorizzare i tipici dati serializzati JSON, ma supporta anche i collegamenti che possono essere utilizzati insieme a IPLD. **DAG-CBOR** consente una flessibilità ancora maggiore. CBOR è un sistema di archiviazione binario che lo rende veloce ed efficiente. Filecoin[32], ad esempio, utilizza CBOR per la sua catena per la sua efficienza e perché CBOR può gestire più tipi di dati rispetto a JSON.

- **Libp2p[33]**: è l'abbreviazione di "library peer-to-peer" è un framework per reti peer-to-peer che consente lo sviluppo di applicazioni P2P. Consiste in una raccolta di protocolli, specifiche e librerie che facilitano la comunicazione P2P tra i partecipanti alla rete, i *peers* appunto. Libp2p si distingue per l'enorme sforzo fatto dagli sviluppatori per creare una libreria che potesse diventare un punto di riferimento tra i vari protocolli e applicativi basati su reti peer-to-peer come ad esempio eMule, Kademlia, Gnutella, tutti in competizione tra loro. Lo sviluppo della libreria per il supporto alla maggior parte dei linguaggi di programmazione e con l'obiettivo di fornire un prodotto multi-platform è un lavoro molto attivo che la Community di Libp2p porta avanti, supportato da IPFS come uno dei maggiori partner del progetto.

[31] https://cbor.io/
[32] https://filecoin.io/
[33] https://libp2p.io/

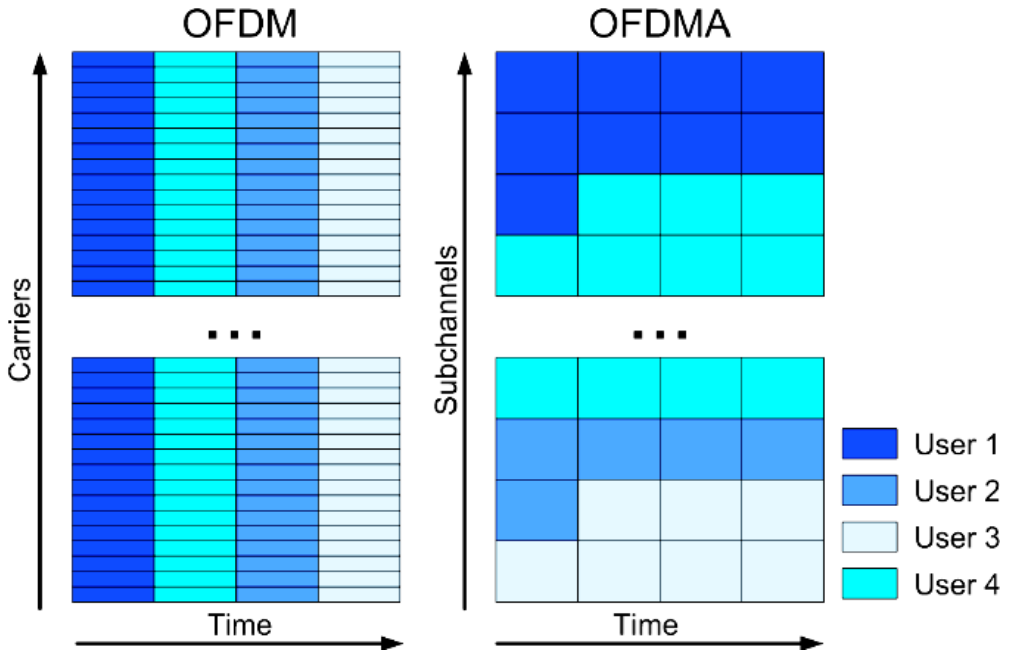
2.1.3. Lo standard IEEE 802.11ax (Wi-Fi 6)

Le prestazioni di rete, che siano esse professionali o domestiche, sono diventate un requisito critico per l'utente che naviga su Internet e ci si aspetta di trovare non solo una connessione in qualsiasi punto ci si trovi, ma che questa sia anche veloce e affidabile. Con gli ultimi avvenimenti relativi alla pandemia, inoltre, questa necessità è diventata ancora più importante dato dal fatto che spesso le attività professionali in smart working, le attività educative o di intrattenimento devono essere soddisfatte contemporaneamente per più utenti. L'elevato numero di dispositivi mobili e IoT costantemente connessi ai punti di accesso richiedono anche che la rete Wireless sappia reagire con efficienza alle congestioni e ai tipi di QoS richiesti dai sempre più diversi tipi di traffico che viaggiano nella rete.

Per superare i problemi più comuni a cui le reti WiFi sono soggette si è cercato di cambiare completamente il tipo di approccio a queste problematiche, in quanto lo standard attuale 802.11ac ha sempre avuto come obiettivo quello di garantire il massimo rate in condizioni di picco. Spostando invece il requisito principale dalla velocità massima al throughput - e quindi poter garantire che la rete soddisfi contemporaneamente i requisiti di banda degli utenti connessi all'access point - diventa l'obiettivo principale della Wi-Fi Alliance che, in collaborazione con l'Institute of Electrical and Electronics Engineers (IEEE), ha rilasciato nel 2018 un nuovo standard chiamato **802.11ax**, più comunemente chiamato in ambito business **Wi- Fi 6.**

Questo nuovo standard vuole rispondere con efficienza alle sempre più eterogenee applicazioni in termini di banda e alla sempre più variabile densità di dispositivi che occupano l'area di un Access Point: la capacità di throughput viene aumentata fino a quattro volte rispetto allo standard 802.11ac. Tra i tanti vantaggi vi è anche la possibilità di sfruttare le bande a 2,4 gigahertz (GHz) e 5 GHz.

Una delle principali modifiche dello standard che lo differenziano dal precedente corrisponde ad una innovativa allocazione delle frequenze in ambito multi-utente, questo tipo di accesso prende il nome di **OFDMA (Orthogonal Frequency Division Multiple Access).** Gli Access Points che implementano OFDMA, in base al tipo di traffico presente in un determinato momento, sono in grado di allocare l'intero canale ad un singolo utente oppure ripartirlo in sottocanali per poter servire più utenti contemporaneamente, riducendo la latenza e aumentando l'efficienza nell'utilizzo del servizio per tutti gli utenti connessi.

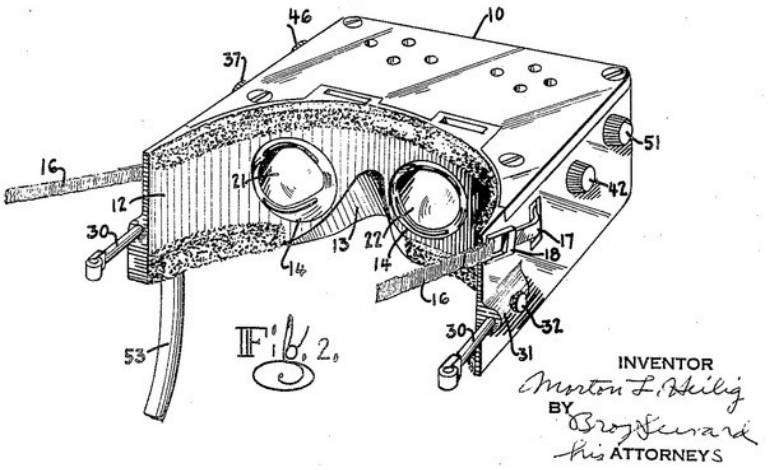


OFDMA, attraverso il riutilizzo più ottimizzato delle frequenze, si adatta molto bene alle applicazioni più comuni che richiedono un consumo di banda contenuto come il trasferimento della voce, ma reagisce con molta più efficienza ai tipi di traffico più intensi - come ad esempio il trasferimento video in HD - che potrebbero presentarsi su più dispositivi contemporaneamente. Per far questo 802.11ax ha apportato notevoli miglioramenti alla tecnologia **Multi-user Multiple Input/Multiple Output (MU-MIMO)** che era stata implementata originariamente nello standard 802.11ac, portando la capacità di trasmissione simultanea da 4 a 8 dispositivi, utilizzando un canale dedicato per ognuno di essi. La tecnologia MU-MIMO ultimamente sviluppata può anche operare su frequenze a 2,4GHz oltre a quelle 5GHz con le quali era stata inizialmente sviluppata.

MU-MIMO purtroppo ha uno svantaggio: per poter operare pienamente, sia il router che i dispositivi ad esso connessi devono implementare questa tecnologia. L'evoluzione dei dispositivi mobili ha fatto sì che moltissimi device come gli smartphone e i tablet di ultima generazione implementino MU-MIMO, ma la variegata presenza nel mercato di dispositivi mobili obsoleti o che ancora non implementano il nuovo standard Wi-Fi 6 non permette ancora di sfruttare al massimo le capacità di questo nuovo standard.

2.1.4. Virtual Reality (VR) e dispositivi

Con il termine ***Virtual Reality*** (o VR abbreviato), si intende uno spazio generato tramite dispositivi informatici che si estende nelle tre dimensioni, così come nello spazio reale. L'immersione in uno spazio VR e l'interazione con gli oggetti in esso presenti può avvenire con un coinvolgimento parziale o totale dei sensi attraverso dei dispositivi che nel tempo sono diventati sempre più sofisticati. La vista è stato il primo organo sensoriale ad aver decretato la nascita della VR, con lo sviluppo dei **visori**.



HMD, tra i primi prototipi di visori ideati da M. L. Heiling (da The VR Book: Human-Centered Design for Virtual Reality, di J.Jerald)

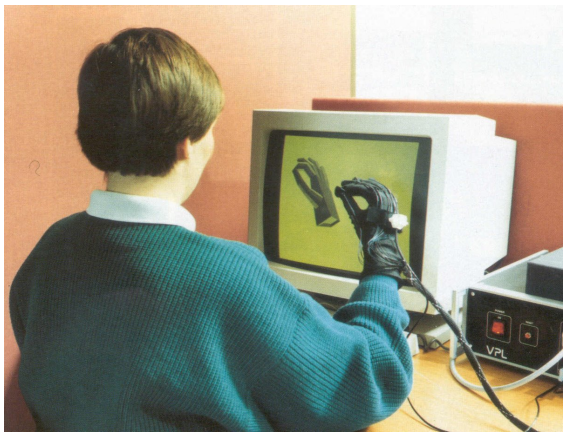
Morton Leonard Heilig, un inventore statunitense che ha lavorato nello sviluppo di innovativi dispositivi cinematografici, è stato sicuramente il pioniere della VR attraverso l'ideazione nel 1957 di una macchina chiamata **Sensorama**, molto simile ad un cabinato di una sala giochi davanti al quale un utente poteva prendere posto su un sedile mobile per simulare l'ondeggiamento dei movimenti e poteva visualizzare delle immagini - attraverso l'utilizzo delle tecniche stereoscopiche - mentre l'esperienza sensoriale veniva arricchita da specifiche periferiche di output che permettevano ad esempio di sentire il vento sul viso o addirittura percepire gli odori.

Sebbene Sensorama non abbia mai trovato un interesse reale di sviluppo, ha dato il via a nuove idee per ridurre il divario tra spazio reale e virtuale. Sempre ad Heiling è da attribuire la

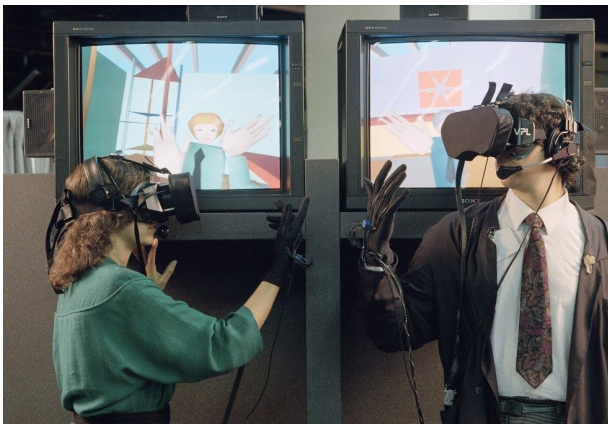
prototipazione della forma dei visori come li conosciamo oggi, infatti sempre negli anni '50, ha ideato una "scatola" chiamata **Head Mounted Display (HMD)**, che proprio come suggerisce il termine veniva posta sulla testa dell'utilizzatore in modo che la sua vista potesse immergersi nelle immagini proiettate all'interno del dispositivo.

Nel 1965 Ivan Sutherland, un inventore e ricercatore statunitense, ideò **Ultimate Display**, un dispositivo simile al visore HMD con la differenza che le immagini proiettate erano generate da un computer. Solo tre anni dopo Sutherland riuscì a realizzare concretamente questo prototipo di visore VR con la creazione di **Sword of Damocles**: l'apparato permetteva di navigare in uno spazio virtuale limitato da muri in wireframe e l'orientamento dell'utente veniva simulato attraverso dei complessi sistemi di tracciamento del capo. Sebbene questa invenzione può essere vista come un primissimo esempio di dispositivo VR, la generazione dello spazio virtuale avveniva attraverso la connessione ad un computer sospeso sopra la testa dell'utilizzatore proprio come una spada di Damocle. Date le dimensioni dei computer di quel tempo la mobilità stessa dell'utente era piuttosto limitata.

Occorre spostarsi di circa due decenni più avanti per trovare sul mercato i primi dispositivi videoludici che iniziano a rendere la realtà virtuale parte integrante del settore dell'intrattenimento. Infatti nel 1984 la Atari, una delle più grosse aziende impegnate nella creazione di console e videogiochi di quel periodo, si divide in due diverse compagnie: da questa scissione **Jaron Larnier** perde il proprio posto di lavoro in Atari ma, insieme al suo collaboratore **Thomas Zimmerman**, riesce a fondare tre anni più avanti la *"VPL Research"* e riesce a produrre due storici dispositivi, i ***Data Gloves*** e gli ***Eye Phones.*** I primi sono dei guanti composti da migliaia di microchip e da una rete di fibre ottiche che permetteva agli utilizzatori di riprodurre i movimenti del braccio e della mano all'interno dello spazio virtuale, riuscendo così a manipolare gli oggetti. I secondi invece riprendono il concetto del Sword of Damocles di Sutherland, ma grazie alle evoluzioni tecnologiche dei componenti elettronici riescono a "miniaturizzare" il dispositivo riducendolo ad un casco meno ingombrante e che lasciava il capo libero nei movimenti a 360 gradi. L' utilizzo della tecnologia delle lenti di Fresnel all'interno del dispositivo, inoltre, ha contribuito ulteriormente alla riduzione del peso dell'oggetto.



Il DataGloves



Utilizzo degli EyePhones, insieme al DataGloves (AP Photo/Jeff Reinking)

Jaron Larnier può essere sicuramente ricordato come il padre della realtà virtuale, in quanto, oltre ad aver realizzato i primi dispositivi elettronici che avvicinavano concretamente i due mondi, è stato colui che ha coniato per la prima volta il termine "Virtual Reality". In ogni caso gli anni '80 hanno visto lo sviluppo di altri progetti pionieristici della realtà virtuale come ad esempio il *Virtual Interface Environment Workstation (VIEW)* della NASA, o il *PowerGlove* della Nintendo.

Il decennio successivo vede soprattutto fallimenti di progetti che avrebbero dovuto garantire dei successi commerciali in larga scala, e i protagonisti sono sempre da ritrovarsi nel settore videoludico come Nintendo con il suo *Virtual Boy*, invece iniziano a delinearsi alcuni interessanti progetti - soprattutto qui in Italia rivolti verso nuove forme d'arte[34] - il cui obiettivo non è immergersi necessariamente in un mondo virtuale attraverso visori o altre interfacce, ma utilizzare tecnologie come telecamere che riprendono esternamente la propria immagine per vederla poi proiettata in un mondo virtuale: il concetto di esperienza in prima persona viene meno, ma comincia a delinearsi un tipo diverso di realtà (*aumentata*) che sarà approfondito nel sottocapitolo successivo.

Il nuovo millennio è caratterizzato da una forte spinta verso la tecnologia dei visori e delle esperienze in prima persona, si prenda ad esempio Google, che con *Street View* nel 2007 ha permesso a chiunque di viaggiare per le strade di quasi tutto il mondo, e il rilascio tre anni dopo di una modalità 3d stereoscopica dello stesso applicativo. Sicuramente di grande interesse

[34] P.Lagonigro, La realtà virtuale nell'Italia dei primi anni Novanta, ISSN 2531-9876

ricopre il progetto Oculus Rift, un visore ideato da un ragazzo di 18 anni, Palmer Luckey, che sfruttava la potenza dei processori di un pc per poter elaborare le immagini del mondo virtuale: tra le altre caratteristiche era presente una visuale a 90° mai sperimentata fino ad ora.

