LUISS

Dipartimento
di Impresa e Management

Cattedra Informatica

# Rivoluzione Blockchain, NFT, Web 3.0 Metaverso

Prof. Luigi Laura
RELATORE

Matr. 244521
CANDIDATO

Anno Accademico 2019/2020

# Indice

# Introduzione

La tecnologia dell'informazione ha già sconvolto notevolmente l'industria e le pratiche commerciali. Internet, d'altra parte, ha creato infiniti nuovi modi di fare business e persino interi nuovi settori che non esistevano nemmeno un paio di anni fa. Chi avrebbe mai pensato che Internet avrebbe reso possibile Spotify, Airbnb o Zoom? Il vero punto di forza della tecnologia dell'informazione è la creazione di modi completamente nuovi e più efficaci di cooperazione tra imprese e persone.

La tecnologia a cui più si dovrebbe prestare attenzione al momento è la tecnologia blockchain. Questa tecnologia abbastanza recente, così come lo è stato per Internet, consentirà modi più facili, più economici e più efficienti di fare affari, ma anche di proteggere quelli meno sicuri. La blockchain è conosciuta soprattutto come la tecnologia alla base della criptovaluta Bitcoin, ma questa tesi vuole esaminare quali altri scopi può ricoprire questa tecnologia rivoluzionaria. Poiché quasi tutti i dati presenti nelle blockchain odierne sono Bitcoin, questa tesi analizzerà brevemente che cos'è esattamente il Bitcoin e perché è in grado di essere utilizzata come valuta alternativa. Tuttavia, l'obiettivo di questa tesi è quello di sottolineare che la tecnologia non è limitata solo a questo scopo e individuarne gli altri campi di applicazione. Infatti, il Bitcoin è stato più volte criticato da grandi economisti e si sostiene che sia un'applicazione piuttosto limitata di questa tecnologia. The Economist (2016b) sottolinea che è quindi essenziale distinguere tra la tecnologia specifica alla base della moneta virtuale Bitcoin e l'idea generale di blockchain.

In poche parole, la blockchain è un libro mastro pubblico, affidabile e condiviso, che si basa su una rete peer-to-peer, il che significa che nessuno la controlla, ma viene mantenuta da migliaia di partecipanti che partecipando al network ne confermano le transazioni. La blockchain è pubblica, poiché è disponibile a tutti i partecipanti. Le informazioni registrate nelle blockchain non possono essere alterate senza attirare l'attenzione, il che, rende la blockchain un libro mastro condiviso affidabile. Queste caratteristiche permettono alla blockchain di trasferire informazioni senza la necessità di alcun intermediaro.

Gli argomenti di questa tesi includono la tecnologia blockchain, la sua importanza, le possibili applicazioni e le sfide. Anche se le applicazioni della tecnologia blockchain sono state analizzate in diversi studi, non è ancora chiaro cosa permetterà di fare oggi e in futuro

# Capitolo 1: Storia della Blockchain

Bitcoin, la prima applicazione decentralizzata costruita sulla tecnologia blockchain, è stata lanciata nel 2009, ma le sue origini risalgono a tempi più lontani. Già nel 1991 Stuart Haber e W. Scott Stornetta descrissero ciò che sarebbe diventato noto come blockchain. Stornetta è stato una figura di spicco nel campo della scienza crittografica e del calcolo distribuito negli anni Novanta. Era un fisico e un ricercatore della comunità scientifica. È stato il primo a fare riferimento all'architettura della blockchain. Stornetta e Haber hanno condotto ricerche sui meccanismi che potevano essere utilizzati per generare *digital time stamps* e ordinare i file registrati in modo sicuro e distinto, con l'obiettivo di prevenire la manomissione dei file. Bellcore è stata inizialmente fondata come azienda da Stornetta e Haber nel 1994. Bellcore offriva servizi per la marcatura temporale digitale utilizzando la struttura nota come "Linked Time Stamping Authority" (TSA). Bellcore è considerata la prima azienda a fornire servizi di blockchain. Tuttavia, nessuno ha mai implementato questa tecnologia blockchain e il suo brevetto è scaduto nel 2004.

Negli anni Novanta sono state avanzate diverse proposte per forme digitali di scambio monetario:

- Digicash (David Chaum, 1989)
- Mondex (National Westminster Bank, 1993)
- Cybercash (Lynch, Melton, Crocker & Winston, 1994)
- E-gold (Gold and Silver reserve, 1996)
- Hashcash (Adam Black, 1997)
- Bit Gold (Nick Szabo, 1998)
- B-Money (Wei Dai, 1998)
- Lucre (Ben Laurie, 1999)

Alla fine, ogni progetto si è rivelato un fallimento per una serie di ragioni diverse. Per cominciare, nessuna di queste valute digitali ha visto un'adozione abbastanza diffusa da parte dei commercianti da poter essere considerata un'opzione valida. In secondo luogo, la maggior parte di essi si affidava a un'autorità centrale e non era in grado di raggiungere un consenso sul libro mastro. Tuttavia, la cosa più importante è che nessuno di questi progetti è riuscito a risolvere il mistero del cosiddetto problema della "doppia spesa". (Gensler, 2018)

Un whitepaper intitolato "Bitcoin: A Peer-to-Peer Electronic Cash System" è stato pubblicato nel 2008 sotto lo pseudonimo di "Satoshi Nakamoto" dagli sviluppatori di Bitcoin. Questo whitepaper incorporava un modello di blockchain nella sua presentazione. Questo modello utilizzava e utilizza tuttora le stesse caratteristiche del modello iniziale di blockchain sviluppato da Stornetta e Haber. Nel whitepaper, Satoshi Nakamoto fa riferimento anche a B-Money di Wei Dai e Hashcash di Adam Black nel whitepaper. Satoshi Nakamoto è riuscito a riunire tutti i migliori di questi progetti falliti, ma soprattutto ha trovato un modo per risolvere il "problema dei generali bizantini" che essenzialmente impedisce agli utenti di spendere due volte le transazioni, rendendo così la blockchain BFT (Byzantine Fault Tolerant). (Double-Spending) (Gensler, 2018)

Nessuno sa con certezza chi o quale gruppo si celi dietro Bitcoin; nessuno si è mai fatto avanti per rivelarne l'identità. Satoshi Nakamoto ha continuato ad essere attivo nello sviluppo di Bitcoin fino al 2010 e attualmente detiene circa il 5% della fornitura totale di bitcoin, che equivale a circa 1 milione di bitcoin. (Hayes, 2021)

Nel 2014, una piattaforma blockchain nota come "Ethereum" è diventata il veicolo per il lancio della cosiddetta seconda generazione della tecnologia blockchain. Vitalik Buterin, un programmatore informatico russo-canadese, e Gavin Wood, un informatico inglese, sono accreditati per la creazione di Ethereum. Wood è anche il creatore di Polkadot e Kusama, protocolli di rete ad architettura multi-chain che consentono il trasferimento di dati arbitrari tra le blockchain. Vitalik Buterin, che aveva solo 20 anni quando è stato lanciato Ethereum, aveva una formazione informatica grazie al padre, Dmitry Buterin, che era un informatico e che ha inizialmente introdotto Vitalik al Bitcoin nel 2011. Al momento del lancio di Ethereum, Vitalik Buterin aveva solo 20 anni. A quel tempo, Vitalik iniziò a lavorare come scrittore per "Bitcoin Weekly" e veniva pagato cinque bitcoin per ogni articolo che produceva. Tuttavia, nel settembre 2011, Vitalik Buterin è stato uno dei principali autori della pubblicazione "Bitcoin Magazine", che ha co-fondato insieme ad altri. Il sito web Bitcoin Weekly è stato chiuso a causa delle entrate insufficienti. Il libro bianco iniziale di Ethereum è stato scritto da Buterin e pubblicato nel 2013. Buterin riteneva che la piattaforma bitcoin necessitasse di un linguaggio di scripting per facilitare lo sviluppo di applicazioni. Egli propose di implementare questo linguaggio nella blockchain di Ethereum con il nome di "Smart Contracts". La rete Ethereum è entrata in funzione nel luglio 2015 e attualmente è la seconda più

grande blockchain, dopo il Bitcoin, in termini di capitalizzazione di mercato totale per le criptovalute.

Charles Hoskinson, che è stato anche uno dei cofondatori di Ethereum, ha fondato nel 2015 una società di ricerca e sviluppo con il nome di Input Output Global (IOG). Questa società è la forza trainante della creazione di una piattaforma blockchain nota come "Cardano". A differenza di Bitcoin ed Ethereum, che utilizzano il meccanismo di consenso "Proof-of-Work", Cardano è stato progettato da zero per essere una blockchain basata su "Proof-of-Stake". Cardano è stata concepita come una piattaforma blockchain più sicura, priva di commissioni e in grado di offrire le stesse funzionalità di Ethereum attraverso l'uso di smart contracts. La tecnologia blockchain nota come Cardano può essere considerata come appartenente alla terza generazione. All'inizio, Cardano si concentrerà sulla risoluzione di problemi simili a quelli affrontati da Bitcoin ed Ethereum. Questi problemi comprendono le elevate commissioni di transazione, l'elevato consumo energetico, la scalabilità e l'interoperabilità. Il progetto Cardano è sviluppato da professionisti del mondo accademico e da ingegneri di alto livello. È stato scritto nel linguaggio di programmazione Haskell ed è interamente open-source. Ad oggi, lo IOG ha pubblicato un totale di 128 articoli accademici relativi alla ricerca su Cardano. Cardano è stato presentato al pubblico per la prima volta nel 2017, ma da allora è stato oggetto di critiche a causa del ritmo glaciale del suo sviluppo. Solo nel 2020 Cardano ha lanciato la sua seconda fase dal lancio, che comprendeva un meccanismo di staking che consentiva ai titolari di token nativi di puntare i propri token (ADA) per ottenere passivamente altri token ADA. Questa è stata la prima grande pietra miliare dello sviluppo di Cardano dal lancio. Settembre 2021 ha segnato l'inizio della terza fase, che ha incluso l'incorporazione di funzionalità di smart contract per lo sviluppo di applicazioni. (Hussey;Hamacher;& Chipolina, 2021)

Le elevate commissioni di transazione e la lentezza delle transazioni su Ethereum sono cresciute al punto che Ethereum è stato costretto a sviluppare un importante aggiornamento che trasformerà il suo meccanismo Proof-of-Work in un meccanismo Proof-of-Stake. Si prevede che questo aggiornamento sarà rilasciato attorno al 15 Settembre 2022.

# Capitolo 2: Fondamenti tecnici della Blockchain

La blockchain è un sistema, un tipo di database condiviso, immutabile e di sola appendice che contiene informazioni in blocchi. I blocchi che memorizzano questi dati sono tutti concatenati tra loro, da cui il nome "Blockchain". Ogni blocco contiene una serie specifica di dati, in genere quelli relativi alle transazioni, e una firma che verifica sia il blocco in questione sia quello che lo precede. Questo garantisce che ogni blocco possa essere distinto dagli altri e che la catena non si interrompa. Per il modo in cui è stata progettata la blockchain, ogni blocco è collegato a quello che lo ha preceduto e a quello che lo seguirà. A causa del modo in cui sono implementati i metodi crittografici, una mutazione in un singolo blocco influenzerebbe l'intera catena successiva. Poiché ciò verrebbe immediatamente notato nella rete, l'unico modo per corrompere il sistema blockchain è quello di apportare modifiche all'intera catena. Poiché sarebbe molto difficile e poco pratico apportare modifiche all'intera catena, le blockchain sono spesso considerate luoghi particolarmente sicuri per l'archiviazione delle informazioni.

Le blockchain sono comunemente concepite come piattaforma per le valute digitali. Le blockchain sono un tipo di DLT (distributed ledger technology) in cui i dati relativi alle transazioni sono memorizzati in un blocco. Nel mondo di oggi, ci sono molti casi d'uso diversi che potrebbero trarre vantaggio dall'implementazione della tecnologia blockchain. Alcuni di questi casi d'uso includono gli smart contracts, i servizi finanziari, le catene di fornitura, l'anticontraffazione, le identità digitali, i sistemi di voto e la sanità. (Euromoney Learning, n.d.) (Hayes, 2021) (Blockchain Overview, n.d.) (Gensler, 2018)

Esistono diversi tipi di sistemi che possono essere implementati utilizzando la tecnologia blockchain, tra cui quelli pubblici, privati, autorizzati, ibridi e sidechain. Chiunque è in grado di leggere, scrivere e verificare le transazioni che avvengono in una blockchain pubblica, il che significa che chiunque può accedere a questo tipo di blockchain. Una blockchain pubblica sarà in genere completamente autogestita e sarà in grado di offrire operazioni realmente decentralizzate, democratizzate e prive di autorità, come quelle offerte dalla rete Bitcoin. (Geroni, 2020) (Seth, 2021)

Una blockchain privata è una blockchain a cui non può accedere chiunque e che può essere gestita on-premise o dietro un firewall aziendale, entrambi elementi che ne aumentano il livello di sicurezza. Le blockchain private possono essere efficienti per le aziende private. Per entrare a far parte di questa rete, gli utenti devono ricevere un invito che sia stato autenticato e controllato. Una blockchain privata sarà sempre governata da qualcuno, ad esempio un'azienda privata. L'operatore di una blockchain privata ha la possibilità di manipolare l'intera catena sostituendo, modificando o cancellando le voci della blockchain. (Seth, 2021)

Le blockchain autorizzate possono essere utili per le aziende la cui architettura blockchain prevede la collaborazione con terzi, come ad esempio una soluzione logistica basata su blockchain. Questo tipo di soluzioni può beneficiare della maggiore sicurezza e privacy che le blockchain autorizzate offrono. Per sviluppare una soluzione di blockchain logistica, si potrebbe concedere l'autorizzazione a chiunque abbia accesso alla catena di fornitura e abbia bisogno di archiviare dati sulla blockchain. Si potrebbe trattare di un rivenditore, un produttore, un fornitore, un trasportatore e così via.

Una blockchain collegata a un'altra blockchain, chiamata catena principale, è nota come sidechain. I dati possono essere spostati avanti e indietro tra la catena principale e la sidechain. Possono esserci più sidechain collegate alla catena principale. Una delle molte ragioni per creare una sidechain è per scopi di sviluppo, anche se ce ne sono molte altre. I prodotti su cui gli sviluppatori stanno lavorando potrebbero essere testati su una "rete di prova", che potrebbe essere una sidechain della catena principale. L'obiettivo finale delle sidechain è quello di far lavorare insieme l'ecosistema di diverse blockchain senza soluzione di continuità. Questo obiettivo sarà raggiunto consentendo alle singole blockchain di mantenere la propria autonomia e, allo stesso tempo, di abilitare la funzionalità cross-chain l'una sull'altra.

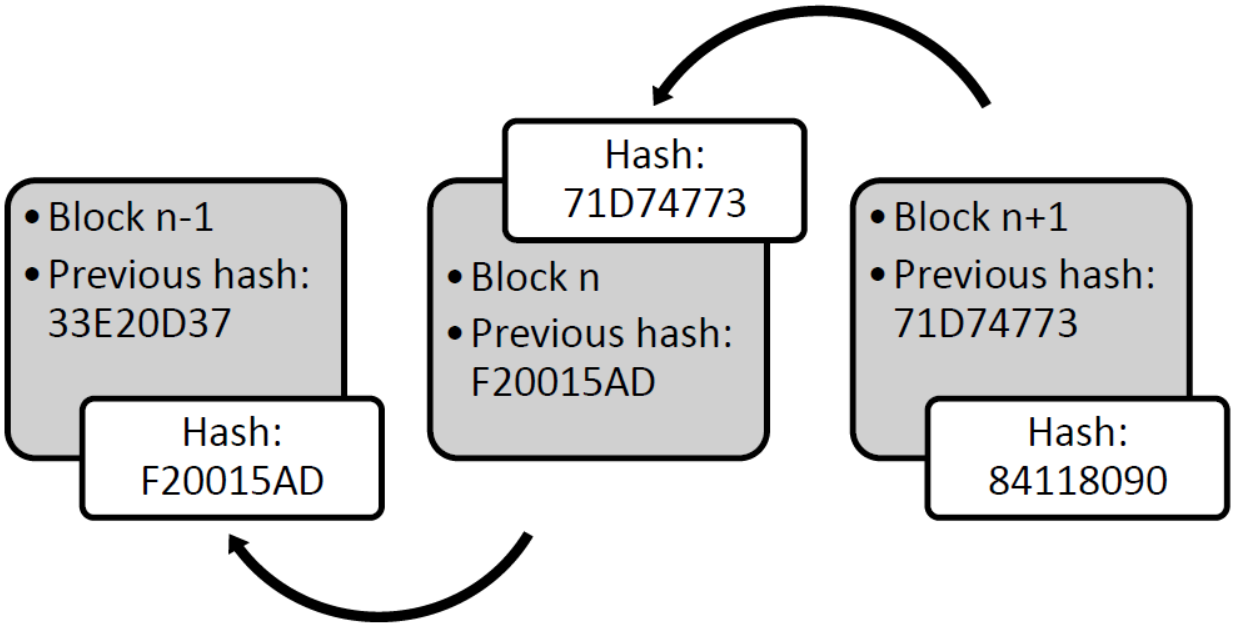
Il termine "blockchain ibrida" si riferisce a un tipo di blockchain che combina elementi di blockchain pubbliche e private. Alcune blockchain possono iniziare la loro esistenza come blockchain ibride per una serie di ragioni, ma alla fine possono trasformarsi in blockchain pubbliche completamente decentralizzate e autogestite. Cardano. CDF è l'acronimo di "Cardano Development Flow".

Secondo la relazione tecnica di Oliver Kattwinkel e Michael Rademacher (Kattwinkel & Rademacher, 2020), "una blockchain non è una tecnologia rivoluzionaria, ma piuttosto una

combinazione intelligente di tre campi: crittografia, decentralizzazione e teoria dei giochi". Di conseguenza, per comprendere il funzionamento di una blockchain, è necessario comprendere le basi di come la crittografia, la decentralizzazione e la teoria dei giochi vengono utilizzate in una tecnologia blockchain. Questo capitolo si concentrerà sui componenti fondamentali che sono essenziali per il funzionamento di quell'insieme più complicato che è la blockchain.

Come si può vedere nella Figura 1, ogni singolo blocco che compone la blockchain ha un hash crittografico memorizzato nell'intestazione del blocco. Questo hash punta all'intestazione del blocco precedente. In questo modo è possibile collegare completamente la blockchain dal blocco più recente fino al primo blocco della catena, noto anche come "genesis block".

Figura 1. Esempio di Blockchain semplificata

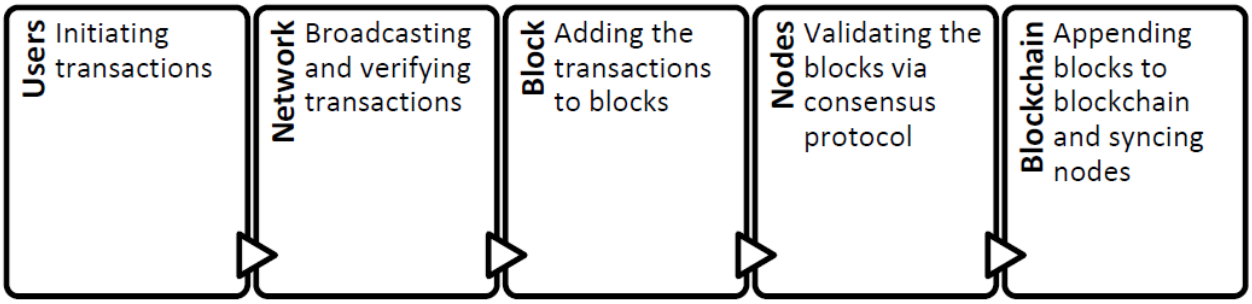



L'immutabilità dei dati conservati nella blockchain è garantita da questa particolare implementazione di un'architettura a liste collegate hash. Se un blocco venisse manipolato nel mezzo della catena, l'hash dell'intestazione verrebbe modificato, compromettendo così l'integrità dell'intero elenco collegato di hash. Per modificare le informazioni contenute in una blockchain, bisogna prima modificare tutti i blocchi successivi e poi far convalidare queste modifiche dalla rete.