Mark Zuckerberg presenta una demo di Oculus Rift e Oculus Touch durante l'evento Oculus Connect 3 a San Jose, California, U.S., on Thursday, Oct. 6, 2016. Bloomberg—Bloomberg (fonte Getty Images)

Il prototipo di Oculus Rift su Kickstarter ha suscitato un notevole interesse ed è stato acquistato nel 2014 da Mark Zuckerberg, CEO di Facebook (ora Meta), alla cifra di 2 miliardi di Dollari americani e ne ha proposto una commercializzazione in larga scala. Nello stesso anno però le più grandi aziende nel settore Tech hanno cominciato a proporre sul mercato i loro progetti, si pensi a Samsung con il suo Gear VR - da utilizzare insieme allo smartphone Samsung Galaxy da cui vengono proiettate le immagini - o al prototipo Morpheus di Sony.

2.1.5. Augmented Reality e AR Cloud

Con il termine ***Realtà Aumentata*** (Augmented reality o *AR* abbreviato) si identifica un tipo di tecnologia in cui le rappresentazioni dei dati virtuali si "sovrappongono" letteralmente all'ambiente reale che circonda l'utente, in modo da aumentare le possibilità di interazione in un modo completamente diverso rispetto alla semplice navigazione di una pagina web da browser.

Le origini della AR vengono in qualche modo confuse con le origini della realtà virtuale, in realtà la distinzione è abbastanza netta in quanto i primi prototipi di visore come la "Spada di Damocle" avevano l'obiettivo di proiettare la percezione dell'utente in uno spazio completamente virtuale, l'obiettivo non era certo di far coesistere elementi virtuali in ambienti della realtà. Il nome Augmented Reality viene dato nel 1990 da Tom Caudell e David Mizzel, due ingegneri della Boeing, che durante la venticinquesima edizione della Hawaii International Conference on System Science presentano la documentazione di un progetto - che non ha mai avuto una vera e propria realizzazione - grazie al quale gli operai degli aerei avrebbero potuto indossare un visore che dava loro la possibilità di vedere come dovevano essere posizionati i cavi all'interno della struttura dell'aereo, facilitandone così il montaggio e le successive verifiche.

Nel 1992 Louis B. Rosenberg ha sviluppato per la US Air Force una piattaforma chiamata **Virtual Fixtures**, un sistema di realtà aumentata immersiva che guidava l'utente nei suoi compiti con istruzioni a schermo. Virtual Fixtures utilizzava due robot fisici reali, controllati da un esoscheletro completo sulla parte superiore del corpo indossato dall'utente. Per creare un'esperienza immersiva per l'utente, è stata impiegata una configurazione ottica unica che prevedeva un paio di ingranditori binoculari allineati in modo che la vista dell'utente sulle braccia del robot fosse portata in avanti per apparire registrata nell'esatta posizione delle braccia fisiche reali dell'utente. Sovrapposizioni virtuali generate dal computer sotto forma di barriere fisiche, campi e guide simulate, progettate per assistere l'utente durante l'esecuzione di compiti fisici reali.

Solo nel 1999 la realtà aumentata si presenta con dei progetti più commerciali con il primo kit per la realtà aumentata della storia, **l'ARToolKit** di Hirokazu Kato dell'Istituto di Scienza e Tecnologia di Nara. È stato il primo software di realtà aumentata per mobile su Symbian nel 2005, per iOS nel 2008 e per Android nel 2010.

Nel corso degli anni sono stati sviluppati numerosi progetti con lo scopo di modificare la realtà in cui viviamo aggiungendo elementi che vanno oltre la capacità percettiva del nostro sistema sensoriale, e dimostrano come l'integrazione tra reale e virtuale diventa sempre più realizzabile.

Di seguito si riportano alcuni di questi progetti maggiormente conosciuti e riconosciuti in ambito AR:

- **Google Glass (progetto interrotto):** è un progetto di Google X reso pubblico nel 2013 e consiste in un visore a forma di occhiali da vista (chiamato appunto Smart Glasses) e si pone l'obiettivo di applicare la Realtà Aumentata nella vita di tutti i giorni. Google Glass è un progetto con una fase di sviluppo costante, ma quello che sappiamo è che dovrebbe permettere di avere davanti agli occhi tutte le informazioni che, per ora, sono accessibili solo tramite smartphone. Google Glass sembra essere uno strumento che ancora solo pochi curiosi acquistano sul mercato a partire dal 2019 ed è stato più che altro tenuto in considerazione dalla casa madre verso ambienti Enterprise. Alcuni problemi che sicuramente hanno riguardato la sua regolamentazione riguardano in particolare la privacy degli utilizzatori degli smart glasses, in quanto non ci sono ancora vere e proprie specifiche o soluzioni che permettono di capire quando e cosa gli occhiali stanno registrando. Google, il 15 marzo del 2023 ha interrotto le vendite anche per il settore enterprise e cesserà completamente il supporto a Settembre dello stesso anno, il progetto resterà con le funzionalità al momento della chiusura e non sarà garantito alcun supporto o manutenzione.

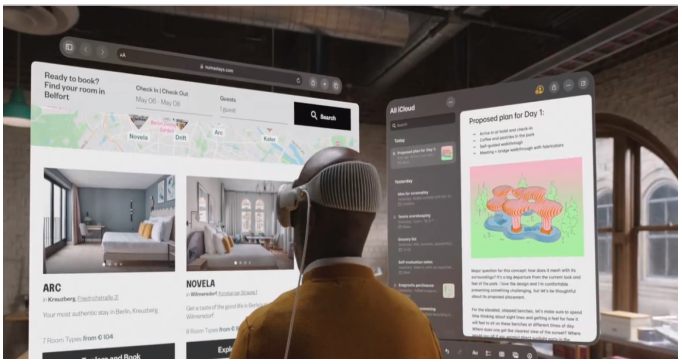
- **Live View AR:** Nonostante Google Glass non sia ancora diventata una realtà affermata, Google è riuscita comunque a sviluppare e rendere pubblica una funzione speciale che introduce la Realtà Aumentata nella vita di tutti i giorni: Live View AR. Esso è correlato al servizio internet Google Maps, che permette agli utilizzatori attraverso la modalità Street View, di visualizzare

immagini 3D che indicano la strada da intraprendere per raggiungere a piedi la destinazione selezionata. Per accedere a questa nuova funzione gli utenti devono utilizzare un dispositivo mobile dotato di fotocamera e GPS.

- **Pokémon Go**: è un videogioco del 2016 che trova le sue basi nella Realtà Aumentata geolocalizzata. Scaricando l'app dallo Store del proprio smartphone, gli appassionati del gioco di carte Pokémon possono andare loro stessi alla ricerca dei famosi mostri tascabili. La forza di questo progetto risiede nel fatto che i luoghi dove possono trovarsi le creature da catturare sono reali: una palestra, un parco, una spiaggia, una chiesa…

- **IKEA Place:** Nel mese di Ottobre del 2017 IKEA ha annunciato il lancio della sua nuova app: IKEA Place. Con questa mossa l'azienda ha portato la sua Customer Experience a livelli estremamente elevati garantendo a tutti i suoi Clienti un'esperienza unica nella scelta del mobilio per la propria casa. Questa Applicazione gratuita, inizialmente disponibile solo per iOS e poi anche per Android, permette a chi la scarica di effettuare una simulazione di arredamento. Puntando la telecamera del proprio Smartphone o Tablet verso il luogo dove si vorrebbero inserire i nuovi mobili IKEA, l'app aiuterà gli utenti nella scelta proiettando digitalmente il risultato finale.

- **Apple Vision Pro:** durante la Worldwide Developers Conference (WWDC) di Apple del 2023 è stato presentato dalla casa madre un nuovo dispositivo che con molta probabilità sconvolgerà il mercato dei prodotti di ***realtà mista***: si tratta dell'Apple Vision Pro, un visore - o meglio definirlo uno "spatial computer" - controllato da mani, occhi e voce dell'utente che permette di operare sul proprio Sistema Operativo *visionOS* in un environment composto dall'ambiente reale circostante e da un overlay virtuale i cui elementi - app, finestre, note, ecc.. - interagiscono completamente nello



spazio circostante in una visuale a 360°. La potenza di calcolo di questo dispositivo è contenuta in un involucro dalle dimensioni non eccessivamente grandi e la parte frontale è costituita da un unico pezzo di vetro tridimensionale che avvolge completamente il campo visivo dell'utente con tecnologie per eliminare la luce diffusa. Il visore rimane saldo sul volto dell'utente grazie ad una fascia elastica e regolabile sulla quale si saldano ai lati della stessa degli auricolari per garantire una migliore diffusione del suono. Vision Pro diventerà un dispositivo utilizzabile singolarmente o integrabile con i dispositivi Apple, l'anteprima ha presentato delle funzionalità veramente interessanti come il trascinamento della finestra di un'applicazione da un Macbook in uno spazio all'interno della propria stanza, per proseguire l'interazione sul visore, oppure la presentazione nel display esterno del visore della ricostruzione in tre dimensioni dei propri occhi per permettere alle persone di capire se si è impegnati in alcune attività sul visore. Il dispositivo, quando entrerà nel mercato, è pensato inizialmente per la vendita al pubblico con un prezzo non indifferente - circa 3500 dollari - ma di certo Apple non ha mai impressionato sul prezzo dei propri prodotti, mettendo sempre al primo posto la qualità e la piena interoperabilità di tutto il mondo di Apple per ritagliarsi sempre una parte importante di mercato nei settori tecnologici di ultima generazione.

2.2. Proto-Metaverso: evoluzione dei Videogames

Molto spesso si sente parlare di Metaverso in relazione ai videogames. Come mai? Perchè in realtà si è visto che molte idee che caratterizzano il Metaverso sono state in qualche modo anticipate dall'evoluzione dei videogiochi, così come le difficoltà di sviluppo che i creatori di videogiochi hanno dovuto affrontare durante gli sviluppi di giochi online: le compagnie che sviluppano videogames sono stati sempre all'avanguardia sulle tecnologie che sono poi gli elementi fondamentali del Metaverso stesso, ad esempio la grafica e la fisica in 3D, il multiplayer, ambienti totalmente virtuali i cui server devono garantire la gestione di sessioni di gioco in tempo reale anche con migliaia di utenti.

Lo sviluppo di un gioco multiplayer in rete porta delle complessità tecniche veramente notevoli, nel quale tutto deve accadere in modo tale che l'esperienza dei giocatori sia "unica" per tutti: si pensi a quei giochi dove gli utenti sono immersi in uno spazio virtuale di guerra simulata - uno

dei più famosi è *Call of Duty* di Activision - e posso utilizzare delle armi per distruggere elementi del gioco o far perdere gli altri giocatori, cosa succede se un utente distrugge un edificio e questo crollando coinvolge dei giocatori che mentre corrono verso un altro punto si ritrovano sotto le macerie? Magari pensarlo è molto semplice, ma tecnicamente parlando ci si può chiedere chi deve gestire queste logiche causa-effetto all'interno del gioco? Potrebbe farlo il game server, ma si presuppone che possa ottenere l'aggiornamento delle coordinate dei giocatori nel giro di alcuni millisecondi: se un giocatore dovesse avere una connessione più lenta teoricamente potrebbe essere teletrasportato da un punto ad un altro nell'esperienza di gioco evitando così di essere coinvolto nel crollo dell'edificio. Oppure il server potrebbe gestire la fisica dell'evento del crollo, comunicare gli effetti dei vari elementi 3D ad ogni singolo giocatore e sarà poi il gioco client di ogni singolo player ad elaborare gli effetti, ma ovviamente se non esiste la massima "sincronizzazione" tra gli eventi fisici per qualcuno potrebbe morire, per qualcun altro potrebbe invece sopravvivere al crollo, chi decide l'esito dei giocatori?

L'Idea di gestire la presenza di se stessi come Avatar porta anche a riflettere se l'elaborazione delle future applicazioni del Metaverso può essere demandata totalmente a macchine virtuali in un ambiente cloud - si veda ad esempio PlayStation con i suoi servizi Network e Plus - che danno la possibilità di giocare collegandosi ad un server online, senza sfruttare la potenza computazionale della propria console: teoricamente potremmo proiettarci in mondi virtuali computazionalmente impossibili da realizzare con le proprie console, che potrebbero essere evolute in periferiche per gestire sempre meglio gli input e gli output fisici, ed è il server remoto in cloud invece a fare il lavoro sporco con la gestione della fisica e il rendering dello spazio.

Di seguito si presenteranno alcune piattaforme non basate su Blockchain ma che sono stati definiti dei Proto-Metaversi (o Beta-Metaversi), avendo dimostrato come l'interazione sociale all'interno di un videogame acquisisce sempre di più un interesse commerciale che spinge le Big Tech a investire su questo mercato.

2.2.1. Second-life

Second Life è una piattaforma di mondo virtuale lanciata nel 2003 da Linden Lab, permette agli utenti di creare Avatar, esplorare ambienti virtuali e interagire con altri utenti in vari modi e mondi: gli utenti possono acquistare o affittare terreni virtuali, costruire case e attività commerciali e partecipare a una vasta gamma di attività, tra cui la socializzazione, il gioco e il commercio. I creatori della Linden Lab si premurano di sottolineare che Second Life non deve essere considerato un gioco con obiettivi da raggiungere o sfide da superare (a differenza di fortnite o Roblox, che vedremo nei paragrafi successivi). Si potrebbe definire uno dei primi esempi di Proto-Metaverso, in quanto permette agli utenti di creare ed esplorare spazi virtuali e di interagire con gli altri in una vasta gamma di attività, seppur la grafica non è certamente la più recente. Tuttavia, è importante notare che Second Life non è così avanzato come le piattaforme Metaverse più recenti e manca di alcune delle caratteristiche e delle capacità di queste ultime: Second Life è un sistema chiuso e non uno standard aperto come le piattaforme Metaverse. Pur avendo avuto il suo maggior successo all'inizio degli anni 2000, Second Life ha ancora un gruppo dedicato di utenti regolari (circa novecentomila) ed è probabilmente l'esperimento più longevo sulle possibilità di un'esperienza simile a un Metaverso.

L'economia virtuale di Second Life è anche una delle sue caratteristiche, in cui gli utenti possono acquistare e vendere beni virtuali e valuta. Gli utenti di Second Life, noti come "residenti", possono pagare denaro reale (ad esempio dollari statunitensi) per acquistare **Dollari Linden (L$)**: questi possono essere utilizzati per acquistare, vendere, affittare o scambiare terreni virtuali, beni digitali e servizi online. I Dollari Linden possono anche essere riconvertiti con dollari statunitensi in base a un tasso di cambio variabile. Tuttavia, Linden Lab non permette a questa valuta di diventare una vera e propria moneta a corso fisso o addirittura una criptovaluta.

Esistono esempi concreti di semplici utenti di Second Life che hanno accumulato grandi fortune operando nell'economia dei mondi virtuali. Un esempio molto noto è quello di Anshe Chung, un avatar di Second Life di una persona reale che, attraverso l'avatar Anshe Chung, ha avviato un'attività immobiliare virtuale in piena espansione all'interno di Second Life. A partire da un investimento iniziale di 9,95$ per un account Second Life da parte della creatrice di Anshe, Ailin Graef, Anshe ha raggiunto la sua fortuna iniziando con acquisti su piccola scala di proprietà

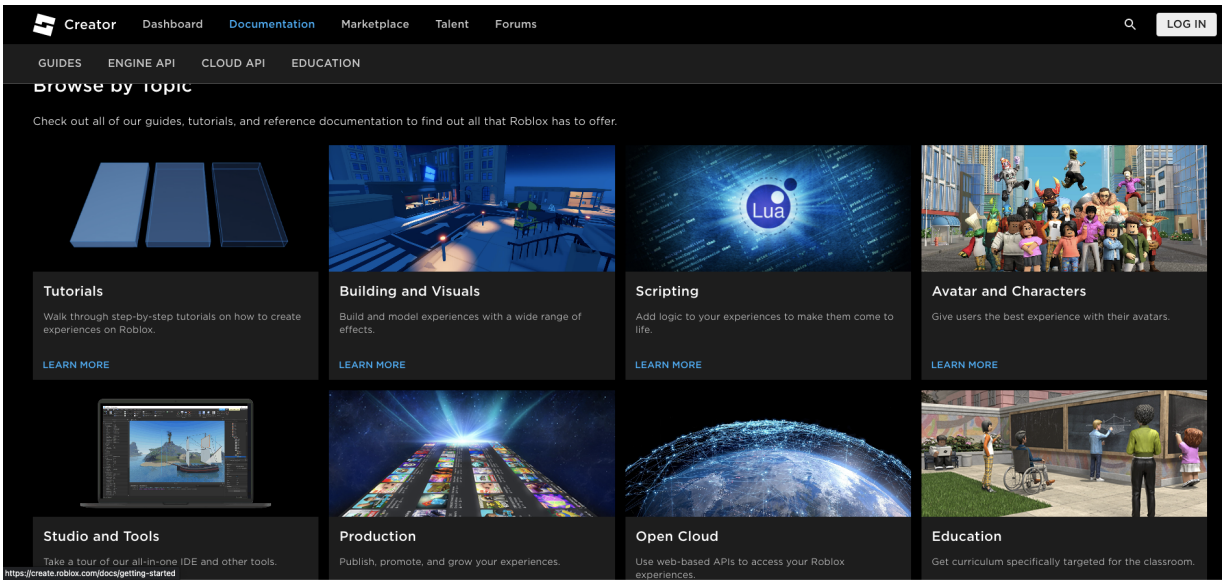
immobiliari virtuali che ha poi suddiviso e sviluppato con giardini e costruzioni architettoniche a tema da affittare e rivendere. Le sue attività sono cresciute fino a includere lo sviluppo e la vendita di proprietà per grandi aziende del mondo reale e hanno portato a una società "spin off" nella vita reale chiamata *Anshe Chung Studios*[35], che sviluppa ambienti 3D immersivi per applicazioni che vanno dall'istruzione alle conferenze aziendali e alla prototipazione di prodotti. Alcune aziende operano nell'economia virtuale di Second Life per promuovere cause benefiche, altre invece la usano come piattaforma di reclutamento e altre ancora per commercializzare il proprio brand.