Il processo di modifica dei dati non è particolarmente difficile, ma la loro convalida attraverso il consenso può essere piuttosto impegnativa. Per poter convalidare questi blocchi manomessi, in genere è necessario controllare oltre il cinquanta per cento della rete blockchain. Ciò è necessario affinché la convalida possa essere concordata tramite l'algoritmo di consenso. (Attacco al 51%)

In generale, si può pensare che un flusso di lavoro blockchain abbia cinque fasi: la prima fase è l'avvio delle transazioni, la seconda fase è la trasmissione e la verifica di tali transazioni nella rete, la terza fase è la creazione di blocchi che includono le transazioni, la quarta fase è la convalida del blocco (ad esempio, il mining) e la quinta fase è l'aggiunta di questi blocchi alla blockchain e la sincronizzazione dei nodi.

Figura 2. Esempio di flusso di lavoro Blockchain (Liu, et al., 2019)




Nella maggior parte dei casi, un programma di portafoglio, che può essere un "full-node" o un "light-node", è quello che gestisce le transazioni e la trasmissione. Il termine "full-node wallet" si riferisce a un portafoglio che memorizza una copia completa della blockchain e di conseguenza può essere di dimensioni piuttosto grandi. Anche il processo di sincronizzazione può richiedere del tempo, soprattutto al primo avvio del portafoglio. È anche una buona idea utilizzare un portafoglio light-node che, in sostanza, ha tutte le stesse funzionalità di un portafoglio full-node, ma invece di conservare la copia completa della blockchain, conserva solo le copie delle intestazioni dei blocchi. Il risultato è un portafoglio molto più compatto e con una velocità di sincronizzazione molto più elevata. (Wallets)

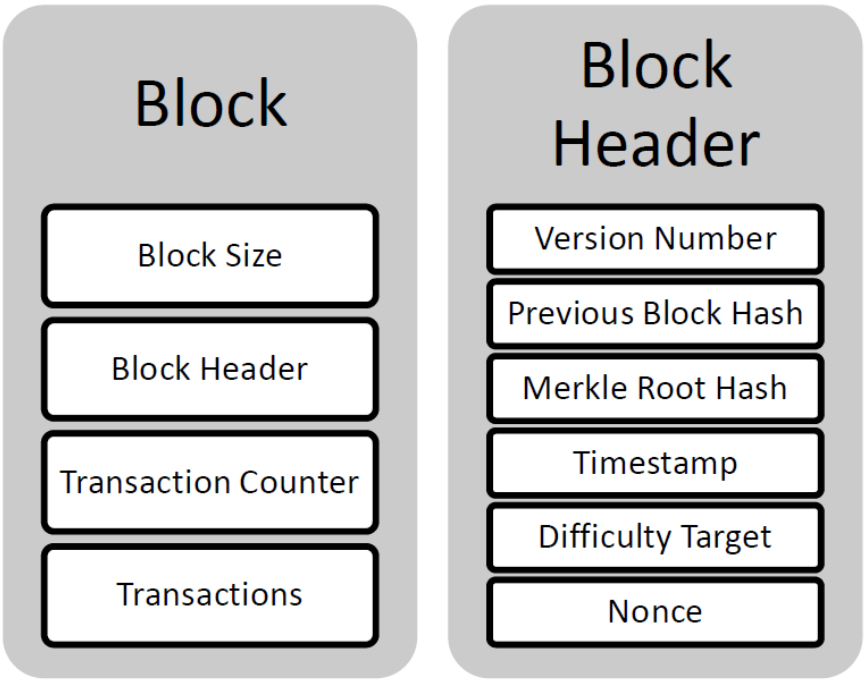
Dopo che la rete ha confermato la legittimità della transazione, questa viene aggiunta a un blocco. Dopo la creazione del blocco, la rete inizia a convalidarlo utilizzando un protocollo di consenso,

che nel caso di un sistema Proof-of-Work (PoW), come Bitcoin o Ethereum, potrebbe essere il mining. Una volta che la rete avrà completato questo processo, il blocco sarà considerato valido. I metodi per raggiungere il consenso sono trattati nel paragrafo 2.3.

### 2.1 Struttura dei blocchi

Dopo aver parlato dei componenti che i blocchi contengono e del ruolo che svolgono nella blockchain, qui di seguito viene approfondito che cos'è un blocco Bitcoin e le informazioni che specificamente memorizza.

Figura 3. Esempio di struttura a blocchi (O'Reilly Media, Inc., 2014)




Di seguito è riportata una sintesi del contenuto del blocco:

- La dimensione del blocco, misurata in byte
- L'intestazione del blocco sotto forma di hash
- Il numero totale di transazioni incluse nel blocco
- Le transazioni specifiche che sono incorporate nel blocco

Una sinossi delle informazioni contenute nell'intestazione del blocco:

- Il numero della versione più recente del protocollo
- Un riferimento all'hash del blocco precedente
- Hash della radice Merkle delle transazioni contenute nei blocchi
- La durata del tempo di creazione del blocco Unix.
- L'obiettivo di difficoltà utilizzato per la creazione di questo blocco nell'algoritmo proof-of-work.
- Nonce, il numero al quale è stato soddisfatto l'obiettivo di difficoltà dell'algoritmo PoW.

Nella sua forma più elementare, un blocco è costituito dai componenti qui descritti. Tuttavia, a seconda della piattaforma, un blocco può contenere una serie di altri tipi di dati oltre a quelli descritti nell'esempio. (O'Reilly Media, Inc., 2014)

### 2.2 Meccanismi di consenso

Un meccanismo di consenso adeguato è una necessità assoluta per le reti peer-to-peer che operano senza autorità centrale. Un meccanismo di consenso non è realmente necessario in un'architettura software più tradizionale, come quella in cui le funzionalità e gli archivi di dati sono mantenuti in un server centralizzato. Una blockchain, invece, ha bisogno di un meccanismo di consenso funzionante per garantire che ogni nodo abbia una copia della blockchain identica agli altri. Oltre al fatto che l'assenza di un meccanismo di consenso appropriato è una responsabilità per la blockchain, l'assenza di tale meccanismo impedisce alla blockchain di funzionare come previsto. Il meccanismo di consenso è un altro fattore che gioca un ruolo significativo nella sicurezza complessiva della blockchain.

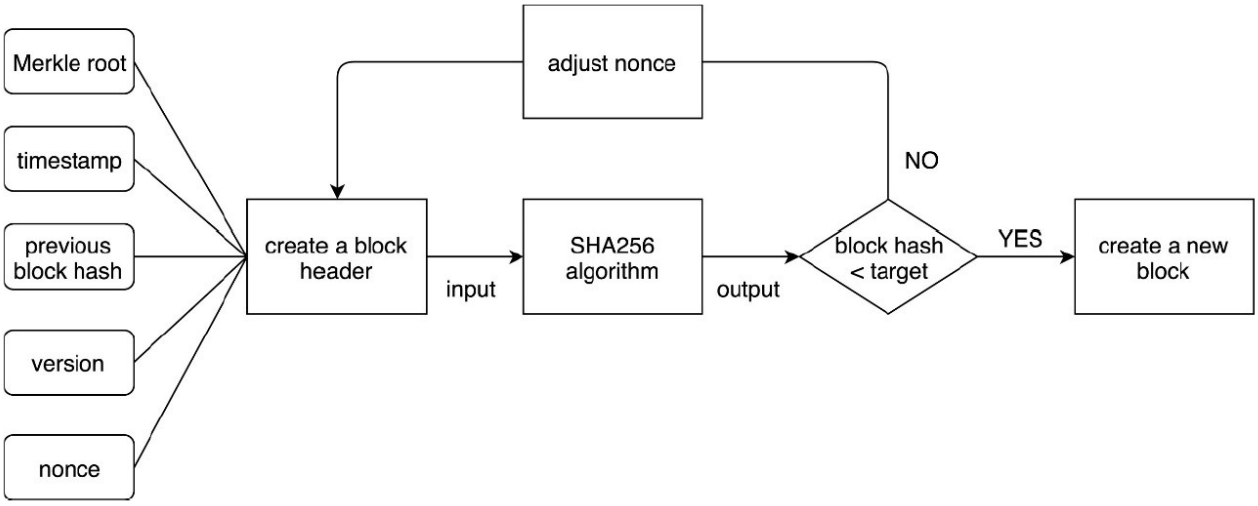
Innanzitutto, un meccanismo di consenso deve essere tollerante ai guasti bizantini. Ciò significa essenzialmente che i nodi devono essere in grado di raggiungere il consenso anche quando operano in un ambiente in cui non è possibile stabilire la fiducia. Ciò dà origine a una discussione sulla tolleranza di fronte ad attori malintenzionati. Quando il meccanismo di consenso di una blockchain è progettato per essere in grado di tollerare errori bizantini, ha anche la capacità di tollerare atti dolosi. Si può dire che la stragrande maggioranza dei meccanismi di consenso, compresi PoW e

PoS, sono considerati tolleranti al 50% di errori. Chiunque controlli più del cinquanta per cento della rete blockchain ha la capacità di centralizzarla e, di conseguenza, di intraprendere attività dannose come la doppia spesa. (Attacco al 51%) (Doppia spesa) (Zhang & Lee, 2019)

### 2.2.1 Proof-of-Work

Il meccanismo di consenso Proof-of-Work è stato il primo a essere utilizzato con Bitcoin; da allora sono state apportate alcune variazioni ai protocolli PoW, ma l'idea generale alla base è rimasta la stessa. Nei modelli Proof-of-Work, il raggiungimento del consenso avviene attraverso l'utilizzo della potenza di calcolo. I nodi lavoratori, noti anche come minatori, partecipano a uno dei diversi tipi di gare, una delle quali richiede a ciascun nodo lavoratore di risolvere un puzzle crittografico. Il primo che riuscirà a trovare la soluzione al rompicapo sarà colui che aggiungerà un nuovo blocco alla blockchain e riceverà di conseguenza una ricompensa in blocchi. Il termine "mining" deriva da questa attività. Nei modelli Proof-of-Work, il livello di difficoltà dell'enigma viene regolato proporzionalmente alla crescita della blockchain e del numero di nodi. Ad esempio, poiché Bitcoin è stato progettato per generare un nuovo blocco ogni dieci minuti circa, la difficoltà del mining di un blocco viene regolata per garantire il mantenimento di questo intervallo di tempo. Vediamo il flusso di processo semplificato della figura 4 per un meccanismo Bitcoin proof-of-work.

Figura 4. Esempio di prova di lavoro (Zhang & Lee, 2019)

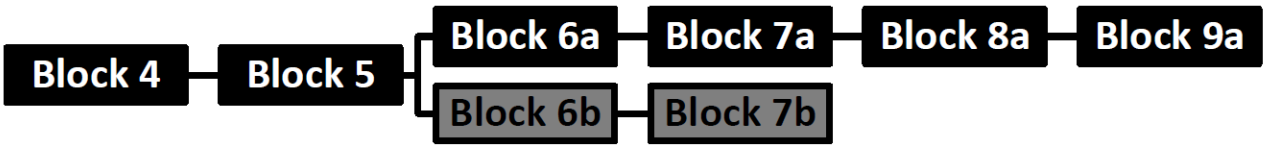


Per cominciare, vengono raccolti i metadati necessari per l'intestazione del blocco, ed è importante notare che in questi dati è incluso anche un nonce. Il termine "nonce" deriva dal fatto che un nonce è un numero casuale che viene utilizzato una sola volta. Nella maggior parte dei casi, il livello di difficoltà target per il blocco corrente è incluso anche nell'intestazione del blocco stesso. In Bitcoin, i dati vengono sottoposti a hashing con l'algoritmo SHA-256 una volta raccolte tutte le informazioni necessarie per l'intestazione del blocco. L'obiettivo di difficoltà, nel contesto di Bitcoin, si riferisce al numero minimo di zeri iniziali che un hash di blocco deve possedere per essere considerato convalidato. In altre parole, la prova di lavoro si considera completata quando sono stati effettuati tentativi sufficienti, utilizzando una varietà sufficiente di nonces, per garantire che l'hash del blocco inizi con il numero di zeri iniziali specificato nell'obiettivo di difficoltà. Quando ciò avviene, viene generato un nuovo blocco e aggiunto alla blockchain. Chi risolve questo rompicapo per primo riceve una ricompensa in blocco sotto forma di una cosiddetta transazione su Coinbase. Una transazione su Coinbase è una transazione in cui non ci sono input e l'unico output è la quantità di bitcoin che viene creata come ricompensa del blocco.

Ora, poiché l'architettura di una rete blockchain è decentralizzata, può capitare che le copie dei nodi della blockchain non siano uguali. Questa discrepanza può verificarsi di tanto in tanto. Ciò potrebbe causare un fenomeno noto come "biforcazione". Quando due minatori risolvono il puzzle PoW quasi contemporaneamente, si parla di "forking". Di conseguenza, la blockchain si divide in due catene separate, ciascuna delle quali contiene due blocchi candidati che potrebbero estendere la catena principale. I minatori scopriranno i nuovi blocchi biforcati in tempi diversi, a seconda della distanza topologica dal propagatore del blocco candidato. Di conseguenza, i diversi minatori inizieranno a estrarre su blocchi diversi quando vengono trovati i nuovi blocchi biforcati. Poiché il protocollo Proof-of-Work è progettato per funzionare in modo tale che i minatori preferiscano sempre la catena cumulativamente più difficile o, per dirla in altro modo, la catena più lunga, qualunque di questi blocchi biforcati venga esteso per primo, alla fine diventerà la catena principale. I blocchi rimanenti saranno chiamati "blocchi stantii". La biforcazione è un evento che si verifica molto raramente sulle principali blockchain e, quando si verifica, viene quasi sempre risolto in un unico periodo di blocco.

L'evento illustrato nella Figura 5 è un caso di biforcazione che si è verificato quando i blocchi 6a e 6b sono stati estratti contemporaneamente. I blocchi 7a e 7b sono stati aggiunti alla catena dopo che questa era stata estesa ancora una volta, ma il blocco 8a è stato estratto prima che potesse essere scoperto un blocco 8b. La rete è giunta alla conclusione che la "catena a" sarà la catena principale perché è la catena più lunga e quella cumulativamente più difficile. La "catena b" verrà gettata via.

Figura 5. Esempio di biforcazione della blockchain (Zhang & Lee, 2019)




Per quanto riguarda gli incidenti di biforcazione e le ricompense dei blocchi, è importante ricordare che le blockchain hanno in genere una quantità predeterminata di tempo contato in blocchi prima che le ricompense vengano distribuite. Ad esempio, Bitcoin impone un periodo di attesa di cento blocchi prima di permettere alle monete ricompensate di essere spese prima di essere considerate mature. Le ricompense per i blocchi obsoleti saranno rimosse.

Dopo aver trattato l'argomento della biforcazione involontaria della blockchain, passiamo alla biforcazione intenzionale, nota anche come "hard-fork" o "soft-fork". Questo tipo di biforcazione può essere utilizzato, ad esempio, per aggiornare o potenziare il protocollo della blockchain. La biforcazione può anche avvenire in modo accidentale. Nei capitoli successivi approfondiremo l'argomento degli hard fork. (O'Reilly Media, Inc, 2014) (Zhang & Lee, 2019)

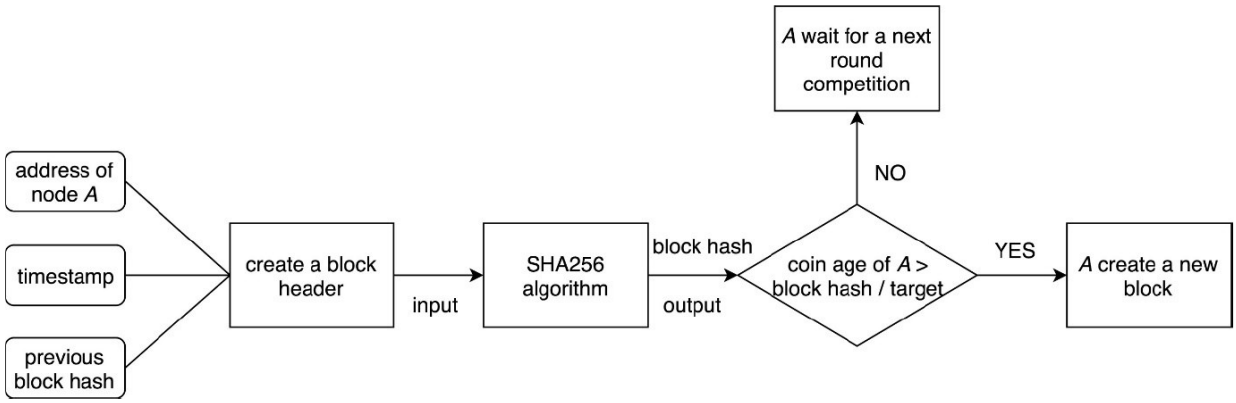
### 2.2.2 Proof-of-Stake

Come abbiamo scoperto nel capitolo precedente, i protocolli Proof-of-Work (PoW) ottengono il consenso attraverso l'uso della potenza di calcolo. Questi protocolli sono stati oggetto di critiche diffuse a causa del potenziale consumo di enormi quantità di energia, in particolare per le principali criptovalute come Bitcoin ed Ethereum. I protocolli PoS (Proof-of-Stake), invece, utilizzano un metodo diverso per raggiungere il consenso. Poiché non è necessario regolare e trovare un nonce

che corrisponda all'obiettivo di difficoltà, non è nemmeno necessario utilizzare una quantità eccessiva di potenza di calcolo, il che si traduce in una significativa riduzione della quantità di energia consumata. Il protocollo Proof of Stake (PoS) si avvale di un metodo per utilizzare le criptovalute che un utente ha scelto di puntare nel sistema. Maggiore è la quantità di denaro scommessa, maggiori sono le ricompense.