2.2.2. Roblox

Roblox è una piattaforma MMORPG (Massive Multiplayer Online) creata nel 2006 dall'azienda Roblox Corporation, con sede a San Mateo in California. Solitamente la piattaforma viene confusa con il videogioco in sé, in realtà è preferibile pensare a Roblox come un ambiente di sviluppo multi-platform che dà la possibilità ai suoi utenti di creare nuovi mondi virtuali in 3D all'interno dei quali vengono ambientati i videogiochi che si desiderano programmare: l'interesse che ha avuto Roblox per le fasce di età a partire dai 10 fino ai 16 anni ha portato questa realtà negli ultimi anni a raggiungere fatturati sopra i 40 miliardi di dollari l'anno. Se nel 2020 - anno segnato dalla pandemia di Covid-19 - la piattaforma Zoom.us è stato considerato il software di riferimento per i lavoratori in smart working, si può dire che Roblox lo è stato per i videogiocatori, con una cifra che si aggira attorno ai 150 milioni di utenti attivi ogni mese.

Con la popolarità di Roblox raggiunta negli ultimi anni, la piattaforma è stata spesso accostata ad un vero e proprio Metaverso ed è facile sentire parlare del Metaverso Roblox: anche se l'idea di Roblox è molto lontana dal concetto di metaverso - si pensi solo all'assenza totale di una struttura Web3 e di una blockchain che dovrebbe stare alla base della piattaforma - sicuramente l'interesse che ha suscitato è stato proprio quello di riuscire a realizzare degli eventi (come il concerto del rapper Ava Max nel 2020) che hanno portato circa 34 milioni di giocatori contemporaneamente a ritrovarsi su Roblox, delle cifre che certamente non possono passare inosservate a chi vede il Metaverso come un'opportunità di guadagno attraverso il Merchandise e per il quale vale la pena investire.

[35] http://acs.anshechung.com/



La documentazione online di Roblox Studio fornisce un punto di riferimento per muoversi attorno alle funzionalità che l'ambiente mette a disposizione: https://create.roblox.com/docs

Roblox Studio

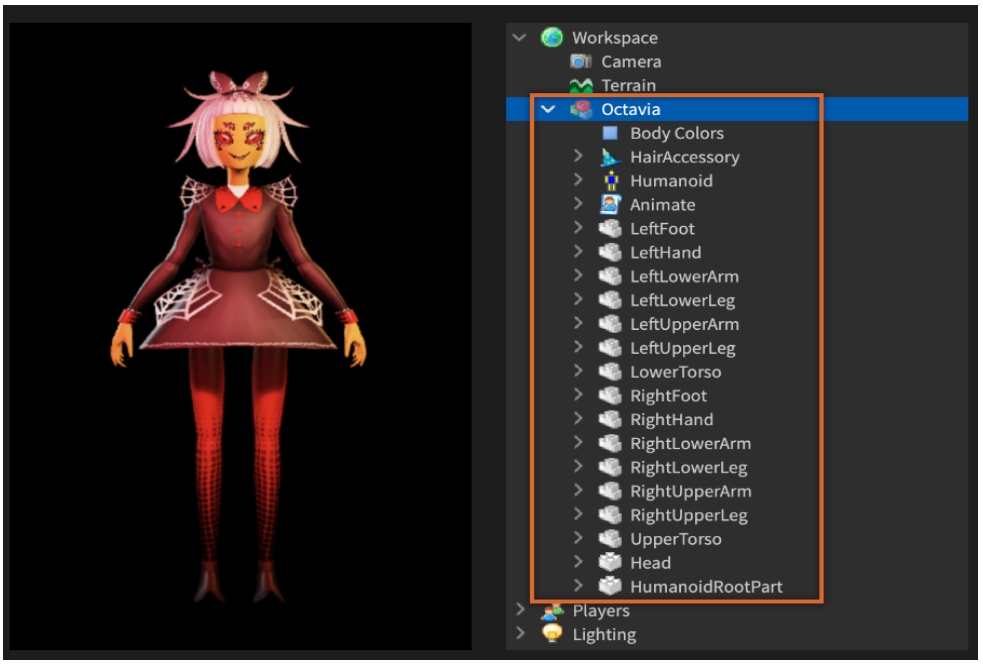
Una volta che un utente si registra ed effettua l'accesso gratuito a https://www.roblox.com, dopo essere passato per la creazione del proprio avatar, ha la possibilità di navigare tra i milioni di mondi creati dagli utenti e provare esperienze di gioco totalmente diverse, dall'action all' horror, dallo sport alle simulazioni passando a quelle avventure che rispecchiano in qualche modo i recenti interessi delle fasce di età adolescenziali, dalle serie televisive più famose ai personaggi che vanno di moda sulle piattaforme come Youtube. Ma al di là dell'utente visto come semplice utilizzatore, Roblox basa il suo successo per aver dato la possibilità ai propri utenti di ricoprire il ruolo di sviluppatori a tutto tondo delle proprie avventure. Grazie all'utilizzo del software **Roblox Studio** è possibile creare le esperienze virtuali a cui i giocatori di Roblox potranno partecipare. Il software viene rilasciato su tutti i principali Sistemi Operativi e con un unico tool è possibile seguire le tre fasi principali del progetto: ***building*** (creazione), ***playtesting*** (prova di esecuzione e test del gameplay), ***publishing*** (pubblicazione del videogioco su Roblox).

Roblox Studio permette di importare i modelli 3D da altri software di modellazione tridimensionali quali ad esempio Blender (open source) o Maya. Tutti gli oggetti e le loro caratteristiche (eventi di input associati, colori, animazioni) all'interno della scena del gioco sono

gestiti secondo una relazione a grafo. Di notevole curiosità è il tool **Terrain Editor** che troviamo all'interno dell'IDE e che permette di creare vaste distese di terreno con materiali completamente personalizzabili, che rappresenterà l'ambiente (environment) dove si svilupperà il videogioco.

Per rendere ancora più personalizzabile l'esperienza di gioco, Roblox Studio permette di utilizzare un potentissimo linguaggio di scripting, chiamato **Luau** e derivante da Lua 5.1. Per chi non fosse a conoscenza del linguaggio Lua, esso ha acquisito sempre più importanza nell'ambito del gaming essendo stato utilizzato in videogiochi molto famosi da Angry Birds a FIFA, giustificato dal fatto che si tratta di un linguaggio di scripting completamente sviluppato in C e quindi computazionalmente molto veloce e facilmente estendibile creando propri metodi e librerie: nei videogiochi che richiedono sempre più esperienze personalizzabili i linguaggi di scripting permettono di mantenere molte logiche di gioco ad un livello più esterno rispetto al core del gioco stesso, agevolando anche il rilascio di patch o aggiungendo nuove funzionalità.

Roblox, per eseguire gli script in linguaggio Luau, utilizza un modello client-server. I tipi di script utilizzati e la posizione in cui vengono memorizzati in Roblox Studio determinano se e quando saranno eseguiti dal client oppure dal server. Studio dispone di un editor di script integrato per la gestione degli script.



La figura mostra la composizione dello spazio di lavoro di Roblox nelle sue varie entità.

Robux

L'economia di Roblox è anche favorita dalla presenza di una moneta virtuale per questa piattaforma che prende il nome di **Robux**. Grazie a questa moneta è possibile acquistare delle potenzialità per il proprio Avatar oppure acquistare e usufruire di contenuti bloccati. Esso diventa la moneta con cui gli sviluppatori possono monetizzare le proprie creazioni, che potrebbero non per forza essere dei videogiochi completi, ma anche solo degli oggetti virtuali creati attraverso Roblox Studio che vanno a completare l'esperienza di gioco. Gli sviluppatori più abili e che rendono il proprio mondo talmente interessante agli occhi degli utenti possono sfruttare il **Roblox Developer Exchange**[36] (DevEx), un programma che permette di convertire i Robux guadagnati con i propri sviluppi in moneta reale. Non tutti gli sviluppatori però possono partecipare attivamente a questo programma, ma bisogna soddisfare dei requisiti imposti dal sistema stesso di Roblox, come ad esempio il raggiungimento di guadagno di almeno 30.000 Robux. Magari non tutti gli utenti che si cimentano nello sviluppo di un videogioco su Roblox possono considerarla una fonte di sostentamento, ma sicuramente questo sistema garantisce una sana concorrenza tra gli utenti e soprattutto permette di dare la giusta importanza a quegli sviluppatori che hanno fatto del proprio videogioco un punto di accesso all'utilizzo di Roblox per milioni di utenti in tutto il mondo.

2.2.3. Minecraft

Minecraft nasce come un prodotto dell'azienda di sviluppo svedese Mojang nel 2011, e per il suo successo avuto nei primi anni dal rilascio al pubblico (si parla di circa duecento milioni di copie vendute) viene acquistato da Microsoft nel 2014 per 2,5 miliardi di dollari. Ciò che rende Minecraft un prodotto di successo è la semplicità del gioco stesso, una realtà composta da blocchi tridimensionali ognuno rappresentante un preciso materiale (terreno, sabbia, pietra, lava, ecc.) che con le sue caratteristiche viene utilizzato dal giocatore per modellare il mondo attorno a lui, e realizzare così tutto quello che può servire per costruirsi un rifugio se si gioca in modalità

[36] https://en.help.roblox.com/hc/en-us/articles/203314100-Developer-Exchange-DevEx-FAQs

survival (sopravvivenza), o semplicemente per creare quello che desidera in una modalità di gioco libero. Il giocatore può utilizzare i vari materiali e mescolarli fra di loro secondo una specifica composizione in modo da realizzare nuovi oggetti da usare nel suo mondo. In Minecraft, in generale, le costruzioni avvengono con il posizionamento di blocchi di materiali specifici.

Ciò che rende Minecraft così popolare è dato anche dal fatto che si tratta di un progetto multipiattaforma disponibile su una vastissima gamma di dispositivi, dalle console come XBox e Playstation ai cellulari, per non parlare anche della compatibilità con gli ultimi visori come ad esempio Oculus Quest di Meta. Inoltre il suo codice è open source ed esistono moltissimi progetti sulla piattaforma Github che offrono un clone del progetto originale scritto in moltissimi linguaggi, e ciò permette di apprezzare la semplicità dell'idea che sta dietro questo progetto.

La community che gira attorno a Minecraft - che si aggira attorno ai 140 milioni di utenti[37] - è molto attiva e gli utenti hanno la possibilità di pubblicare i propri mondi e condividere esperienze con gli altri partecipanti. Questo è uno dei motivi per cui Minecraft viene classificato tra i Proto-Metaversi di maggiore interesse per capire la direzione verso cui puntare nello sviluppo di nuovi rivoluzionari spazi virtuali, dove la socialità e il confronto fanno sempre da fulcro per la vita digitale stessa dell'utente: il fatto che le ultime generazioni siano coinvolte nel progetto Minecraft, e soprattutto la loro tendenza ad abbandonare difficilmente questo gioco nel tempo, fa sì che Minecraft diventi un esempio da tenere in considerazione per capire cosa cerca un utente digitale: in questo caso la semplicità della grafica non è assolutamente correlata negativamente al successo del mondo virtuale, anzi: consideriamo che i giovani di oggi hanno possibilità approcciarsi al mondo del gaming con dei videogiochi dalla grafica sempre più sorprendente - i progressi del rendering e delle tecnologie di intelligenza artificiale per l'ottimizzazione delle immagini nelle schede grafiche hanno elevato sempre più gli standard dei videogiocatori - e quindi ci si può chiedere se la grafica è veramente un requisito fondamentale per l'interesse dei videogiocatori. La risposta sicuramente è sì, ma lì dove non arriva la grafica, quello che vince è l'idea, per questo Minecraft vince su molti altri titoli. In ogni caso anche Minecraft si evolve, vengono ad esempio aggiunti nuovi shaders per migliorare l'effetto delle luci sui materiali, ma in ogni caso la grafica rimane sempre un dettaglio non vincolante per il divertimento del gioco stesso.

[37] https://www.statista.com/statistics/680139/minecraft-active-players-worldwide/

Le possibilità che offre il mondo di Minecraft

In Minecraft è possibile giocare nel proprio pc o dispositivo, collegati in una rete locale o in modalità online, e si può decidere se giocare in modalità single-player o multiplayer. Una volta scelto il proprio avatar - opzionale - è possibile scegliere una ulteriore modalità di gioco: il gioco libero o la modalità Survivor, nella quale la sopravvivenza nel mondo popolato dai mob (così sono chiamate le creature comandate dal Server di Minecraft) diventa l'obiettivo principale del gioco. Gli avatar possono interagire con i vari materiali e in modalità sopravvivenza un materiale come la lava o l'acqua alta, possono diventare pericolosi per l'utente facendogli perdere salute o farlo morire. La salute del proprio avatar può essere anche compromessa dalla fame, per cui è compito del giocatore procurarsi il cibo necessario alla sopravvivenza coltivando il grano (e trasformandolo poi in pane), raccogliendo bacche, mele o cacciando gli animali che si aggirano nel territorio. Esiste anche una ulteriore modalità nel gioco multiplayer chiamata PvP (Player vs Player) nel quale i giocatori in una modalità Survival devono anche sopravvivere alle minacce degli altri avatar che possono coalizzarsi, formare dei clan, e dichiarare guerra agli altri giocatori.

Come era stato già accennato in precedenza, su Minecraft si può partecipare al Minecraft Partner Program[38] ed è possibile condividere e vendere le proprie creazioni sul marketplace proprietario, creando skin, mappe, reami, add-on e texture.

Progetto "Natale su Minecraft"

Con questo progetto Tembo, un'agenzia di comunicazione con sede a Torino, ha vinto l'Oro nella categoria Eventi Digitali agli NC Digital Awards del 2021. Dopo quasi un anno di smart working forzato a partire da Marzo 2020, alla fine dello stesso anno i dipendenti di Tembo hanno riflettuto insieme sulle esperienze positive e negative vissute nel periodo più duro della pandemia di Covid-19, e all'unanimità si è cercato di valutare quello strano modo di essere stati sempre virtualmente "presenti" in quei mesi di lockdown solo con la voce o con qualche videocamera accesa, e pensare di non potersi ritrovare tutti insieme durante le cene pre-natalizie organizzate dall'Azienda aveva generato sicuramente un grosso dispiacere tra i dipendenti. È proprio da questa necessità di trovare le giuste occasioni per rafforzare il senso di identità ed appartenenza,

[38] https://www.minecraft.net/en-us/partner

che alcuni dipendenti propongono di organizzare la Cena aziendale di Natale del 2020 su Minecraft, e la proposta ottiene un grande consenso: alcuni sviluppatori di Tembo, quindi, prendono in mano il proprio "piccone virtuale" - questo è l'elemento che l'utente si trova in mano una volta dentro Minecraft - e iniziano a realizzare nella maniera più fedele possibile l'esterno e l'interno della sede dell'Azienda, rispettando tutto quello che contraddistingue il luogo di lavoro: le stanze, la sala riunioni, i luoghi ricreativi, le cantine del palazzo….

Trattandosi di un mondo completamente virtuale, gli sviluppatori non si sono limitati alla rappresentazione di ciò che era presente realmente, hanno pensato di inserire un passaggio segreto dietro l'ufficio che magicamente apriva le porte verso un parco giochi virtuale, e quella è stata la sede dove i vari dipendenti si sono divisi in squadre e hanno portato a termine degli obiettivi tutti organizzati all'interno del mondo di Minecraft. Dopo un paio d'ore di puro divertimento, la serata si è conclusa con uno spettacolo di fuochi d'artificio e un selfie di gruppo con la speranza di ritrovarsi nuovamente insieme il prima possibile.

Minecraft come strumento educativo

Minecraft Education[39] è un ambiente di apprendimento open come il gioco di base di Minecraft (anche se non è compatibile con la versione più diffusa del gioco), e dà la possibilità agli utenti/studenti di sperimentare all'interno dei mondi superando le sfide che vengono realizzate dagli educatori. Ogni obiettivo è realizzato con l'intento di mettere alla prova le capacità collaborative degli utenti, e per introdurre ai sempre più giovani utilizzatori di Minecraft un approccio responsabile all'utilizzo degli spazi virtuali.