Come si può vedere nella Figura 6, il processo fondamentale di generazione di un nuovo blocco si attiene a una serie di regole molto simili tra loro. La differenza principale sta nel modo in cui i nodi raggiungono il consenso. Nei sistemi point-of-sale (PoS), esiste una variabile nota come "età della moneta". L'età delle monete viene determinata moltiplicando il numero totale di monete puntate per il tempo di puntata. A titolo di esempio, l'età della moneta sarà di cinquanta anni se si puntano cinque monete per un periodo di dieci giorni. L'età di ogni moneta viene azzerata ogni volta che un nodo genera un nuovo blocco. (Zhang & Lee, 2019)

Figura 6. Esempio di prova d'acquisto (Zhang & Lee, 2019)




### 2.2.3 Efficienza energetica

Discutendo i protocolli di consenso Proof-of-Work e Proof-of-Stake, siamo giunti alla conclusione che i sistemi Proof-of-Stake sono significativamente più efficienti dal punto di vista energetico rispetto ai sistemi Proof-of-Work. Tuttavia, esistono alcuni modi per ridurre la quantità di energia necessaria al PoW. Ad esempio, i minatori di Bitcoin si affidano a dispositivi denominati "ASIC" (Application-Specific Intergrated Circuit). Queste macchine sono progettate da zero per svolgere

un'unica funzione specifica: la risoluzione degli algoritmi Bitcoin. Una semplice CPU o GPU da tavolo non sarebbe mai in grado di completare il compito di provare diversi nonces allo scopo di creare un blocco con la stessa rapidità degli ASIC utilizzati in Bitcoin. Per questo motivo, Bitcoin ha un consumo energetico estremamente elevato. D'altra parte, poiché alcune piattaforme desiderano utilizzare il proof-of-work per una serie di motivi, i moderni algoritmi di proof-of-work sono progettati per essere resistenti agli ASIC. Ciò indica che l'algoritmo Proof-of-Work non funzionerà correttamente se si cerca di risolverlo con gli ASIC. Le monete resistenti agli ASIC, come Ethereum, vengono quindi minate con le GPU e questo ha portato a un fenomeno piuttosto inaspettato: le moderne GPU sono esaurite quasi ovunque, in tutto il mondo. Ciò è dovuto al fatto che i minatori hanno utilizzato le GPU per minare monete resistenti agli ASIC come Ethereum.

L'algoritmo Proof-of-Work (PoW) di per sé può avere un impatto significativo sulla quantità di energia richiesta dal protocollo di consenso e le varie criptovalute che utilizzano PoW hanno implementato una varietà di algoritmi PoW diversi. Non deve sorprendere che la crescente popolarità delle criptovalute abbia un impatto significativo sulla quantità di energia consumata.

Confrontiamo il consumo energetico del protocollo Ouroboros di Cardano con quello del PoW di Bitcoin. A gennaio 2022, il PoW di Bitcoin potrebbe consumare fino a 200.000 GWh/anno, mentre Ouroboros consumerebbe solo 15 MWh/anno. Questo confronto contribuirà a rendere più chiara la distinzione tra il consumo energetico di PoS e PoW. In questo scenario, PoS sarebbe 13.300.000.000 di volte più efficiente in termini di consumo energetico. Questo non solo si traduce in un minor consumo di energia, ma ha anche un impatto sulle commissioni associate alla conduzione delle transazioni. A titolo di esempio, consideriamo Ethereum e Cardano, entrambe piattaforme per la gestione di smart contracts; tuttavia, Ethereum utilizza un sistema proof-of-work, mentre Cardano utilizza un sistema proof-of-stake. (Figura 7) (Tardi, 2021) (Costello, 2020)

Figura 7. Confronto delle commissioni di Ethereum e Cardano (Messari: Asset Screener, 2022)

| Platform | Median Transaction Volume (USD) | Median Fee (USD) |
|---|---|---|
| Ethereum (PoW) | 324,35 | 18,43 |
| Cardano (PoS) | 348,53 | 0,203 |

Possiamo chiaramente notare che i volumi delle transazioni sono simili, ma l'ammontare delle commissioni pagate su entrambe le piattaforme è radicalmente ineguale. Questo è uno dei motivi per cui Ethereum sta progettando di aggiornare l'intera piattaforma al protocollo PoS.

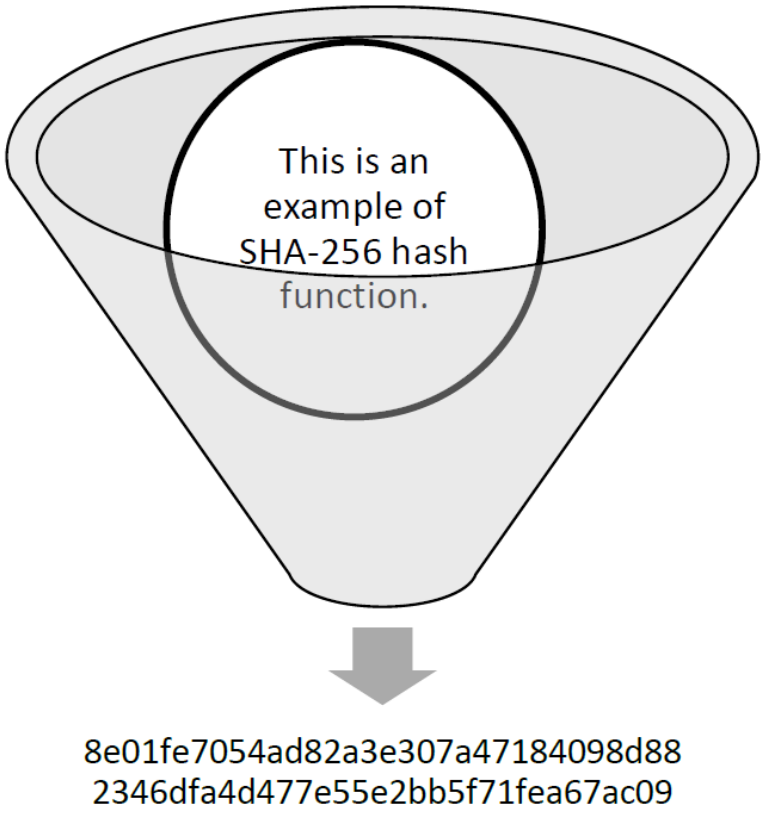
## 2.3 Crittografia nella Blockchain

A causa dell'uso diffuso della crittografia nella tecnologia blockchain, il termine "criptovaluta" è diventato sempre più popolare. Per garantire l'immutabilità, la sicurezza, l'integrità e la provenienza dei dati contenuti nella blockchain, vengono utilizzati metodi crittografici. Le funzioni di hash e gli algoritmi asimmetrici sono i due tipi di algoritmi crittografici più utilizzati nelle blockchain.

### 2.3.1 Funzioni Hash

Uno degli aspetti più importanti di un sistema blockchain è la presenza di funzioni hash crittografiche. Qualsiasi dato di dimensioni arbitrarie può essere compresso in un valore hash di dimensioni predeterminate utilizzando le funzioni hash. È possibile pensare alle funzioni hash come a funzioni unidirezionali, poiché è matematicamente impossibile annullare il processo di hashing una volta eseguito. Ciò significa che le funzioni hash rendono molto efficace la compressione dei dati. Esistono diversi algoritmi di hash che possono essere utilizzati nella tecnologia blockchain. Ad esempio, Bitcoin si affida in larga misura a SHA-256, noto anche come Secure Hash Algorithm, che fa parte della famiglia SHA-2. La National Security Agency (NSA) degli Stati Uniti d'America ha sviluppato SHA-2 nel 2001. L'algoritmo SHA-256 riduce i dati a un hash di 256 bit, come suggerisce il nome. Keccak-256, utilizzato da Ethereum, e BLAKE2, utilizzato da Cardano, sono solo due esempi dei diversi algoritmi di hash utilizzati dalle principali criptovalute.

Figura 8. Esempio di funzione di hash SHA-256




Le funzioni di hash sono i metodi crittografici più utilizzati nella tecnologia blockchain. Queste funzioni vengono utilizzate per una serie di scopi, tra cui l'hashing di dati come le intestazioni dei blocchi e gli alberi di merkle, la generazione di chiavi pubbliche e indirizzi, la verifica delle transazioni e il contributo agli algoritmi utilizzati dai protocolli di consenso. (Turner, 2019)

### 2.3.2 Crittografia a chiave pubblica

La crittografia asimmetrica o a chiave pubblica fa uso di coppie di chiavi costituite da chiavi private e pubbliche. Queste coppie di chiavi possono essere utilizzate per l'autenticazione oltre che per mantenere la riservatezza; tuttavia, la chiave privata deve essere protetta dall'accesso non autorizzato, mentre la chiave pubblica può essere distribuita a chiunque, indipendentemente dal suo

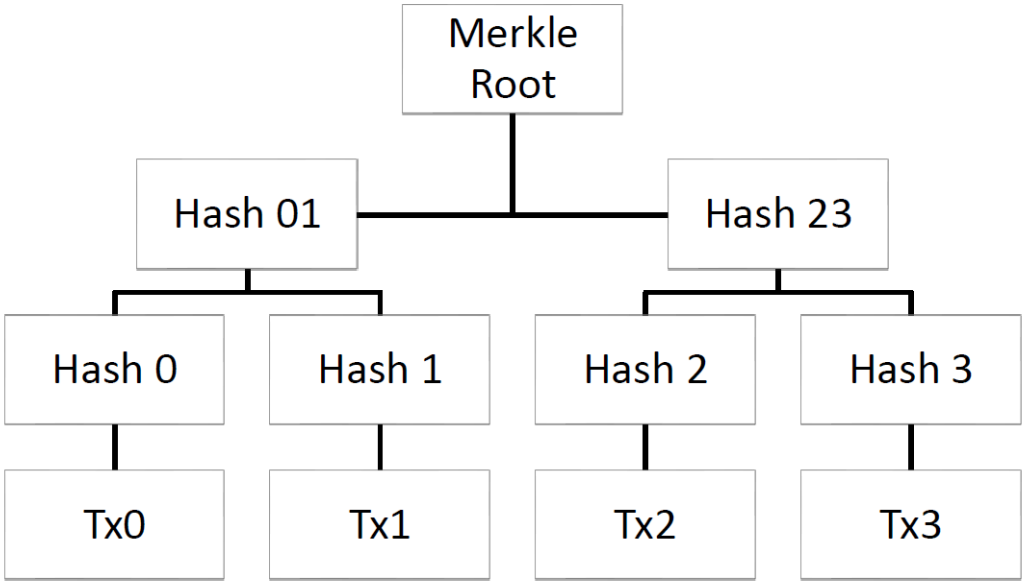
livello di affidabilità. L'uso di un algoritmo asimmetrico, ad esempio, si ritrova nelle firme digitali e nella crittografia e decrittografia dei dati.

Per semplificare, in una blockchain, le chiavi private sono utilizzate per autenticare le transazioni in uscita con una firma digitale, mentre le chiavi pubbliche sono utilizzate come indirizzi delle persone che ricevono denaro dalla blockchain. Poiché ogni transazione è firmata digitalmente con una chiave privata, è praticamente impossibile commettere frodi modificando una transazione o apparendo come qualcun altro, a condizione che la chiave privata sia tenuta al sicuro. Questo perché ogni transazione è firmata digitalmente con una chiave privata. (Poston, 2021)

### 2.3.3 Albero di Merkle

Come si è detto, le transazioni sono salvate in blocchi; tuttavia, per fornire informazioni più specifiche, va notato che le transazioni sono in realtà salvate in una struttura ad albero di Merkle all'interno del blocco, e solo la radice di Merkle è salvata nell'intestazione del blocco. Poiché viene salvato solo l'hash della radice dell'albero delle transazioni, questa struttura di dati consente ai blocchi di avere una dimensione complessiva inferiore. Oltre a garantire l'integrità dei dati per le transazioni, questa struttura fornisce anche un metodo rapido ed efficiente per la verifica delle transazioni. Gli alberi di Merkle possono essere concettualizzati allo stesso modo delle blockchain, in quanto sono entrambi elenchi collegati con hash. Tuttavia, a differenza delle blockchain, le Merkle Trees consentono agli utenti di convalidare le transazioni utilizzando solo un singolo ramo, anziché richiedere il download dell'intero albero (101 Distributed Ledgers, 2020).

Figura 9. Esempio di semplice albero di Merkle (Liu, et al., 2019)

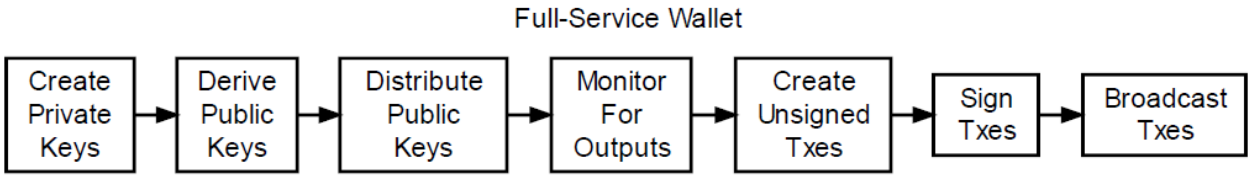


Esistono alcune varianti dell'albero di Merkle che si possono trovare nelle blockchain. Ad esempio, Ethereum utilizza il cosiddetto Albero di Merkle Patricia, che ha una struttura un po' più complicata.

## 2.4 Wallets

La funzionalità di Wallet può essere suddivisa in tre funzioni principali: distribuzione della chiave pubblica, firma e trasmissione in rete. Ciascuna di queste funzioni è descritta più avanti. È possibile che un singolo programma di wallet non supporti tutte queste funzioni, ma il wallet che esamineremo qui è un esempio di wallet a servizio completo.

Figura 10. Portafoglio a servizio completo



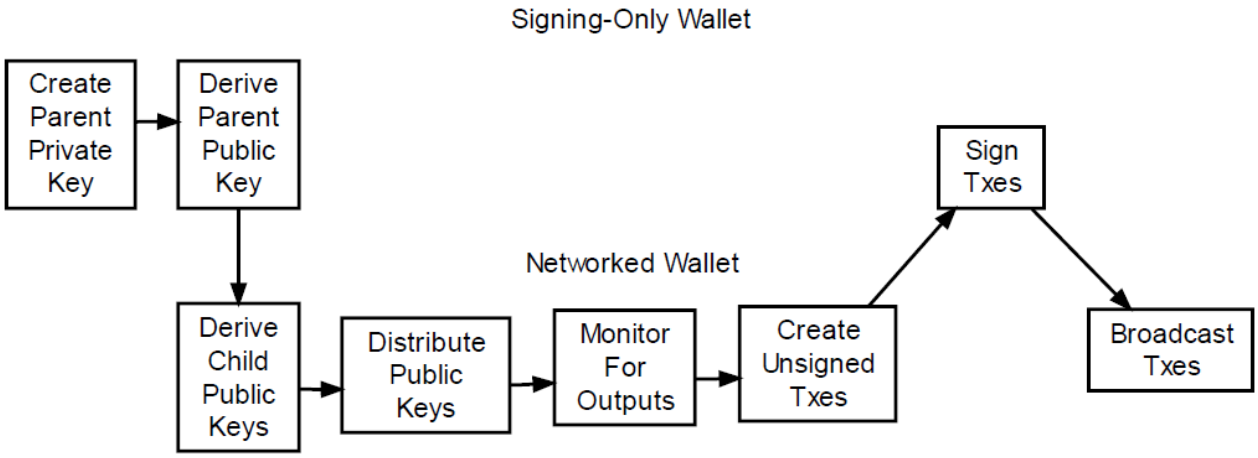

Un portafoglio full-service è in grado di eseguire i seguenti compiti: generare chiavi private, generare chiavi pubbliche basate sulle chiavi private, distribuire le chiavi pubbliche, controllare le uscite, generare transazioni non firmate, firmare le transazioni e trasmettere le transazioni firmate alla rete.

Si discute su quanto sia sicuro un portafoglio completo quando si tratta di memorizzare le chiavi private sul dispositivo stesso; tuttavia, questo aspetto è in genere gestito dal programma del portafoglio, che fornisce la crittografia dei file del portafoglio che contengono le chiavi private per ulteriori livelli di protezione.

Come accennato in precedenza, le funzioni del portafoglio possono essere suddivise in modo da essere gestite da programmi separati. Ad esempio, nel caso in cui si desideri una maggiore sicurezza per le chiavi private, è possibile generare e memorizzare le chiavi private in un portafoglio di sola

firma. Un portafoglio di sola firma genera una chiave privata madre e da questa ricava una chiave pubblica madre. Questa chiave pubblica genitore sarà utilizzata in un portafoglio in rete, che genererà una chiave pubblica figlio dalla chiave pubblica genitore. La chiave pubblica figlio gestirà tutte le funzionalità del portafoglio, ad eccezione della firma delle transazioni.

Figura 11. Portafoglio di sola firma




I portafogli offline, i portafogli hardware e i portafogli progettati esclusivamente per la distribuzione sono altri tre tipi comuni di portafogli. I portafogli offline, nonostante il nome, non sono ovviamente completamente operativi in modalità offline. Tuttavia, forniscono un ulteriore livello di sicurezza gestendo la generazione delle chiavi e la firma delle transazioni in modalità offline. Senza entrare troppo nei dettagli, si può convenire che un portafoglio offline offre un modo molto sicuro di gestire le transazioni, ma d'altra parte richiede un notevole impegno da parte dell'utente per completare i processi richiesti. Questo è un aspetto su cui si può concordare senza entrare troppo nei dettagli.

A differenza dei portafogli software, i portafogli hardware hanno la forma di dispositivi fisici, ma il loro funzionamento è fondamentalmente analogo a quello di un portafoglio di sola firma. Anche se offrono una maggiore sicurezza, i portafogli hardware rendono più difficile completare una transazione rispetto ai portafogli software.

I portafogli progettati al solo scopo di distribuire le chiavi pubbliche ad altri portafogli sono noti come portafogli "di sola distribuzione". I portafogli di questo tipo potrebbero essere utilizzati in ambienti con un livello di sicurezza inferiore.

### 2.5 Coppie di chiavi private e pubbliche e indirizzi

Le coppie di chiavi private-pubbliche sono uno degli aspetti fondamentali delle transazioni su blockchain. Queste coppie consentono agli utenti di firmare le transazioni e di inviare e ricevere denaro. Poiché quando si possiede la chiave privata si ha la completa proprietà e il controllo sui fondi associati a queste chiavi, a volte si parla di chiave segreta. Questo potrebbe essere un nome più appropriato rispetto all'uso più comune del termine "chiave privata".

Come si è detto nel capitolo precedente, i portafogli sono in genere responsabili della generazione delle coppie di chiavi private-pubbliche, nonché della gestione della firma e della trasmissione delle transazioni. Gli utenti dei portafogli nel mondo di oggi raramente hanno accesso diretto alle chiavi private stesse; piuttosto, ricevono una frase seme che funge da codifica per la chiave privata.