Esistono moltissimi casi di studio di scuole e aziende che hanno sfruttato Minecraft come strumento educativo, per citare un esempio nella città di Riga, in Lettonia, il suo utilizzo ha permesso di avvicinare i giovani alla pianificazione urbanistica della città in cui vivono, con la possibilità di scoprire in maniera diversa i suoi sobborghi, approfondire l'architettura del luogo e la sua storia e proporre nuove costruzioni che avrebbero arricchito l'identità socio-culturale dei giovani cittadini[40].

[39] https://education.minecraft.net/en-us
[40] https://urbcultural.eu/news/gamification/minecraft-as-a-tool-to-think-out-of-the-box/

Uno sguardo nel Metaverso

Come sappiamo Minecraft non basa le fondamenta del suo gioco su una struttura decentralizzata e su una blockchain, per questo motivo non può essere considerato tecnicamente un Metaverso, però dal momento in cui il gioco di Minecraft ha iniziato il suo grande successo, sono stati creati diversi progetti tutti correlati al mondo Minecraft e ai Non-Fungible Tokens. Alcuni di questi progetti sono, per citarne alcuni più importanti:

- **NFT Worlds**[41]: è una piattaforma di gioco completamente decentralizzata, completamente personalizzabile, orientata alla comunità, in cui i proprietari dei mondi possono creare i propri giochi o esperienze di un Metaverso senza limiti per i giocatori o per le comunità esclusive all'interno dei loro mondi. Utilizzando Minecraft e il suo vasto ecosistema open-source, NFT Worlds si basa sulla spina dorsale di decenni di sviluppo open source all'interno della comunità di Minecraft e la espande radicalmente per consentire un tipo completamente nuovo di metaverso di gioco 3D basato su voxel, decentralizzato e supportato dalla blockchain di Ethereum. Ogni NFT ha un "world seed", ovvero un codice in grado di generare un mondo Minecraft. Le destinazioni Metaverse possono anche essere ospitate sul server di un giocatore con l'aiuto di costruttori verificati. Nel 2021 NFT Worlds si dota di una sua criptovaluta $WRLD basata su Token ERC-20 e a partire da Luglio 2022 il progetto ha annunciato l'abbandono della piattaforma Minecraft per la creazione di un proprio Metaverso, ma senza il gioco di Mojang difficilmente avrebbe raggiunto questo successo.

- **Uplift World**[42]**:** è un Metaverso di tipo "play-to-earn" il cui mondo è costruito su Minecraft, il suo obiettivo è ricompensare i giocatori per il tempo che impiegano all'interno del mondo virtuale, e porta avanti i valori del crafting e della condivisione delle proprie realizzazioni con gli altri utenti. Per entrare a far parte di questo Mondo occorre avere a disposizione un Wallet Digitale per accumulare le ricompense di Uplift World nella sua valuta ($WAX), e poi basta accedere al server Minecraft con la modalità di gioco su Server remoto.

[41] https://nftworlds.com/
[42] https://theuplift.world/

- **Enjincraft[43]:** nasce come un plugin di Minecraft ed estende le potenzialità della blockchain all'interno dei mondi. EnjinCraft permette infatti di integrare, utilizzare e scambiare oggetti di gioco blockchain nel proprio Server. Tramite i comandi di gioco della console di Minecraft si può collegare l'identità di un asset blockchain agli oggetti di gioco o ad esempio collegare il proprio Digital Wallet al proprio avatar. Sulla base degli assets blockchain che gli utenti possiedono, è possibile dare loro oggetti o permessi speciali nel mondo di Minecraft, o in base alla loro disponibilità di moneta virtuale si possono scambiare i propri beni con altri giocatori: il baratto non diventa più l'unica modalità di scambio possibile su Minecraft.

2.2.4. Fortnite

Fortnite è stato sviluppato e poi pubblicato autonomamente da Epic Games nel 2017, è considerato senza dubbio un gioco di successo nell'ambito multiplayer. Agli inizi il gioco aveva soltanto una modalità in cui i giocatori dovevano sopravvivere in un mondo virtuale a orde di mostri, ma è solo nel momento in cui è stata rilasciata la nuova modalità free-to-play chiamata *Battle Royale* (un deathmatch in cui un massimo di 100 utenti si sfidano in una gara di sopravvivenza tutti contro tutti, con la possibilità di costruire delle strutture per difendersi o raggiungere punti irraggiungibili nella mappa) il gioco ha preso uno slancio senza precedenti in termini di popolarità e interesse. Infatti Fortnite ha dimostrato come un gioco fatto di precisi obiettivi è diventato - senza volerlo - la meta di ritrovo in Internet di milioni e milioni di utenti. Infatti si può dire che in Fortnite partecipare è molto più avvincente che vincere: è vero, sopravvivere ad altri novantanove utenti incalliti in un mappa enorme che pian piano va a restringersi è sicuramente un momento di gloria che rimane per sempre nella memoria dei giocatori, ma per tutto ciò che gira attorno alla battaglia diventa uno dei motivi per cui vale la pena partecipare. Infatti i creatori aggiornano la mappa sempre con nuovi contenuti, ad esempio l'Avatar di un personaggio famoso, oppure da la possibilità agli utenti di fare delle attività che sono completamente scorrelate ai fini della vittoria, tipo andare a pescare o cacciare cinghiali. La malleabilità del mondo di Fortnite, che risponde molto bene alle mode del momento e invoglia i video-giocatori di qualsiasi fascia di età sempre con nuovi contenuti, è stato sicuramente uno dei fattori che hanno spinto, ad esempio, la Sony ad investire altissime somme di denaro (200

[43] https://enjin.io/blog/enjincraft-plugin-for-minecraft

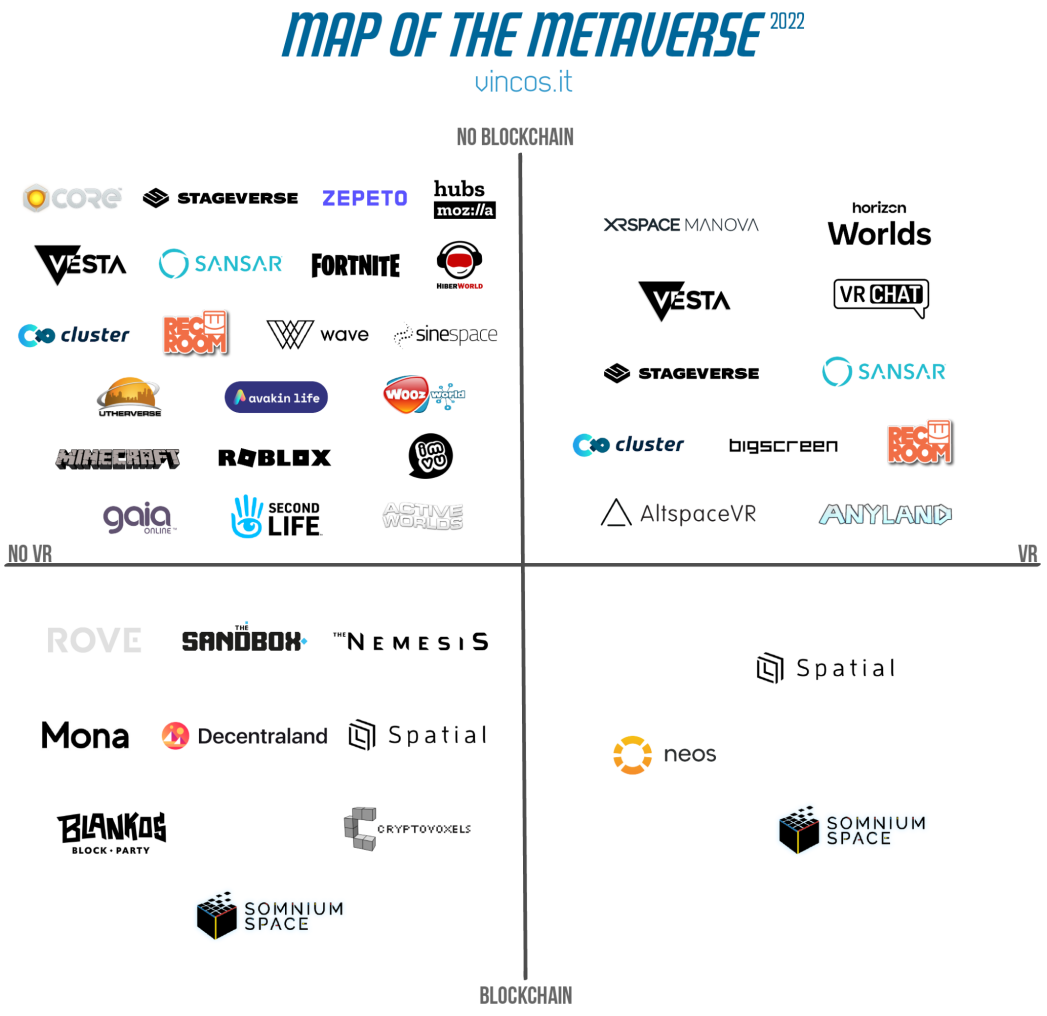
milioni di Dollari nel 2020 e 250 milioni di Dollari nel 2021) per poter arricchire sempre di più le esperienze degli utenti.

La mappa di Fortnite è stata stimata in un'estensione di circa 11.700 chilometri quadrati[44].

[44] *https://fortnite.gg*

Capitolo 3 - Metaverso e Blockchain

In questo capitolo sarà presentata una panoramica dei principali progetti che negli ultimi anni hanno proposto le loro soluzioni di Metaverso. Come viene mostrato nel grafico dell'immagine successiva, le attuali applicazioni del Metaverso possono essere rappresentate in uno spazio a due dimensioni, sulla base delle tecnologie che vengono utilizzate: se il Metaverso è stato sviluppato o meno seguendo i principi della Blockchain, e se presenta o meno il supporto alla Virtual Reality. Si discuterà di alcune soluzioni che all'interno della mappa fanno parte dei due quadranti in basso, ovvero quelli che hanno implementato la Blockchain. È interessante notare come con ciò che viene definito ad oggi Metaverso, con un certo abuso di definizione, fanno parte tutti quei Progetti che sarebbe preferibile invece definire "Proto-Metaversi" ed in particolare interessano il settore del gaming (si veda Fortnite, Roblox, Minecraft).



Mappa del Metaverso (aggiornata al 16/4/2022), fonte viscos.it

Un'altra proprietà della distribuzione degli attuali Metaversi riguarda invece i due quadranti in basso - di nostro interesse - ed è facile notare come alcuni di questi Progetti sono presenti come soluzioni che prevedono il supporto o meno della VR, il che ci fa capire come il mercato delle Aziende che puntano sul Metaverso si adatta alle tecnologie di massa attuali (browser) e cerca di proiettarsi già in un prossimo futuro all'utilizzo di tecnologie ancora più immersive.

3.1. The Sandbox (SAND)

Il progetto the Sandbox rappresenta l'evoluzione di una tecnologia desktop riadattata su una versione 3d dell'omonimo gioco in stile pixel art bidimensionale[45] creato nel 2012 da Pixowl. La società viene rilevata nel 2018 da Animoca Brands che proietta le logiche del vecchio applicativo in un mondo a tre dimensioni e nel 2020 viene rilasciato su blockchain Ethereum. Lo scopo principale del progetto è quello di dare la possibilità agli utenti della community di creare i propri spazi virtuali in maniera completamente decentralizzata grazie alla blockchain, e poter monetizzare i propri giochi e i propri oggetti. Le regole di questo Metaverso sono disponibili nel suo più recente Whitepaper[46].

L'utente può effettuare l'autenticazione a The Sandbox con diversi metodi e dopo aver creato il proprio Avatar attraverso un wizard che permette una vasta scelta di dettagli da personalizzare, può seguire una procedura molto semplice per confermare la sua reale identità attraverso una webcam. In ogni caso chi vuole diventare proprietario di un pezzo di terra virtuale in The Sandbox deve possedere un Crypto Wallet, un portafoglio virtuale che permette di effettuare transazioni con la criptovaluta di Ethereum (ETH). Le attività principali che possono essere svolte su The Sandbox sono essenzialmente tre, e vengono descritte di seguito.

Diventare un proprietario di terreni

La mappa di The Sandbox è composta da circa 165.000 LAND, appezzamenti di terreno virtuale dalla dimensione di 3072x3072x4096 voxel (pixel volumetrici) e certificati dalla Blockchain attraverso NFT. Il prezzo di ogni LAND può variare per grandezza o ricchezza di elementi

[45] https://www.thesandbox2.com/home

[46] https://installers.sandbox.game/The_Sandbox_Whitepaper_2020.pdf

aggiuntivi, che caratterizzano appunto il valore intrinseco del terreno, oppure in base alla vicinanza della LAND ad altri terreni di brand conosciuti. Inoltre è stato sviluppato un concetto di aggregazione sulle terre in modo che l'utente potrebbe acquistare più LAND contigue per creare un ESTATE, e la composizione di più ESTATE da parte di proprietari diversi può formare un DISTRICT. I terreni possono essere acquistati attraverso il marketplace interno oppure sono resi disponibili anche sui mercati di compravendita NFT come ad esempio OpenSea.

Diventare un creatore di ASSET

Gli ASSET sono oggetti virtuali utilizzabili nel Metaverso di The Sandbox, possono essere ad esempio abiti, edifici, elementi interattivi. Gli utenti che vogliono cimentarsi nella creazione di questi oggetti possono utilizzare **Vox Edit**, un software che permette la creazione da zero di oggetti in stile voxel, che possiamo pensarla come l'unità di misura del mondo di The SandBox, e attraverso questo tool è possibile poi trasformarli in NFT ERC-1155, quindi elementi virtuali commercialmente validi nella Blockchain, a questo punto possono essere messi in vendita nel marketplace di The Sandbox[47] ed è possibile così monetizzare il proprio lavoro di assets creator.

Gli assets che vengono creati possono avere delle caratteristiche, che vengono descritte in due tipologie diverse di Token di tipo ERC-20:

- *CATALYST:* può essere di quattro tipi (Common, Rare, Epic, Legendary) e corrisponde al livello di rarità di un asset.
- *GEMS:* corrisponde alle gemme, ognuna rappresentante le funzionalità dell'asset come Power, Defence, Speed, Magic e Luck.

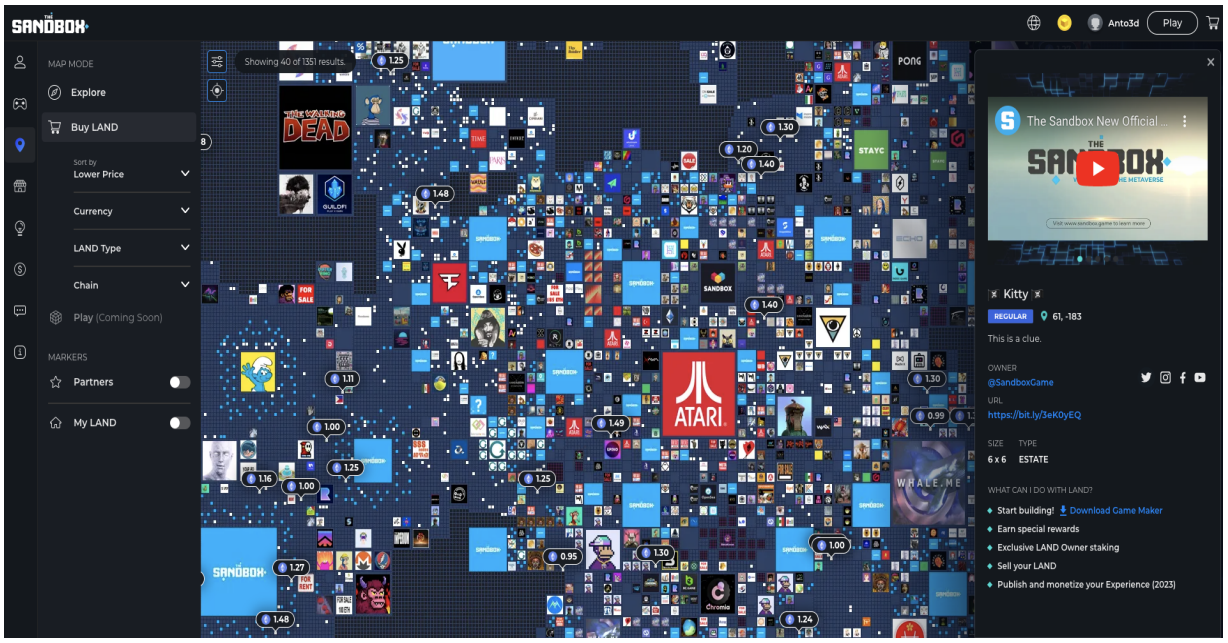
Dalla combinazione tra Catalyst e Gems di un asset si definisce il prezzo dell'oggetto che sarà venduto.