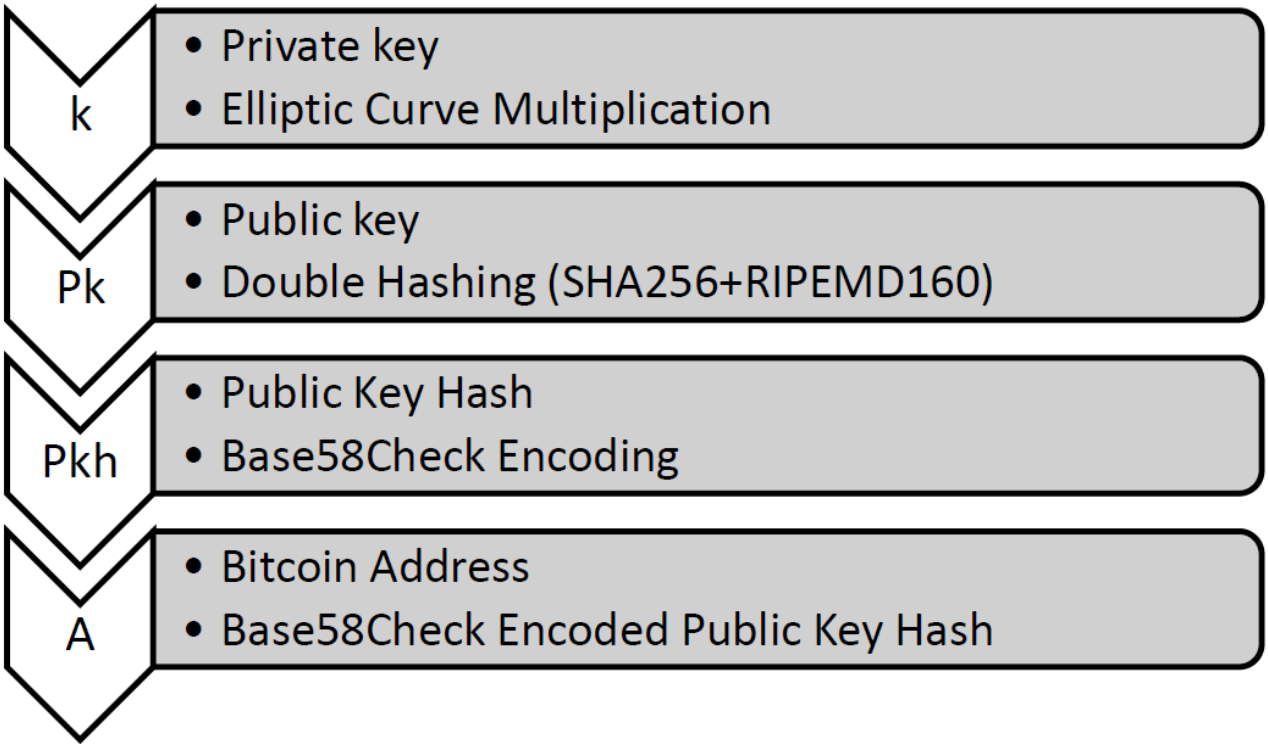
Per la criptovaluta Bitcoin, ad esempio, la chiave privata non è altro che un numero casuale a 256 bit. L'ECC viene utilizzato per eseguire un calcolo indecifrabile che ricava la chiave pubblica dalla chiave privata (Elliptic Curve Cryptography). L'algoritmo di firma digitale a curva ellittica (ECDSA) di Bitcoin utilizza parametri predefiniti definiti dallo standard "secp256k1" stabilito dal National Institute of Standards and Technology.

Il valore della chiave pubblica, indicato con "Pk", si ottiene moltiplicando il valore della chiave privata, indicato con "k", per il punto base della curva ellittica, indicato con "G".

$$Pk=k*G$$

In parole povere, la chiave pubblica può essere considerata come il numero del vostro conto corrente bancario, che dareste ad altre persone per ricevere pagamenti, mentre la chiave privata può essere usata per verificare i pagamenti che vengono inviati nel mondo. Tuttavia, in Bitcoin, la chiave pubblica viene ulteriormente codificata in un particolare indirizzo Bitcoin.

Figura 12. Coppia di chiavi e indirizzo Bitcoin (O'Reilly Media, Inc., 2014)




Come si evince dalle informazioni presentate in precedenza, la chiave pubblica di Bitcoin viene inizialmente sottoposta a hashing con l'algoritmo SHA256 e il risultato viene ulteriormente sottoposto a hashing con l'algoritmo RIPEMD160 prima di generare l'indirizzo finale di Bitcoin utilizzato per ricevere i fondi. Questo doppio hashing porta alla produzione dell'indirizzo bitcoin, anche se per comodità gli indirizzi bitcoin sono quasi sempre presentati nella loro forma codificata.

La codifica Base58Check aggiunge un prefisso di versione agli indirizzi ed è possibile determinare il tipo di indirizzo solo in base a questo prefisso. Esistono diversi tipi di indirizzi Bitcoin, ma i più comuni sono i seguenti:

- P2PKH (Pay-to-Pubkey Hash) Indirizzo, **prefisso 1**
    - Esempio: **1**7VZNX1SN5NtKa8UQFxwQbFeFc3iqRYhem
- P2SH (Pay-to-Script Hash) Indirizzo, **prefisso 3**
    - Esempio: **3**EktnHQD7RiAE6uzMj2ZifT9YgRrkSgzQX

L'indirizzo P2PKH è l'indirizzo legacy di bitcoin utilizzato per le transazioni, ma gli indirizzi P2SH sono utilizzati per ottenere un certo tipo di condizionalità nelle transazioni. Gli indirizzi P2SH sono utilizzati per ottenere un certo tipo di condizionalità nelle transazioni. Un indirizzo P2SH funziona come un indirizzo legacy, ma invece di puntare a una chiave pubblica, punta a uno script. Questo permette all'indirizzo di funzionare come un indirizzo legacy. Questo script è nascosto al mittente, ma è in grado di determinare che si tratta di un indirizzo P2SH in base al prefisso. 2014 pubblicazione di O'Reilly Media, Inc. (Documentazione per gli sviluppatori, portafogli, n.d.)

### 2.6 Transazioni

Le transazioni che avvengono su una blockchain sono paragonabili al battito cardiaco della rete. I restanti componenti della tecnologia blockchain lavorano insieme per garantire che le transazioni siano eseguite in modo legittimo e vengano aggiunte al libro mastro. Come abbiamo visto nei capitoli precedenti, la prima fase dei protocolli di consenso consiste nel raccogliere i dati che saranno memorizzati in un blocco prima di creare effettivamente il blocco. Questa fase avviene prima della creazione del blocco. Dopo che un utente ha creato una transazione ed entrambe le parti l'hanno firmata digitalmente, la transazione può essere trasmessa alla rete per essere elaborata. I nodi ricevono la transazione in diversi momenti e, non appena la ricevono, possono iniziare a convalidarla. La transazione arriverebbe a nodi diversi in tempi diversi. Una volta che la transazione è stata convalidata in quasi tutta la rete, viene aggiunta al blocco, che viene quindi creato e aggiunto alla blockchain. Successivamente, il blocco verrà aggiunto alla catena. Ora, se un nodo riceve un'altra transazione prima che la precedente sia stata convalidata in tutta la rete, la transazione in sospeso entrerà in un cosiddetto "mempool" per attendere come transazione non confermata. Questo processo avviene quando un nodo riceve più transazioni contemporaneamente. Il mempool è una componente essenziale del processo di transazione e un modo in cui può essere interpretato come indicatore della congestione della rete è una sorta di metro. (Wiesflecker, 2020) (Mempool, n.d.)

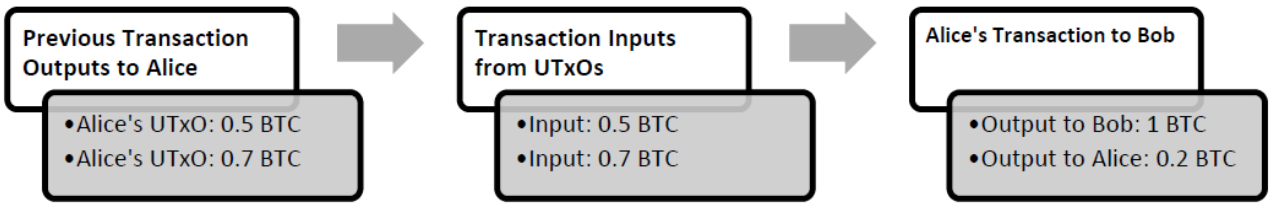
Il modello conto/bilancio e il modello UTxO sono i due tipi principali di modelli di transazione che si possono trovare nei sistemi basati su blockchain. I modelli basati sul conto, utilizzati da Ethereum, sono paragonabili a quelli che le persone sono abituate a vedere nelle banche convenzionali. Il sistema blockchain è in grado di tenere traccia dei saldi dei conti degli utenti e,

quando questi effettuano delle transazioni, il sistema sposta i saldi degli utenti da un conto all'altro in base alla transazione. I modelli basati sugli UTxO, invece, si discostano dall'approccio convenzionale nel senso che, anziché tenere traccia dei saldi dei conti, il sistema tiene traccia degli UTxO; di conseguenza, le transazioni sono composte da entrate e uscite, e gli UTxO vengono spesi in base a queste categorie. Questo è un modo intelligente di registrare un libro mastro, anche se non è il metodo più intuitivo. Pubblicazione 2014 di O'Reilly Media, Inc. (Frankenfield, 2020)

### 2.6.1 Modello UTxO

L'Unspent Transaction Output, o UTxO in breve, è una funzionalità introdotta per la prima volta da Bitcoin e associata ai modelli basati sulle transazioni. Il modello UTxO utilizza gli output, denominati UTxO, come input e genera poi nuovi UTxO da questi input. Si tratta quindi di un ciclo di ingressi e uscite, e il saldo spendibile dell'utente è rappresentato dalle uscite che non sono state spese.

Figura 13. Esempio di UTxO




Per una migliore comprensione, dividiamo la Figura 13 in parti;

1. Alice ha ricevuto un totale di 1,2 Bitcoin in due uscite separate. Si tratta di due UTxO distinti, ciascuno del valore di 0,7 BTC e 0,5 BTC rispettivamente.
2. Alice desidera dare a Bob un bitcoin come pagamento. Utilizzerà entrambi gli UTxO come input della transazione, poiché gli UTxO valgono rispettivamente 0,5 BTC e 0,7 BTC.
3. Alice crea una transazione con due uscite, una delle quali invia 0,1 bitcoin ad Alice e l'altra invia 1 bitcoin a Bob.

4. A questo punto, Bob possiede un UTxO del valore di 1 BTC e Alice possiede un UTxO del valore di 0,2 BTC. Entrambi questi UTxO possono essere utilizzati come input nelle transazioni successive, se necessario.

Nota bene: in circostanze reali, ad Alice verrebbe richiesto di pagare alcune commissioni di transazione; ad esempio, la transazione verso Bob potrebbe creare uscite di 1 BTC per Bob e 0,19 BTC per Alice, con la differenza delle commissioni che sono state detratte dal saldo di Alice.