Diventare un Game Creator

The Sandbox mette a disposizione un software, chiamato appunto Game Maker, che permette di creare GAME attraverso i quali gli utenti del metaverso possono cimentarsi nel superamento delle sfide create dallo sviluppatore: questi giochi possono essere pensati come dei veri propri ASSETs, infatti anche il gioco può essere messo in vendita nel Marketplace di The Sandbox

[47] https://www.sandbox.game/en/shop/

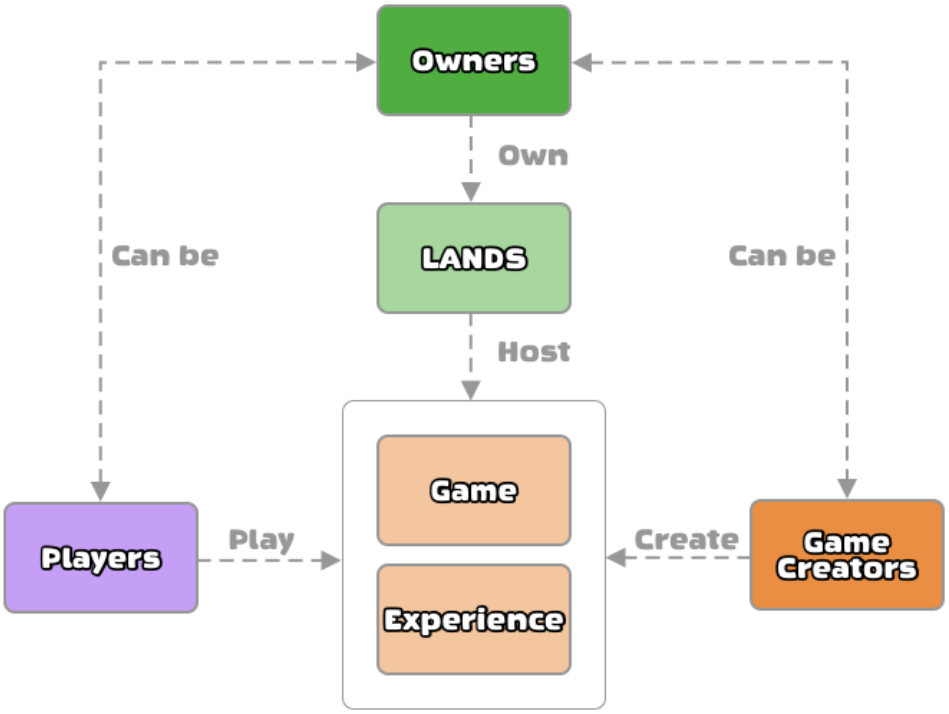
attraverso la coniatura in NFT ERC-1155. Per estendere l'esperienza di sviluppo di videogiochi anche a chi non è uno sviluppatore di codice, il tool di Game Maker fornisce anche un tipo di programmazione *no-code*, quindi non bisogna avere necessariamente delle competenze di programmazione. Inoltre grazie al Game Maker è possibile non solo pensare allo sviluppo di esperienze rivolte all'ambito ludico, ma la creazione del proprio mondo potrebbe avere anche fini totalmente estranei dal combattere mostri o risolvere enigmi: è possibile infatti creare delle gallerie virtuali di NFT, creare un proprio spazio virtuale da personalizzare secondo i propri gusti facendolo diventare un luogo di incontro con altri utenti più immersivo rispetto ad una semplice videochiamata o una chat, o organizzare/creare qualsiasi tipo di evento facendo diventare il proprio terreno virtuale un social hub. Le possibilità di monetizzare la propria esperienza diventano praticamente infinite.



The Sandbox si presenta con la mappa delle sue LAND, dove è possibile distinguere le terre già acquistate o offerte alle aziende che hanno voluto investire sul metaverso. Dalla mappa è possibile vedere il costo delle LAND libere in valuta di Ethereum.

Le diverse transazioni delle LAND, degli ASSETs e delle realizzazioni con il Game maker sono regolate dalla criptovaluta di The Sandbox, o SAND, esso è un token ERC-20 (si veda Cap. 1.7.3) che è stato emesso in 3 miliardi di unità, può essere acquistato nelle principali piattaforme di exchange o, come si è visto, lo si può "guadagnare" partecipando attivamente nel metaverso: le sue fluttuazioni sono caratterizzate dalla variazione della domanda e dell'offerta della

criptovaluta, così come le attività che vengono intraprese nel Metaverso stesso di The Sandbox (eventi importanti organizzati dall'Azienda stessa per incentivare la partecipazione, o dai Brand molto famosi che decidono di presentarsi nel metaverso).



Il grafico mostra le tipologie di utenti che possono partecipare nel Metaverso di The Sandbox, e le attività che possono compiere in relazione ai Tools (Vox Editor e Game Maker) che The Sandbox mette a disposizione per interagire nel suo Metaverso.

3.2. Decentraland (MANA)

Decentraland è un progetto basato su Blockchain Ethereum ed stato sviluppato da Esteban Ordano e Ari Meilich nel 2017, aperto poi al pubblico nel 2020, inizia la prima vendita di terreni con una ICO (Initial Coin Offer) che ha generato 26 milioni di dollari in ETH. Le attività di Decentraland e le sue basi teoriche sono descritte all'interno del suo White Paper[48].

Per vivere al meglio l'esperienza su Decentraland si dovrebbe procedere all'acquisto della sua criptovaluta MANA (usando un Digital Wallet come Metamask), con la quale sarà possibile

[48] https://decentraland.org/whitepaper.pdf

acquistare nel Metaverso assets, giochi,altri oggetti virtuali presenti al suo interno, ma soprattutto si diventa parte integrante del processo decisionale sugli sviluppi di Decentraland. Infatti la gestione delle regole di Decentraland è stata affidata ad una DAO che decide, attraverso la votazione dei possessori del token MANA, in merito alle linee di sviluppo del metaverso. Questo meccanismo influisce su tutto, dai tipi di oggetti consentiti fino ad arrivare alle tasse da praticare. Il processo decisionale viene gestito da un software chiamato Aragon. I NAMES di Decentraland sono ERC-721 negoziabili, completamente integrati con il sistema dei nomi di Ethereum. Questi nomi unici leggibili dall'uomo consentono agli utenti di scambiare i token attraverso transazioni conservate in blockchain. L'acquisto delle LAND, gli appezzamenti di terreno può essere compiuto sul Marketplace di Decentraland[49] o su OpenSea[50]. Come abbiamo visto su The Sandbox, il valore di una zona dipende molto dalla vicinanza con attrazioni popolari o strade e piazze trafficate. Tutte le transazioni vengono registrate sulla blockchain di Ethereum come prova dell'avvenuto passaggio di proprietà.

Se si entra per la prima volta in questo Metaverso, prima di tutto occorre creare il proprio Avatar, scegliendo il tipo di conformazione fisica, l'abbigliamento e gli accessori. Alcuni elementi sono gratuiti, ma per una personalizzazione massima se ne possono comprare altri utilizzando la moneta virtuale. A questo punto si viene proiettati nella piazza principale, chiamata Genesis Plaza, dalla quale si può decidere cosa visitare sfogliando i vari "mega-totem" contenenti le informazioni più recenti dei mondi o scegliere un terreno dalla mappa globale dove si può essere proiettati. Esistono diversi tipi di mondi realizzati, chi propone giochi con sfide da superare, chi si è occupato di allestire delle mostre digitali di opere NFT che poi possono essere vendute, chi vuole visitare la sala dei concerti in attesa di un evento di qualche cantante famoso, o anche solo per chi vuole ritagliarsi uno spazio personale diverso dalla piazza dove incontra i propri amici nella vita reale, e personalizzarlo a proprio piacimento.

[49] https://nftplazas.com/virtual-blockchain-worlds/marketplaces/
[50] https://opensea.io/assets/decentraland

Genesis Plaza, il punto di inizio per vivere l'esperienza quando si entra in Decentraland.

Gli utenti, per modificare il proprio mondo virtuale possono utilizzare il Builder Tool[51] che Decentraland mette a disposizione, ma chi ha dimestichezza con linguaggi tipo Typescript può utilizzare il Software Development Kit (SDK)[52], scaricabile come plugin dell'IDE di sviluppo Visual Studio Code, e creare il proprio mondo potendo anche importare i modelli 3D e creare una più personalizzata esperienza di gioco o navigazione nel mondo.

Tecnicamente, Decentraland ha un'infrastruttura p2p composta da tre layer (o strati):

- **Consensus Layer:** è il livello più basso dell'architettura, corrisponde alla base di dati dove vengono conservate le informazioni sulle particelle di terreno, le transazioni relative agli scambi di proprietà nel sistema di Decentraland. Questa base di dati è realizzata attraverso la blockchain.

- **Land Content Layer:** ogni appezzamento di terreno ha una coordinata unica nel mondo virtuale, un proprietario e un riferimento ad un file di descrizione che rappresenta il contenuto del terreno stesso, sia a livello di meta-informazioni, sia come il terreno deve essere renderizzato e l'intera logica applicativa. Per fornire qualche ulteriore dettaglio, i tipi di file che il Land Content Layer può conservare sono di tre tipologie:

    a) **File di contenuto**: fanno riferimento a tutti i file statici per il processamento di audio/video all'interno del terreno. Ogni file è

[51] https://builder.decentraland.org/
[52] https://docs.decentraland.org/creator/development-guide/sdk-101/

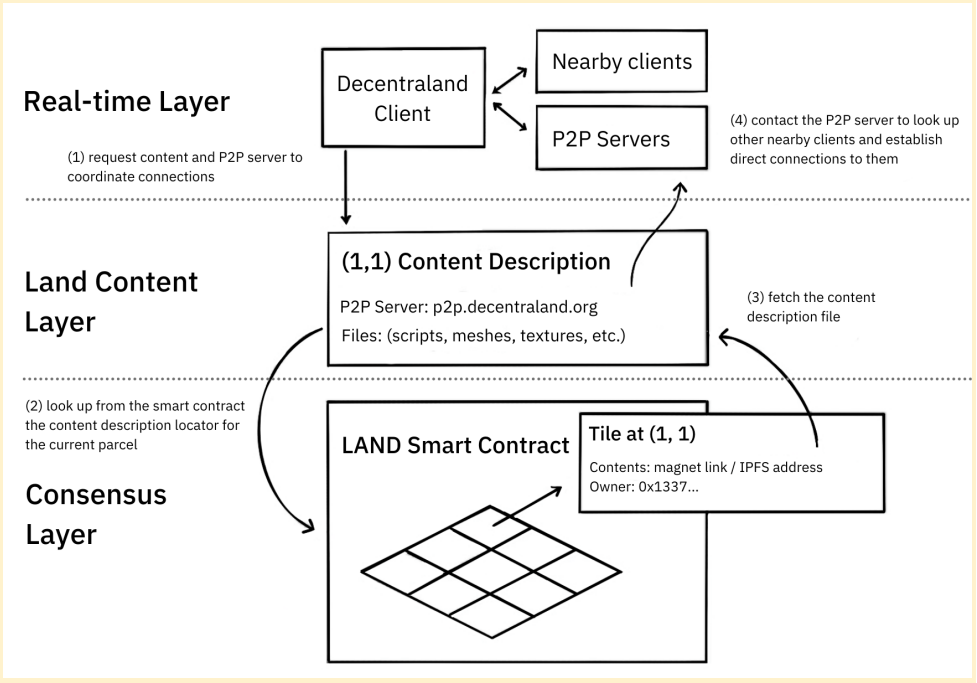
identificato da un hashcode e da questo riferimento il contenuto può essere scaricato da BitTorrent o IPFS.

b) **File di script**: che definiscono il posizionamento e il comportamento del contenuto a cui si fa riferimento.

c) **Interaction Definition** - interazioni peer-to-peer come gestualità, chat vocale e messaggistica.

- **Real-Time Layer**: corrisponde allo strato più esterno dell'architettura e si occupa di gestire l'interazione degli utenti all'interno dello stesso terreno, a livello di gestione dei flussi di dati, come ad esempio le chat vocali, i micropagamenti attraverso il sistema Payment Channel Infrastructure e la gestione degli avatar attraverso l'Identity System. Essendo una struttura completamente decentralizzata ogni proprietario in decentraland deve poter mettere a disposizione dei server di rendez-vous per coordinare gli utenti p2p che si trovano simultaneamente all'interno del proprio appezzamento di terreno. Questo permette di rendere più resiliente il terreno virtuale. Un riscontro lo si ha avuto, ad esempio, esempio quando c'è stato un problema con le API NFT che, invece di mandare in down l'intero sistema, si sono semplicemente visti gli avatar senza vestiti[53].

[53] https://twitter.com/menduz/status/1465860337727647744



Rappresentazione grafica dei layer, presente nel White Paper, in cui è suddivisa l'infrastruttura di Decentraland.

L'interesse che suscita Decentaland dal punto di vista della sua architettura, ovviamente attrae la curiosità di molti tecnici impegnati a valutare le potenzialità dei sistemi decentralizzati e del Web3 in generale, ma sicuramente deve fare molti passi avanti affinché diventi una piattaforma di riferimento per chi vorrà creare le proprie esperienze in un Metaverso. Soprattutto, vista la competizione con altri Metaversi come the Sandbox, non può in alcun modo limitarsi a diventare solo una piattaforma di acquisto di terreni virtuali, ma deve sicuramente spingere molto sulla personalizzazione degli stessi fornendo tools sempre più friendly e aperti a persone che non abbiano necessariamente competenze di programmazione o di modellazione 3D avanzate. Decentraland infatti deve provare ad evitare la perdita di interesse da parte degli utenti[54], cosa che è stata riscontrata in particolari avvenimenti pubblici, come in occasione della creazione del mondo virtuale 837X[55] a Giugno del 2022, una replica del negozio newyorkese di Samsung, adesso ridotto ad una città fantasma. Vale comunque la pena fare un salto nel Metaverso ed esplorare interessanti attività, anche se di vita breve, che circolano in Decentraland.

[54] https://www.everyeye.it/notizie/decentraland-solamente-38-utenti-popolano-giornalmente-metaverso-612662.html
[55] https://www.samsung.com/us/explore/metaverse-837x/

Il negozio virtuale 837X durante i giorni dell'apertura e della pubblicizzazione da parte di Samsung.

Capita ancora spesso che su Decentraland, negli spazi più di interesse dove era presente un po' di gente, un utente si ritrovi completamente da solo senza la possibilità di interagire con altri avatar.

3.3. Spatial.io

Il Metaverso Spatial.io (https://www.spatial.io/) è una piattaforma di realtà virtuale basata su Blockchain e consente agli utenti di creare, esplorare e interagire in spazi totalmente personalizzabili. È stato progettato per essere utilizzato in diversi settori, tra cui l'istruzione, i giochi, le imprese. Spatial è uno dei Metaversi maggiormente utilizzati per organizzare mostre o eventi e attraverso la sua integrazione con OpenSea, un marketplace di NFT, permette di acquistare elementi 3D per arricchire il proprio spazio virtuale.

Per creare il proprio spazio e modificare stanze, edifici, paesaggi all'interno di Spatial.io è necessario un Toolkit da utilizzare con Unity (https://unity.com/), un popolarissimo Game Engine Framework con il quale è possibili creare non solo giochi, ma viene usato anche in diversi ambiti dove il 3D diventa necessario. Ogni elemento del proprio spazio quindi può essere oggetto o meno di un'interazione degli utenti, come pulsanti, porte, o qualsiasi utilizzo si vuole dare ad un modello tridimensionale.

Una delle caratteristiche principali sulle quali Spatial.io vuole puntare è l'integrazione sociale - possibilità di connettersi sulle piattaforme dei social media e invitare altri utenti ad unirsi al proprio spazio - e la collaborazione degli utenti in tempo reale, dal gioco alla partecipazione di un evento virtuale come mostre o presentazioni. Non per nulla nel Luglio del 2022 è stato utilizzato, ad esempio, per presentare per la prima volta - all'Università di Torino - un lavoro di Tesi all'interno di un Metaverso, in cui il tesista e i vari relatori si sono incontrati sia fisicamente che su Spatial.io per seguire la discussione dell'elaborato, in presenza di alcuni altri utenti (tra parenti, amici e curiosi) che per motivi di distanza e per le limitazioni imposte dai protocolli COVID non hanno potuto essere presenti alla discussione dal vivo.

I progetti di Spatial.io nascono multipiattaforma (PC, Mac e dispositivi mobili) e sono nati per essere navigabili inizialmente da browser, ma si stanno facendo grossi passi avanti nel poter fruire di questi spazi attraverso la VR, utilizzando Oculus Quest o HTC Vive.

La Laurea di Edoardo di Pietro dell'Università di Torino, il primo studente a discutere il lavoro di tesi sia in presenza dei relatori, che nel Metaverso.

3.4. Somnium Space (CUBE)

Somnium Space[56] è un Metaverso multipiattaforme navigabile via web o in realtà virtuale, ed è basato su Blockchain Ethereum: a differenza di altri progetti che offrono la possibilità di acquistare terreni, creare o importare oggetti e/o avatar e commercializzare con una propria criptovaluta (CUBE), l'intero suo ambiente viene modellato interamente dagli utenti che vi partecipano e che possono costruire da zero gli spazi che poi saranno condivisi tra gli altri utenti del Mondo. CUBE è un token crittografico progettato per essere sicuro, decentralizzato e soprattutto - qualità che contraddistingue Somnium Space da altri Metaversi - è intercambiabile tra diversi metaversi VR, in quanto Somnium è membro della associazione di settore "VRBA" (Virtual Reality Blockchain Association).

Secondo le parole di Artur Sychov, il CEO di Somnium Space**:** *"L'obiettivo finale è quello di portare un sogno duraturo per l'umanità di immergersi completamente in un mondo enorme che è in continua evoluzione e non è mai lo stesso, non importa quando tu decida di unirti"*. Infatti uno dei principali obiettivi di Somnium Space è quello di creare attorno a questo mondo una community che partecipi attivamente alla realizzazione, che possa scambiare suggerimenti e feedback, al fine di migliorare gli spazi virtuali in cui si è immersi. Inoltre sono state sviluppate

[56] https://somniumspace.com/

delle metriche apposite che definiscono il grado di partecipazione e di interesse dell'utente all'interno del mondo.

L'interazione in questo Metaverso può avvenire tramite dispositivi VR oggi presenti sul mercato, ma è interessante scoprire che lo spazio può essere anche navigato in due dimensioni da un PC estendendo l'accesso su una vastissima gamma di dispositivi. Uno degli obiettivi che si è posta Somnium Space è quello di rilasciare un dispositivo VR, dotato di un'apertura auricolare di 115° e Open Source: sempre secondo le parole del CEO Sychov l'esperienza di gioco virtuale deve essere personalizzabile su tutti i livelli e per questo motivo saranno rilasciati i modelli in 3D per permettere agli utenti di realizzare e personalizzare in completa autonomia i pannelli del proprio visore.

In Somnium Space i vari terreni appartenenti agli utenti sono collegati da strade e per gli utenti che acquistano più di un lotto le strade stesse diventano disponibili alla modifica. Esistono diverse dimensioni dei lotti che possono essere acquistati ed edificati e al momento è possibile scegliere tra le seguenti dimensioni:

- **Small**: 10 metri quadrati
- **Medium**: 25 metri quadrati
- **Large:** 50 metri quadrati

Builder

Una volta acquistato il proprio lotto è possibile, attraverso il Builder di Somnium Space, cominciare la creazione delle proprie strutture virtuali: è possibile scegliere una vasta gamma di risorse già pronte oppure se si vuole aumentare la personalizzazione dello spazio si possono acquistare nuove risorse attraverso il Somnium Store. Grazie all'utilizzo della blockchain la compravendita dei beni all'interno dello Store viene regolato attraverso lo scambio di NFT il cui valore dipende dalla risorsa.

Somnium Space Builder, il tool di creazione dei propri edifici su Somnium Space.

Karma level

Il Karma level è un' interessante metrica creata nel mondo di Somnium Space che calcola la "prospettiva etica" di un utente attraverso:

- *Engagement*: basato sull'economia dell'utente, viene misurata attraverso il numero di proprietà dei lotti nel mondo e sul tempo trascorso dall'utente all'interno di essi.
- *Fattori sociali*: azioni che effettua l'utente come ad esempio l'organizzazione di eventi, supporto agli altri utenti.

La ricompensa al Karma Level viene ottenuta nella valuta CUBE, che regola gli scambi di Somnium Space.

Live forever

Una delle funzionalità più interessanti su cui Somnium Space sta puntando viene chiamata "Live forever" (*vivi per sempre*) e si delinea come una novità tra i vari Metaversi conosciuti fino ad oggi. L'idea, principalmente, è quella di fornire agli utenti di Somnium la possibilità di costruire un proprio Twin 3D che non rappresenti soltanto la funzione di Avatar nello spazio virtuale, ma è pensata come una fedelissima rappresentazione in tre dimensioni di un utente non solo nell'aspetto ma anche nei comportamenti, nei movimenti delle sue mani e del suo corpo, nelle

sue espressioni, nella sua memoria. Questo gemello digitale è considerato dagli ideatori di Somnium una sorta di **"eredità digitale"** di sé stessi, che può vivere anche dopo la nostra vita fisica e può essere raggiungibile dai propri cari in qualsiasi momento collegandosi nello spazio virtuale. Somnium prevede di integrare le potenzialità dell'intelligenza artificiale con la raccolta e la classificazione dei dati relativi ai comportamenti della persona in modo da rendere le interazioni del proprio gemello digitale più simile all'utente fisico che al momento, se vuole provare il servizio, è costretto a scegliere tra una gamma predefinita di movenze e comportamenti e non lo rendono completamente personalizzabile.

L'opzione "*Live Forever*" suscita una notevole curiosità tra gli utenti che vogliono provare le potenzialità del Metaverso, ma fa sorgere anche moltissimi punti interrogativi, soprattutto sulla privacy e sicurezza dei dati che vengono raccolti per gestire il proprio Twin 3D. Per questo motivo Somnium punta alla massima trasparenza sui dati che la compagnia stessa potrebbe vendere alle aziende: nasce pertanto il dubbio se questo servizio può essere un'estensione gratuita di questo Metaverso oppure dovrebbe essere rilasciato come un servizio a pagamento, o comunque dato a disposizione ad utenti in una modalità Premium di utilizzo di Somnium, in quanto la preoccupazione principale è proprio il fatto che nei servizi offerti gratuitamente il valore scambiato sono proprio i nostri dati.

Capitolo 4 - Futuro del Metaverso

In questo capitolo saranno presentati quattro possibili scenari che il *Copenhagen Institute of Future Studies*, in un suo recente Whitepaper[57] ha magistralmente descritto per categorizzare la futura evoluzione del Metaverso, essi sono identificati nelle seguenti tipologie:

- Free Metaverse
- Nerdverse
- Betaverses Disunited
- One Metaverse to rule them all

Ogni singolo scenario ha le sue precise caratteristiche, e per ognuno di essi si forniranno degli spunti di riflessione per capire gli elementi chiave che potrebbero delineare in un prossimo futuro i successi o i fallimenti del Metaverso, delle sue tecnologie e degli impatti che potrebbe avere sulla società.

Dal momento in cui si è sentito parlare sempre più di Metaverso, le principali Aziende che hanno investito su di esso hanno iniziato a pubblicizzare questa nuova tecnologia facendo perno sulle potenzialità della Realtà Virtuale, senza considerare però che proiettarsi nel Metaverso richiede il superamento di limiti tecnologici (visori per la VR, blockchain) che dovrebbero rendere appetibile lo sviluppo di proprie attività in questa nuova dimensione virtuale, e avere la certezza che le persone siano prima di tutto interessate ad utilizzarlo. Al momento però lo sviluppo tecnologico sul Virtuale procede con una velocità diversa da quella sperata, facendo spostare il focus su un'altro tipo di realtà, quella aumentata. Il riscontro più evidente lo abbiamo avuto proprio con Meta (ex Facebook Inc.) che fino al 2022 ha puntato a pubblicizzare il Metaverso come mondo virtuale e agli inizi del 2023 invece lo vediamo più incentrato all'applicazione e allo sviluppo della tecnologia come supporto ed estensione delle possibilità nel mondo reale, sottolineando gli impatti positivi che l'utilizzo della AR potrà avere negli ambienti dell'agricoltura, della medicina, e del lavoro in generale[58].

[57] https://cifs.dk/metaverse

[58] https://about.meta.com/it/metaverse/impact/

Situazione diversa invece per Microsoft, che negli ultimi anni ha portato avanti una serie di importantissime acquisizioni nel settore videoludico - si consideri il caso più recente dell'acquisizione del gruppo Activision (che comprende Activision, Blizzard e King) e le battaglie legali con Sony che si oppone fortemente a questo potere che Microsoft sta esercitando nel mercato - e pare abbia come obiettivo il controllo dei più importanti Mondi Virtuali nel settore del gaming. Se l'acquisizione di Activision dovesse andare a buon fine, Microsoft potrebbe aggiungere nella sua lista di spazi virtuali oltre a quelli in possesso (Minecraft e Altspace VR) anche Call of Duty, World of Warcraft e Starcraft: questo scenario vedrebbe un oligopolio in cui Microsoft e Sony riuscirebbero a tagliare via qualsiasi altro competitor, Meta compreso, in quello che al momento sembra essere il settore più concreto per l'applicazione dei concetti basilari del Metaverso così come è stato inizialmente concepito, dove mondi totalmente diversi tra loro nelle caratteristiche e negli scopi potrebbero garantire ***esistenza e persistenza*** degli Avatar e degli assets. Nel secondo Capitolo ho fornito una panoramica sulle principali tecnologie che dovrebbero caratterizzare in un prossimo futuro la connessione e la presenza dell'utente nel Metaverso, ma ci chiediamo se questa nuova dimensione un giorno potrà essere considerata uno ***spazio unico*** nel quale sarà possibile spostarsi tra i vari mondi interattivi che saranno creati nei più svariati ambiti della conoscenza umana, ma in qualche modo regolati da principi comuni e dalla piena interoperabilità tra essi: l'unicità richiede anche il Metaverso sia in qualche modo ***open,*** quindi aperto dal punto di vista della proprietà e delle tecnologie che lo compongono, indipendente dal punto di vista delle entità commerciali che lo regolano e, soprattutto, gratuito e accessibile indistintamente da tutti. In realtà questa idea, vedendo i precedenti storici dell'evoluzione tecnologica del web, può sembrare alquanto utopistica: possiamo pensare alla famosa Guerra dei Protocolli che ha portato alla creazione di Internet come la conosciamo e usiamo oggi, o senza andare troppo indietro nel tempo ricordiamo ad esempio come si è evoluta la storia dei Web Browser - che sono tuttora il mezzo principale e il punto di riferimento per accedere a Internet - o anche i servizi web più recenti che vengono messi a disposizione per creare applicazioni in Cloud: essi sono tenuti nelle mani delle compagnie che da sole rappresentano la fetta più grossa del mercato del web (Google, Meta, Amazon, ecc..) il cui guadagno deriva non solo dall'affitto delle risorse tecnologiche - cpu, ram, storage - che mettono a disposizione, senza dimenticare il valore dei dati raccolti sugli utenti che utilizzano i loro servizi e gli end-users che a loro volta utilizzano le applicazioni sviluppate sui loro servizi.

Ciò che si è delineato negli ultimi anni, e sulla base dell'analisi dei progetti che si sono spinti maggiormente oltre nell'idea del Metaverso, è che ogni singolo Mondo (o Progetto, inteso ad esempio come Sandbox, Decentraland, ecc..) è sviluppato per specifici scopi ma l'esperienza utente è blindata solo a quel Mondo, chi ha ad esempio creato un gioco su Sandbox non può ricevere come ricompensa un pezzo di terra su Decentraland, oppure chi ha acquistato l'NFT di un oggetto virtuale può usarlo solo all'interno del mondo dove è stato sviluppato. Al momento si può parlare più di Metaversi chiusi, o Proprietari, che allontanano l'idea di un metaverso unico, bensì delineano il formarsi di un Metaversi multipli, o più in generale di **Multi-Metaverso**. Infatti molti Proto-Metaversi - come quelli relativi agli esempi forniti nei capitoli precedenti - possono essere visti come progetti fini a sé stessi: se prendiamo in considerazione tutti quei Metaversi che non dipendono da blockchain, abbiamo già perso uno degli elementi fondamentali dell'unicità, ovvero l'indipendenza dalle tecnologie e la loro decentralizzazione. Per fare un esempio, si può immaginare che in un futuro non molto lontano Amazon proponga un suo Metaverso basato totalmente sulle tecnologie dei suoi servizi AWS (Amazon Web Services), sviluppa dei protocolli molto efficienti di gestione della blockchain e garantisce l'accesso a questo nuovo spazio in maniera globale e condivisa in tutto il mondo, dando la possibilità di connettersi con una vastissima gamma di dispositivi VR/AR di altre aziende come Oculus di Meta o Playstation VR di Sony, inoltre sviluppa un marketplace di NFT i cui oggetti possono essere utilizzati su diversi mondi: sebbene questa idea ci farebbe pensare ad un Metaverso aperto - o almeno più aperto rispetto a quelli attualmente conosciuti - ci sono dei punti molto importanti su cui prestare attenzione, prima di tutto il fatto che l'intero insieme di tecnologie si basa su protocolli proprietari - i visori potrebbero registrare le abitudini dell'utente o le interazioni con gli altri players per scopi commerciali e di re-marketing, magari con l'obiettivo di invogliare il cliente ad effettuare acquisti nel proprio negozio, fisico o virtuale - senza prendere in considerazione il fatto che Amazon potrebbe regolare il sistema monetario del Metaverso con una sua criptovaluta e dare la possibilità agli utenti AWS di acquistare moneta con denaro reale, diventando in qualche modo il "price maker" del proprio Metaverso.

Come attualmente sta avvenendo con gli sviluppi degli attuali Metaversi, la concorrenza è basata proprio nel fornire sempre qualcosa di nuovo, o qualcosa di meglio rispetto all'altro, per puntare su ciò che il competitor non può fornire: proprio da qui inizia la corsa allo sviluppo di tecnologie chiuse in cui l'utilizzo delle informazioni per propri scopi e quei concetti di libertà e indipendenza che vengono dati agli utenti vengono sempre mascherati dietro a delle tecnologie molto più profonde come la blockchain.

4.1. Free Metaverse - Il Metaverso Libero

Anche se al momento questo risulta lo scenario più utopistico, è anche vero che un Metaverso regolato da protocolli globali a livello applicativo e di interazione tramite dispositivi VR/AR open source porterebbe a pensare il Metaverso come un'estensione, se non una sostituzione, del World Wide Web così come siamo abituati adesso ad utilizzarlo.

Le tecnologie non proprietarie attorno alle quali si è sviluppato questo Metaverso definiranno il modo in cui gli oggetti in 3D, gli spazi e gli assets digitali saranno rappresentati e in che modo si può interagire con essi in maniera indipendente dall'utilizzatore: un po' come accade oggi con le risorse JPEG che, importando lo stesso file su diversi siti web mostrano sempre lo stesso contenuto. Non si parlerà solo di Virtual Reality, ma si potrà interagire con gli assets in contesti di Augmented Reality: ad esempio l'AR potrà essere utilizzata come supporto allo sviluppo degli assets che poi saranno utilizzati inVR nel Metaverso, e questo sarà possibile proiettando su layers sovrapposti allo scenario reale l'oggetto da creare, per poterlo modellare, colorare e poi condividerlo in tempo reale con gli altri sviluppatori per poterlo rifinire in contemporanea e, una volta pronto, metterlo a disposizione di tutti come risorsa libera o venderlo come risorsa NFT. Quindi sulla base delle periferiche che si utilizzeranno, potenti o meno, l'utente avrà la possibilità di "vedere" o rappresentare la risorsa con un livello di dettaglio differente, ma in ogni caso potrà utilizzarla in quanto nel suo codice sono definite le sue caratteristiche intrinseche e il modo in cui potrà essere utilizzato: alla base delle periferiche AR/VR esisteranno i visori e lenti a contatto per l'output e i dispositivi aptici (guanti, tute), telecamere e scanner di retina e impronte digitali, encoder vocali come device di input. La percezione sarà portata a livelli più profondi dando la possibilità di interagire con altri sensi come il gusto o l'olfatto. In ogni caso, per chi non avrà possibilità di accedere con questi dispositivi, l'alternativa mouse/monitor sarà comunque garantita per entrare nel Metaverso.

Sicuramente se si vuole pensare ad un Metaverso unico e libero ci sarà bisogno di definire degli **standard tecnologici** legati ai dispositivi per accedervi e ai protocolli di comunicazione che permetteranno la persistenza dei dati tra i vari mondi. I dati dovranno necessariamente essere ospitati in una struttura decentralizzata come la blockchain per garantire la massima resilienza, ma non si può pensare che un solo fornitore possa prendersi in carico la gestione della base di dati che crescerà ogni giorno con milioni, o forse miliardi di transazioni, dovrà essere un impegno comune che metterà insieme tecnologie e competenze diverse. Basandosi su

architetture decentralizzate come la blockchain, gli assets e le risorse fisiche e virtuali potrebbero essere regolate da NFT e l'utilizzo delle criptovalute regolerebbe le transazioni che potrebbero essere convertite in tempo reale nella valuta locale o internazionale degli attori della transazione, annullando le limitazioni degli scambi in valute reali. In questo Metaverso verrebbe a delinearsi una nuova figura di business incentrata sulle Organizzazioni Autonome Decentralizzate, o DAO (da Decentralized Autonomous Organisations), che potrebbero accorpare dal punto di vista commerciale i Brand internazionali in nuovi modelli di organizzazione globale del mercato: si vedrebbe una concorrenza con i Brand Web3-natives, sorti nel Metaverso e che vendono esclusivamente assets virtuali.

L'impatto sociale che potrebbe avere questo scenario potrebbe essere notevole: la facilità con cui si potrà interagire nel Free Metaverse sarà data dal fatto che l'esperienza virtuale sarà sempre più simile ad una esperienza reale e questo agevolerà gli utenti che si approcciano per la prima volta a questa tecnologia, sia da grandi che da piccoli. Al giorno d'oggi molte persone anziane - facenti parte di un'epoca in cui le attuali tecnologie erano solo una fantascienza durante la loro gioventù - fanno fatica ad utilizzare le funzionalità che un PC mette a disposizione, ma magari imparano facilmente a navigare su Internet, nel Free Metaverse questa distinzione potrebbe effettivamente ripresentarsi in una forma diversa ma sicuramente agevolerà il neofita della tecnologia coinvolgendolo in un'esperienza totalmente nuova, più emozionante e sicuramente più stimolante.

4.2. Nerdverse - Il Metaverso dei pochi, o degli smanettoni

La teoria del **Nerdverse** si basa su una possibile involuzione del Free Metaverse: in pratica esso nasce sempre con l'idea di realizzare un Metaverso unico e accessibile a tutti con l'obiettivo di sostituire il World Wide Web, ma con il passare del tempo, una volta che è superata la curiosità iniziale, oppure i servizi offerti dal Web3 non soddisfano pienamente le esigenze degli utenti in termini di utilità o accessibilità, l'interesse viene sempre meno e di conseguenza il suo utilizzo. La direzione verso il Nerdverse viene giustificata dal fatto che il Metaverso potrebbe concentrarsi su tecnologie estremamente avanzate a cui non tutte le classi di utenti potrebbero avere accesso - dispositivi VR/AR estremamente costosi o difficili da usare a causa della complessa elaborazione dello spazio 3D, requisiti di rete troppo elevati per garantire una qualità

di servizio decente utilizzando le reti domestiche - e questo porterà l'utilizzo del cyberspazio solo a quei pochi utenti che possono permettersi, economicamente parlando, una totale esperienza immersiva e alle categorie più ristrette di sviluppatori negli ambiti della realtà virtuale che realizzano i servizi nel e per il Metaverso. Infatti è proprio per questi motivi che l'idea del Metaverso è stato associata - in modo alquanto dispregiativo - alla classe dei "nerd", termine utilizzato per identificare quella categoria di giovani abilissimi nell'utilizzo delle nuove tecnologie: essendo più o meno esperti in questi settori, ma parlando una lingua comune, essi tendono a proteggere la loro categoria esaltando le proprie qualità di "smanettoni" e tenendo fuori dai loro interessi quelle persone che non hanno lo stesso rapporto con la tecnologia.

Il fatto che il Metaverso possa essere vissuto da categorie di persone esperte nel settore più che dalla gente comune fa sorgere moltissimi timori a livello sociale, in particolare con l'utilizzo della blockchain e del totale anonimato sulle transazioni che essa può garantire, esso può diventare il luogo adatto alle attività illecite delle organizzazioni del cybercrimine, creando ancora di più quell'effetto di deterrenza all'utilizzo degli spazi virtuali. Inoltre, tra gli interessi delle compagnie che sviluppano i servizi nel Metaverso, potrebbero sorgere conflitti di natura economica o di potere in generale, che vanno totalmente in contrasto con gli ideali del Metaverso unico: nulla vieterebbe loro di privatizzare l'esperienza di un utente nel cyberspazio, portando nuovamente alla creazione di spazi virtuali fini a se stessi che non comunicano tra di loro.

4.3. One Metaverse to Rule Them All - La falsa idea del Mono-Metaverso

Abbiamo visto nello scenario precedente una visione di molti Metaversi indipendenti gestiti dalle Big Tech, si prevede che solo alcuni di essi diventino più popolari rispetto ad altri e proseguano la competizione del miglior Metaverso in una lotta all'ultimo sangue fatta di investimenti, nuove tecnologie e pubblicizzazione dei contenuti, fino a quando soltanto uno di essi supererà la concorrenza e diventerà il punto di riferimento dominante per il Metaverso dove gli utenti possono lavorare, socializzare, giocare, imparare, comunicare, interagire e, in poche parole, vivere a 360 gradi le loro esperienze virtuali. In realtà il Metaverso che si viene a delineare non è libero nel vero senso della parola, infatti una delle cause del fallimento della concorrenza è proprio il fallimento stesso degli strumenti tecnologici che sono serviti per costruire i vari

Metaversi: ci troviamo in un contesto in cui l'economia e il profitto vincono sempre all'open source, dove i maggiori progetti hardware e software vengono acquisiti dalle Big Tech che li sviluppano solo ed esclusivamente per monetizzare i loro investimenti; in questa realtà l'utilizzo delle applicazioni basate su blockchain per la gestione di NFT e criptovalute non raggiungono un grado di autonomia e sicurezza tale da essere considerate delle tecnologie trusted, e vengono tenute sotto il controllo di entità amministrative che monitorano il grado di legalità del servizio dato che potrebbero esistere applicazioni create per scopi illeciti e attività criminali, un compromesso che in ogni caso dovrebbe essere accettato in quanto l'alternativa sarebbe quella di identificare ogni singolo avatar nel Metaverso con una persona nel mondo reale, andando contro qualsiasi tipo di gestione della riservatezza degli utenti. Effettivamente questo scenario, in cui la blockchain non viene considerata una tecnologia sicura, non dipende dalle solide basi teoriche su cui si fonda questo tipo di ledger distribuito, bensì da chi viene programma e con quali criteri, ed è un monito che molti esperti nel settore della sicurezza rivolgono alle più popolari blockchain conosciute al giorno d'oggi, si pensi alla più recente vulnerabilità comunicata sotto il nome di RAB13: i ricercatori di Halborn, guidati dal Senior Offensive Security Engineer H. Mohamed, hanno trovato molteplici vulnerabilità all'interno del codice open-source di reti blockchain come Dogecoin, Litecoin, aventi in comune una base di codice simile, la vulnerabilità più critica scoperta riguarda le comunicazioni peer-to-peer in cui gli aggressori possono creare messaggi di consenso e inviarli a singoli nodi mettendoli offline [59].

Le regolamentazioni delle entità amministrative, se non dovessero seguire una policy riconosciuta a livello globale, potrebbero portare a limitare o censurare i contenuti nel Metaverso sulla base di motivi geopolitici o di costume che caratterizzano la loro realtà, causando frammentazione interna degli spazi virtuali in cluster di utenti che sono considerati simili dal punto di vista socio-culturale. Ecco perché si parla di una falsa idea del Mono-Metaverso, un unico mondo, è vero, ma non libero come dovrebbe essere, dove gli interessi economici e sociali si proiettano anche nello spazio virtuale.

[59] https://www.halborn.com/blog/post/halborn-discovers-zero-day-impacting-dogecoin-and-280-networks

4.4. Beta-verses: Il Multi-Metaverso dei Prototipi

Ho deciso di presentare il quarto scenario come l'ultimo della lista perché, a mio parere, rappresenta in maniera davvero significativa la situazione attuale del Metaverso, o meglio "dei tanti Metaversi": se mai dovesse un giorno realizzarsi per un breve periodo di tempo un Metaverso unico, libero e soprattutto utile, questo potrebbe anche diventare lo scenario in cui il Metaverso potrebbe nuovamente degenerare.

Se Mark Zuckerberg nel 2020 non avesse presentato al pubblico la sua idea di Metaverso, forse oggi moltissimi investimenti economici sarebbero stati dedicati ad altre aree in ambito scientifico/tecnologico, e il cyberspazio sarebbe rimasto un termine di fantascienza da non scomodare per forza. Quando però oggi si parla di Metaverso lo si fa sicuramente con un pesante abuso di definizione: si dovrebbe parlare ancora, e molto di più, di **Proto-Metaversi (o Beta-verses),** in particolare per tutti quelli non basati sulla tecnologia blockchain, e ancora di più dove gli elementi di unificazione e interoperabilità tra essi non sono nemmeno concepiti. È uno scenario in cui le Big Tech si presentano nella loro grandezza e a breve potrebbero detenere il controllo delle tecnologie e degli spazi virtuali in maniera molto simile alle modalità con cui gestiscono oggi le loro applicazioni nel web: un esempio molto evidente - che riporta l'Università di Copenaghen - lo vediamo nei servizi di messaggistica istantanea, come Messenger, Telegram, WeChat dove non esiste la possibilità di condividere contatti, messaggi o media tra una chat e l'altra, o dove oggi viene aggiunta una funzionalità e l'obiettivo dell'altra compagnia diventa quello di copiare il servizio o dare qualcosa in più, il tutto con lo scopo di invogliare l'utente a scegliere la propria applicazione. Avere questi Metaversi "chiusi" comporta che ognuno di essi può evolversi diversamente dagli altri sulle tecnologie e sui servizi offerti, ma porterebbe l'utente a dover scegliere e utilizzare soluzioni diverse per gli stessi scopi (proprio come nelle app di messaggistica). Lo stesso problema si sta verificando con le periferiche che in un prossimo futuro potrebbero essere gli elementi essenziali per entrare negli spazi virtuali, come i visori o i dispositivi aptici senza i quali il Metaverso si riduce ad un'esperienza da mouse e tastiera.

Se provassimo a dare con un po' più di attenzione uno sguardo alle mappe dei Metaversi che abbiamo descritto precedentemente come Spatial.io o Decentral ci accorgiamo come le porzioni più grosse di terreni virtuali sono in mano alle grosse Aziende dei diversi settori merceologici che ricoprono importanti fette di mercato: dato che il loro obiettivo è vendere, pubblicizzare i

propri prodotti e guadagnare, esiste una dimensione migliore di uno spazio virtuale in 3d per intercettare le caratteristiche dell'utente dai comportamenti del suo Avatar e ottimizzare le attività di marketing? Questo aspetto non è da sottovalutare, l'attività di marketing ai tempi del Web2 non è altro che una sfida continua per tracciare i comportamenti dell'utente e far diventare questi dati un valore: possono essere dati in pasto a processi di data mining per creare dei cluster di utenze sulla base di interessi comuni, possono essere venduti ad altre aziende traendone puro profitto. Così come noi utenti di Internet non ci accorgiamo o meglio non facciamo caso al fatto che accettando le cookie policy diamo il consenso a poter tracciare le nostre azioni (che non è detto siano solo i click o i tempi di permanenza su una pagina, ma consideriamo che esistono tool che analizzano anche il tempo di permanenza del mouse su una particolare area della pagina in cui ci siamo soffermati), l'analisi del comportamento di un utente che interagisce in un mondo virtuale darebbe la possibilità di capire molti più dettagli rispetto a dei movimenti del mouse su una pagina web. Immaginiamo che Adidas presenti una nuova collezione speciale con le riproduzioni Digital Twin di magliette, scarpe e altri accessori nel Metaverso, chi è interessato a questo evento si registra e inizia a navigare all'interno dello store virtuale, ovviamente si soffermerà sugli oggetti di proprio interesse, e magari decide di provare sul suo Avatar diverse combinazioni di abbigliamento, chi può impedire all'azienda di tracciare tutte queste attività? In che modo posso essere protetto dall'anonimato delle mie azioni perché non voglio che qualcuno possa trarne profitto?

Queste sono domande proprie di un'idea di Metaverso che deve essere esplorata ancora molto a fondo per valutarne realmente pregi e difetti, oggi il Metaverso viene dichiarato per quello che non è, un insieme di spazi virtuali che al momento non risolvono vere e proprie esigenze se non qualche piacere correlato all'intrattenimento e allo svago, con il tipico elemento sensazionalistico della novità e della moda del momento. Possiamo definirli dei punti di ritrovo di durata nettamente inferiore rispetto al tempo medio che un utente trascorre online durante l'arco dell'intera giornata, la sfida si presenta molto ardua. Al momento la maggior parte degli investimenti fatti dai Big Brand nasce perché si vedono profitti e vantaggi di natura puramente egoistica. Presentarsi oggi nel Metaverso può essere paragonato all'esclusività di essere stati tra i primi ad aver avuto un App per mobile del proprio sito Internet, quando ancora nessuno conosceva i template responsivi. La corsa al Metaverso dei Big Brand potrebbe spingere molte compagnie ad investire cifre altissime in criptovalute per tuffarsi dentro i Metaversi, soltanto per avere il proprio appezzamento di terreno accanto alla zona della Nike o di McDonald. Questo potrebbe spingere altri competitor a comportarsi allo stesso modo e partecipare a questa corsa,

sentendo quasi un'ansia da prestazione e con la paura di arrivare tardi all'appuntamento. Il problema è che la facilità di entrare in un Metaverso e acquistare un proprio spazio è un'attività totalmente diversa dal prendersene cura, in quanto devono essere messe in gioco competenze tecniche come la modellazione 3D, la programmazione, che non è detto l'Azienda abbia "in casa" aumentando i propri costi di gestione e manutenzione: se il risultato del proprio mondo che si è costruito non raggiunge un livello di gradevolezza tale da suscitare l'interesse degli utenti nel visitarlo - attività che richiede un'attività costante, come quando si pubblicano nuovi contenuti sul proprio blog - lo spazio virtuale diventa praticamente inutile: forse il modo per riprendere parzialmente i costi dell'investimento potrebbe essere rivendere il terreno alla multinazionale della porta accanto o a qualche Azienda che per la prima volta si affaccia nei mondi virtuali.

4.5. Conclusioni: Partire dai fallimenti

Nel paragrafo precedente ho descritto, con una considerazione molto critica, la situazione di come oggi ci viene presentato il Metaverso, o forse per meglio dire di come ci è stato "venduto". Questo però non significa che non riesco a immaginare o vedere concretamente gli effetti positivi che il Metaverso sta portando allo sviluppo di idee e tecnologie: dobbiamo ricordarci che Metaverso non può ridursi al concetto di una singola tecnologia, come abbiamo visto esso è un insieme di tante tecnologie, a diversi livelli, che devono cooperare fra di loro, e ognuno di essi è fondamentale per la riuscita del progetto sperato. Anche se non si raggiungerà mai il Metaverso per eccellenza, o se i progetti dovessero crollare sotto il peso di una umanità che non è ancora pronta per fare questo balzo in avanti in questo preciso momento storico, la spinta che ha dato il Metaverso per fare evolvere delle tecnologie considerate fino a poco tempo fa solo dei prototipi potrebbe aprire sicuramente nuove strade a servizi di utilità globale, con impatti sociali veramente concreti e molto più ampi di quelli per cui il Metaverso è stato pensato.

Sappiamo ad esempio che il Metaverso non può esistere se non basa la propria struttura dei dati su ledger decentralizzati, e quindi fa affidamento alla tecnologia blockchain da cui possono essere realizzati gli NFT o le criptovalute che regoleranno il suo mercato, ma con una frequenza quasi bimestrale sentiamo parlare di enormi fallimenti di banche che avevano investito nel settore delle criptovalute - si veda i più recenti casi come Silver Gate o il caso di Bankman-Fried con il crollo dell'exchange FTX - truffe milionarie o furti di digital wallets a utenti che avevano

investito i loro risparmi in criptocurrency. Se queste cose dovessero succedere nel Metaverso, l'intero spazio virtuale perderebbe di senso e crollerebbe, ma la tecnologia blockchain sopravvive al Metaverso anche con tutti i suoi fallimenti. È possibile affermare lo stesso con le tecnologie del Web3 e ad esempio con la sua tecnologia IPFS che sta alla base dello storage decentralizzato del nuovo web.

Se oggi dovessimo chiederci perché in un prossimo futuro dovremo essere presenti nel Metaverso, è probabile che non troveremo una risposta precisa, sicuramente se potessimo tornare indietro e chiederci la stessa cosa all'avvento di Internet avremmo avuto gli stessi dubbi. Credo che la risposta non dobbiamo cercarla nel passato e neanche nel futuro, se ci chiediamo invece perchè oggi passiamo tre quarti della nostra giornata su Internet di sicuro saremmo tutti d'accordo nell'affermare che Internet ha soddisfatto le nostre necessità, ha permesso di diffondere apertamente il sapere, ha creato nuove professionalità, ha dato la possibilità di connettere in tempo reale persone e macchine distanti migliaia di chilometri. Dobbiamo chiederci quali ulteriori distanze potrà ridurre il Metaverso?

Credo sia giusto sperimentare, provare le esperienze dei Proto-Metaversi, è uno dei tanti motivi per cui la mia deformazione professionale mi ha portato ad analizzare con un occhio molto critico questo tema e pormi più dubbi che certezze per il futuro, ho sentito il bisogno di indossare almeno una volta un visore ed entrare nel mondo della realtà virtuale, esperienza per altro divertentissima. Proprio per questo motivo vorrei presentare in conclusione di questa Tesi alcuni dei più evidenti fallimenti, conseguenze dei tentativi di sperimentare (forse troppo presto) il Metaverso o di ritagliarsi una fetta di popolarità usando questa parola. Alcuni sono un po' ironici, altri un po' meno vedendo le cifre che sono state investite, ma la speranza è quella in un futuro spero non molto lontano, di trovare dietro questi fallimenti qualcosa che mi faccia ricredere e affermare che averci provato ne è valsa veramente la pena.

La prima partita di calcio nel Metaverso[60]

« *Ci presentiamo come pionieri di una fase storia piena di innovazioni tecnologiche che aprono la strada a rivoluzionarie possibilità di trasmissione, raggiungendo e coinvolgendo sempre più*

[60] https://www.gqitalia.it/tech/article/prima-partita-di-calcio-metaverso-fallimento-totale

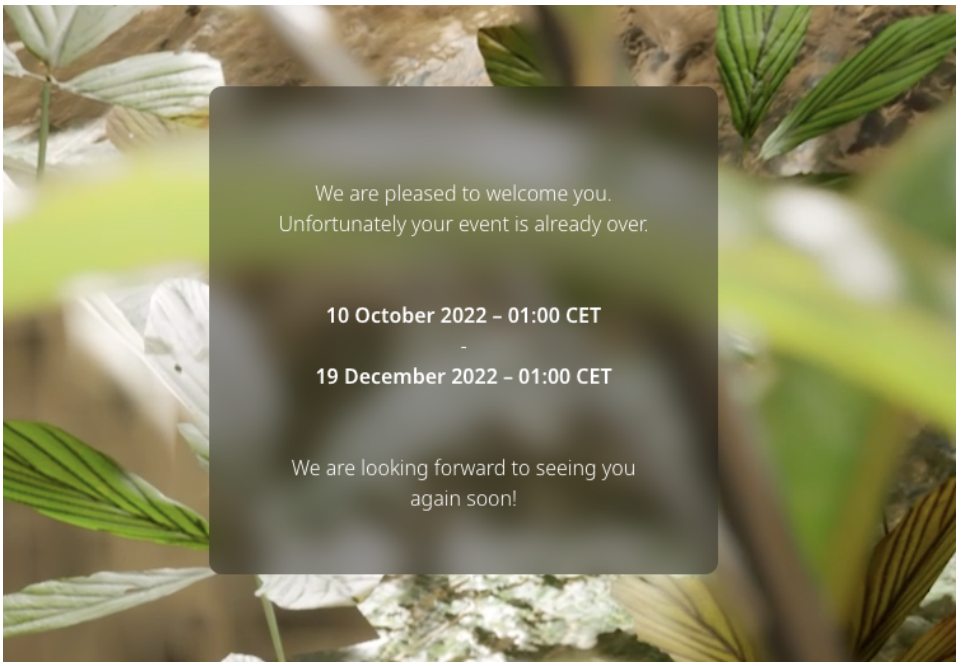
giovani tifosi in tutto il mondo ». Con queste parole Luigi De Siervo, amministratore delegato della Lega di Serie A nel Maggio del 2022 ha voluto presentare per la prima volta il calcio italiano nel Metaverso con la partita Milan - Fiorentina: l'utente ha avuto la possibilità di entrare in questo spazio virtuale dove uno schermo proiettava la partita mentre l'utente poteva chattare con le altre persone. Tutto ciò che ruotava attorno al match non aveva niente di più che vedere una partita in live stream sui canali come Youtube, che mettono accanto al video un servizio di chat per poter commentare in tempo reale gli avvenimenti della diretta. Se è questa l'idea di Metaverso a cui si vuole arrivare si è sicuramente lontani, ma anche queste esperienze possono farci capire in che modo si potrebbe, o vorrebbe, vivere e condividere nel Metaverso un evento sportivo: è vero che il Metaverso deve essere fatto di persone, ma è principalmente fatto di dati, e capire come poter sfruttare queste risorse per aumentare il coinvolgimento degli spettatori diventa una parte estremamente importante. Si pensi, ad esempio, a cosa significherebbe assistere ad una partita di calcio in "prima persona" attraverso il proprio visore, magari volando da una parte all'altra del campo o rivedere la moviola mettendosi nelle stesse condizioni di un arbitro, oppure spingersi ancora più oltre avendo a disposizione in tempo reale i parametri e fisici di un giocatore (saturazione, battito cardiaco, affaticamento muscolare) e sulla base di questi dati sfruttare le potenzialità di una blockchain applicata ad un sistema di votazione, per permettere agli spettatori di decidere le tattiche in campo e pilotare le sostituzioni. Insomma ridurre il Metaverso ad un semplice "pub" virtuale non rappresenta sicuramente il modo migliore di dire con orgoglio che si è fatto un passo nel futuro.

Global Gateway, il Metaverso Europeo

La curiosità che suscita il Metaverso e le infinite possibilità su quello che potrebbe diventare per un ampio numero di utenti, ha spinto la Commissione Europea a investire notevoli somme di denaro - circa quattrocentomila euro - per la realizzazione di uno spazio virtuale chiamato Global Gateway[61] con l'obiettivo di coinvolgere e sensibilizzare i giovani membri delle nazioni dell'Unione Europea sui temi che richiedono una partecipazione globale come i cambiamenti climatici e il lavoro. Indipendentemente dalle responsabilità di chi ha promosso o meno questa iniziativa virtuale, e come lo abbia fatto, Global Gateway è stato un vero e proprio flop analizzandolo dai seguenti dati: la Commissione afferma di aver coinvolto circa trecento utenti nei due mesi di vita del Metaverso, mentre il giornalista Vince Chadwick di Devex (il primo

[61] https://global-gateway.campaign.europa.eu/it/

analista della piattaforma) è convinto di aver trovato soltanto sei persone attive[62] con degli avatar molto particolari (a forma di graffetta). Inoltre il portavoce della Commissione afferma che la campagna si è conclusa il 15 dicembre 2022 quando il primo evento che è stato promosso su Global Gateway è datato 19 ottobre 2022, e a qui sono sorte moltissime critiche sulla quantità di denaro che è stato investito[63] per promuovere una iniziativa durata soltanto pochi mesi e che ha coinvolto un numero quasi nullo di persone.



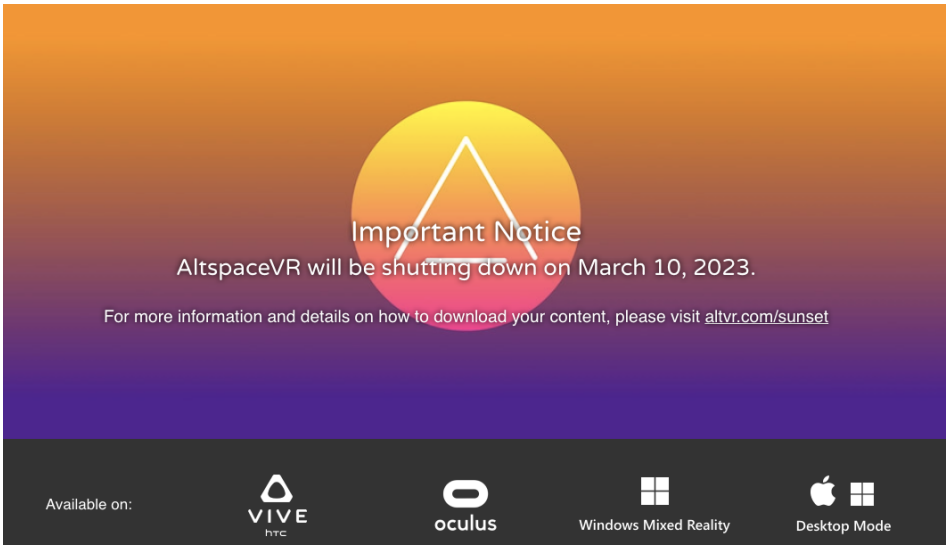
Così si presenta la pagina iniziale del progetto europeo Global Gateway nel Febbraio 2023. Il progetto risulta concluso.

Il Progetto AltSpaceVR di Microsoft

"Con un cuore tremendamente pesante comunico a tutti voi che chiuderemo AltspaceVR il 3 agosto alle 19:00 PDT. L'azienda ha incontrato difficoltà finanziarie impreviste e non possiamo più permetterci di tenere accese le luci virtuali. Questo è sorprendente, deludente e frustrante per ognuno di noi che ha messo la propria passione e le proprie speranze in AltspaceVR…".

[62] https://www.devex.com/news/eu-defends-party-in-387k-metaverse-claims-300-visitors-104601
[63] https://www.wired.it/article/metaverso-commissione-europea-global-gateway-flop/

Con queste parole Microsoft ha annunciato la chiusura di AltSpaceVR, la piattaforma di realtà virtuale sociale che ha acquisito nel 2017 (quando la startup stava per chiudere per problemi finanziari) e che chiuderà i battenti nel marzo del 2023. La notizia sicuramente suscita scalpore per il quantitativo enorme di investimenti che sono stati fatti attorno ad uno dei primi progetti in ambito VR, non solo in termini di denaro ma anche di risorse umane, considerando che circa 10.000 dipendenti erano coinvolti nello sviluppo e nel mantenimento della piattaforma. Microsoft assicura che la chiusura di AltSpaceVR non deve essere pensata come un fallimento, bensì come un trasferimento di competenze verso un progetto più grande come Microsoft Mesh[64]. L'obiettivo di Mesh sarà incentrato sulla centralizzazione della persona in un ambiente totalmente virtuale attraverso la realizzazione di Avatar e del nuovo servizio in via di sviluppo chiamato Holoportation™, attraverso il quale sarà possibile proiettare se stessi in una realtà mista come se la persona fosse presente fisicamente, e l'utilizzo del nuovo visore HoloLens.



L'homepage di https://altvr.com/ che annuncia la chiusura del Portale per il 10 marzo del 2023.

[64] https://www.microsoft.com/en-us/mesh

Appendice

Confronto tra i vari Algoritmi di cifratura

Di seguito è mostrata una panoramica degli algoritmi di cifratura in rapporto alla loro tipologia di algoritmo utilizzato.

Algoritmo/Cifratura	Simmetrica	Asimmetrica	Hash
N. di chiavi	1	2	0
Gestione delle chiavi	Difficoltà Elevata	Difficoltà Bassa	N/D
Effetto della compromissione delle chiavi	N/D	Compromissione del Ricevente e del Destinatario	Compromissione solo del proprietario della chiave privata
Velocità degli algoritmi	Veloce	Relativamente Bassa	Veloce
Complessità	Media	Alta	Media
Esempi di algoritmi	AES, RC4, Blowfish, 3DES	DSA, RSA, Diffie-Hellman	SHA-1,SHA-256, SHA-512
Lunghezza delle chiavi raccomandata	128 bits	2048 bits	256 bits

Principali Piattaforme Blockchain e tipo di Proof utilizzato

I dati sono ordinati per data di creazione del progetto.

Progetto Blockchain	Data di creazione	Tipo di proof
Bitcoin	2009	Proof of Work
Litecoin	2011	Scrypt Proof of Work
Ripple	2012	Consensus Algorithm
Nxt	2013	Proof of Stake
Ethereum	2015	Proof of Work
Cardano	2017	Proof of Stake
Near Protocol	2018	Proof of Stake
Algorand	2019	Pure Proof of Stake
Cosmos	2019	Tendermint BFT
Filecoin	2019	Proof of Replication
Helium	2019	Proof of Coverage
Theta Network	2019	Multi-Level BFT
Avalanche	2020	Avalanche Consensus
Binance Smart Chain	2020	Delegated Proof of Stake
Polkadot	2020	Nominated Proof of Stake
Solana	2020	Proof of History / Proof of Stake
Chia	2021	Proof of Space and Time
Ethereum 2	2023 (possibile rilascio)	Proof of Stake

Classifica dei Metaversi / Proto-Metaversi

Di seguito è presentata una classifica dei 20 Proto-Metaversi/Metaversi, ordinata in base ad uno Score secondo quanto riportato da https://mapsofmetaverse.com/ (situazione aggiornata a Marzo 2023).

Brand	Settore Merceologico	Metaverso/Proto Metaverso
Gucci	Fashion	Roblox
SKODA	Automotive	The Nemesis
Nike	Fashion	Roblox
Hublot	Luxury	Spatial
Stranger Things	Entertainment	Roblox
Heineken	Beverage	Decentraland
Samsung	Electronics	Decentraland
Monza Meta Circuit	Sport	The Nemesis
Spotify	Music	Roblox
Walmart	GDO	Roblox
Rai Cinema	Entertainment	The Nemesis
Wired Next Fest 2022	Magazine	Spatial
Atari	Video Games	The SandBox
Gucci	Fashion	Zepeto
Vans	Fashion	Roblox
Bulgari	Luxury	Zepeto
Christie's	Auction House	Spatial
Netflix	Entertainment	Decentraland
Gucci	Fashion	The SandBox
Bored Ape Yacht Club	Community	The Nemesis
Federico Bernardeschi	Celebrity	The Nemesis

I Brand che hanno provato un “salto” nel Metaverso

Il fondatore di MTVRS Fabio Lalli[65] ha raccolto una lista con più di 300 dei brand più importanti nella sfera internazionale, che sono stati censiti da Interbrand come i marchi che hanno già compiuto un salto nel Web3 e che si sono presentati in un - più o meno definito - Metaverso, si elencano di seguito i più importanti:

- Adidas https://lnkd.in/e6YAa3fv
- Alpitour https://skift.com/2021/08/15/why-this-new-luxury-hotel-in-venice-is-hopping-on-the-nft-frenzy/
- ATP https://art.tennis/
- Audi (VW Group) https://lnkd.in/ez_qQVVw
- Australian Open https://lnkd.in/e-nj_jUZ
- Balmain https://lnkd.in/eb8aSvzc
- BMW https://lnkd.in/eqa3x2Pe
- Bud Light (AB InBev) https://lnkd.in/ezBmK9_g
- Budweiser (AB InBev) https://nft.budweiser.com/
- Burberry https://lnkd.in/ewshTs5x
- Cartier https://nftcartier.online/
- Charles & Keith https://lnkd.in/e7ZRH5Me
- Disney https://lnkd.in/efAHFSRs
- Dolce & Gabbana https://lnkd.in/embgKiNj
- Estée Lauder https://lnkd.in/eyNpCt8b
- Ford https://lnkd.in/eXJZc7vK
- GAP https://nft.gap.com/
- Givenchy (LVMH) https://nft.givenchy.com/
- Gucci (Kering) https://lnkd.in/estudKCw
- H&M https://lnkd.in/eU8YiH9x
- Heineken https://lnkd.in/eyQX9x8X
- Hello Kitty https://lnkd.in/ey44MMjF
- Hennessey (LVMH) https://lnkd.in/evFSq_zf
- Hermes https://lnkd.in/e97uxyWB

[65] https://www.linkedin.com/in/fabiolalli/

- Hublot (LVMH) https://lnkd.in/eAJ-DhHD
- Hugo Boss https://lnkd.in/eB4-gW-B
- Hyundai Motor https://lnkd.in/e464kjFy
- Instagram https://lnkd.in/ei9Crt4v
- IWC https://nft.iwc.com
- Jack Daniels https://lnkd.in/eFT2M758
- Jacob & Co. https://jacobandco.com/nft
- KFC https://lnkd.in/eDvmb6rw
- L'Oréal https://lnkd.in/egFnCZfD
- Lacoste https://undw3.lacoste.com/
- Lamborghini (VW Group) https://lnkd.in/eq2dTM_Z
- LimeWire https://limewire.com/
- Louis Vuitton https://lnkd.in/epsJWZCc
- Marc Jacobs (LVMH) https://lnkd.in/es5Qtzk2
- Mastercard https://lnkd.in/ezmBT4-Q
- McDonalds https://lnkd.in/eTg4c5cZ
- McLaren https://nft.mclaren.com/
- NBA https://nbatopshot.com/
- Netflix https://lnkd.in/ebNqRUga
- New York Knicks https://nyknft.com/
- NFL https://nflallday.com/
- Nike https://lnkd.in/ejcAHPR4
- Nissan https://lnkd.in/eRfhtfMF
- Nivea https://lnkd.in/eVZQSHqu
- Panerai https://lnkd.in/eMxcpdgV
- Pepsi https://lnkd.in/e2gq4geM
- Philipp Plein https://lnkd.in/efn8QEKg
- Pinko https://metalovebags.pinko.com/
- Porsche (VW Group) https://nft.porsche.com
- Prada https://lnkd.in/euK6iqKy
- Puma https://lnkd.in/ez7GhnyM
- Ralph Lauren https://lnkd.in/etm5N2ge
- Ray-Ban https://lnkd.in/ebCgvJif
- Red Bull https://lnkd.in/eWM7Urkt

- Rimowa https://lnkd.in/eCQNGzm3
- Skoda (VW Group) https://lnkd.in/eFVFJRQ8
- Starbucks https://lnkd.in/e9FxsZ5B
- Tag Heuer https://lnkd.in/eAv-6ZpN
- Tiffany & Co https://nft.tiffany.com
- Time Magazine https://nft.time.com/
- Timex https://www.timex.com/the-timex-blog/go-ape-with-timex-x-bayc.html
- Trix (Nestle) https://www.nestle-family.com/en/thetrixglobe
- Visa https://crypto.com/nft/drops-event/61eff59ba9de35638f345d7d7695f902
- Youtube https://lnkd.in/e_nz8Nz7
- Yves Saint Laurent Beauté (L'Oréal) https://lnkd.in/e567h8eu
- Zara https://lnkd.in/enDpmW2q