Ora, supponiamo che Alice possieda un UTxO del valore di cento BTC, ma che voglia inviare a Bob solo due BTC. L'intero UTxO del valore di 100 BTC verrebbe speso per un input di transazione, che produrrebbe un output di 2 BTC inviati a Bob e 98 BTC inviati ad Alice. Pertanto, gli UTxO non possono essere scomposti nelle loro parti componenti e devono essere utilizzati come un'unica entità. Successivamente, il "cambiamento" verrà ritrasmesso come UTxO più compatto.

Anche le transazioni che avvengono all'interno di una blockchain possono essere considerate come una catena a sé stante. Ogni transazione effettuata farà riferimento agli output ricevuti nella transazione precedente e ogni transazione includerà sia gli input che gli output. Il fatto che tutte le transazioni siano registrate nel libro mastro pubblico (la blockchain) e che la rete blockchain le convalidi e le confermi rende le transazioni trasparenti e irreversibili.

Anche se nella rete blockchain non ci sono transazioni fatte dall'utente che non richiedono input, la rete Bitcoin ha una cosa chiamata "Transazioni Coinbase", che sono essenzialmente le ricompense dei minatori e le monete che vengono generate dal sistema una volta creato un blocco. Le reti blockchain non consentono transazioni create dagli utenti senza input. Pubblicazione del 2014 di O'Reilly Media, Inc. (Bitcoin's UTxO Model, n.d.) (Documentazione per gli sviluppatori, transazioni, n.d) (Frankenfield, 2020)

### 2.6.2 Modello EUTxO

L'Extended Unspent Transaction Output, in breve eUTxO, è un modello innovativo ideato e creato dall'azienda IOG, responsabile anche dello sviluppo del sistema blockchain Cardano. Il concetto iniziale era quello di combinare il modello UTxO utilizzato da Bitcoin con la capacità degli smart

contracts offerti da Ethereum. Il modello UTxO presenta una serie di vantaggi, tra cui una buona scalabilità, la privacy e un processo di verifica delle transazioni semplice; tuttavia, l'incompletezza del modello UTxO nella sua forma più elementare rappresenta uno svantaggio significativo. Nel campo dell'informatica, la capacità di un sistema di risolvere qualsiasi problema di calcolo, in genere attraverso l'uso di un linguaggio di programmazione, viene definita "completezza di Turing". La completezza di Turing è una forma abbreviata del termine. IOG voleva trovare un modo per mantenere i vantaggi del modello UTxO, pur avendo la flessibilità di gestire una varietà di attività più ampia rispetto alle sole transazioni di pagamento. Sono riusciti a estendere le capacità del modello UTxO consentendo agli UTxO di memorizzare dati arbitrari oltre ai fondi e alla logica sotto forma di script che controllano essenzialmente la validità della transazione. Questa è stata la chiave del loro successo. Se le condizioni dello script restituiscono il valore vero, la transazione può essere elaborata e le entrate possono essere spese.

Uno dei principali vantaggi dell'utilizzo di un modello UTxO esteso è che consente l'uso di smart contracts. Inoltre, cosa forse più importante, consente di prevedere con precisione le commissioni. (Sanchez, 2021) (Sanchez, 2021. -b) (Przybilla, 2021)

### 2.7 Sicurezza della Blockchain

Oltre a tutti i dettagli crittografici e tecnici che sono principalmente "codificati" nel sistema, la sicurezza di una blockchain dipende in larga misura dalla presenza di una rete P2P (peer-to-peer) sufficientemente grande, distribuita e funzionale. Come risultato di questi fattori, un numero significativo di grandi piattaforme sta lavorando per sviluppare i propri sistemi blockchain con la decentralizzazione come uno degli obiettivi principali dei propri sforzi. La blockchain sarà più vulnerabile a falle di sicurezza come l'attacco del 51% se viene implementata su sistemi più piccoli o non distribuiti. Se qualcuno controlla più della metà della rete, avrà di fatto il controllo completo della rete e potrà intraprendere una serie di attività subdole. È importante notare che questo problema riguarda principalmente solo le blockchain pubbliche.

### 2.7.1 Decentralizzazione

La decentralizzazione nelle blockchain può essere associata a molti aspetti diversi, che vanno dalla socioeconomia all'economia politica. Tuttavia, in termini di tecnologia, la decentralizzazione è molto importante perché permette di creare una rete veramente priva di fiducia, sicura e coerente. La presenza di una rete peer-to-peer veramente decentralizzata che gestisce e convalida le transazioni in un ambiente privo di fiducia rende possibile condurre transazioni di fondi e le cosiddette funzionalità di smart contract senza il coinvolgimento di terze parti che potrebbero interferire. Grazie a queste caratteristiche, le blockchain possono diventare una piattaforma valida per fornire alternative a una serie di funzioni sociali, come il voto digitale, le identità digitali, i sistemi finanziari e quindi l'attività bancaria per i non bancari, tra le altre funzioni sociali. Nei capitoli successivi, approfondiremo i casi d'uso e le applicazioni che verranno discusse.

### 2.7.2 Attacco al 51% del network

Uno scenario noto come attacco al 51% descrive una situazione in cui qualcuno ha ottenuto il controllo di più della metà della rete. Ipoteticamente, questo è possibile anche nelle reti più grandi; tuttavia, a titolo di esempio, in una rete blockchain che utilizza un algoritmo di consenso PoW (Proof-of-Work) che in ultima analisi richiede potenza di calcolo, o potenza di hashing per essere precisi, sarebbe necessario un supercomputer molto potente per rappresentare più del 50% della potenza di hashing della rete, il che è praticamente impossibile. D'altra parte, per convalidare le transazioni utilizzando una rete Proof-of-Stake (PoS), un utente deve possedere il 51% della criptovaluta che viene puntata, il che è estremamente costoso e difficile da acquisire. La piattaforma di Proof-of-Stake (PoS) Cardano ha più del settanta per cento dell'offerta totale di token, il che indica che nessuna borsa ha sufficiente liquidità per fornire più del cinquanta per cento dei token.

Un attacco riuscito al 51% può essere utilizzato per una serie di atti dolosi, come ad esempio ottenere il monopolio del mining in una rete PoW e impedire ad alcuni o a tutti gli altri utenti di effettuare il mining, ottenendo così tutti i guadagni derivanti dal mining. Un altro esempio di atto doloso che può essere compiuto utilizzando un attacco al 51% è il furto di tutte le ricompense

derivanti dal mining. Esiste anche la possibilità di manomissione dei blocchi, che può essere utilizzata nel processo di doppia spesa. (Attacco al 51%, 2021) (Frankenfield, 2021)

### 2.7.3 Doppia spesa

La pratica di spendere una criptovaluta più di una volta e poi manipolare la blockchain in modo tale da far sembrare che queste transazioni non abbiano mai avuto luogo viene definita doppia spesa. Questo tipo di eventi si sono verificati in passato e una delle forme di frode più dannose si è verificata nel maggio 2018, quando la criptovaluta nota come "Bitcoin Gold" è stata oggetto di un attacco del 51%. Gli autori sono riusciti a rubare oltre 18 milioni di dollari USA di Bitcoin Gold spendendo due volte in una serie di transazioni diverse nel corso di diversi giorni. (Frankenfield, 2020)

# Capitolo 3: Ethereum blockchain, Smart contracts e NFT

## 3.1 Introduzione

Ethereum è stato creato con l'intento di utilizzare la programmabilità per portare la tecnologia blockchain e le criptovalute a un livello superiore. Grazie al successo dell'implementazione degli smart contract nella piattaforma Ethereum, è iniziata una nuova era nella storia della tecnologia blockchain. Il fatto che Ethereum possa essere programmato ha incoraggiato un gran numero di sviluppatori a costruire su Ethereum. Le applicazioni decentralizzate, o dApp, che saranno al centro della nostra discussione nel capitolo 2.3 , comprenderanno un vasto assortimento di concetti lungimiranti supportati dalla blockchain di Ethereum. Le dApp costruite su Ethereum hanno incluso la "Finanza decentralizzata", nota anche come "DeFi", i "Token non fungibili" (NFT), le "DAO" o le "Organizzazioni autonome decentralizzate", nonché giochi e altre applicazioni.

Le commissioni di transazione associate a Ethereum sono significativamente più alte di quelle associate a un sistema blockchain Proof-of-Stake (come si è visto in precedenza nella Figura 7). Ciò è dovuto al fatto che tutte le dApp che girano su Ethereum generano un maggior numero di transazioni, che a loro volta richiedono il pagamento di commissioni aggiuntive e il completamento di ulteriori operazioni di mining. Non solo i costi potenziali associati alle commissioni, ma anche la quantità di energia consumata continua ad aumentare. Per il momento, il consumo energetico annuale di Ethereum può essere stimato fino a quasi 110 TWh nel gennaio 2022. Questa cifra si basa sulle proiezioni attuali. Gli sviluppatori di Ethereum sono consapevoli di questa situazione e hanno in programma un significativo aggiornamento da Ethereum a Ethereum 2.0.

L'introduzione di un nuovo algoritmo di consenso proof-of-stake nella rete sarebbe uno degli obiettivi principali di Ethereum 2.0. Questo algoritmo è potenzialmente in grado di aumentare le probabilità di successo di Ethereum. Questo algoritmo ha il potenziale di ridurre il consumo energetico complessivo della rete di circa il 99,95%. La transizione a una catena proof-of-stake già operativa, nota come "Beacon Chain", è prevista per la prima metà del 2022. (Blog della Fondazione Ethereum, 2021) (Energy Consumption, 2022) (Gulley, 2021) (Energy Consumption, 2022)

### 3.2 Smart Contracts

Come spiegato prima nel capitolo 1 i dati memorizzati in un blocco possono includere informazioni relative a vari aspetti, come chi, cosa, quando, dove, quanto o in quali condizioni i dati sono stati memorizzati. Gli smart contracts sono un'altra caratteristica che può essere inclusa in una blockchain. Si tratta di programmi informatici che hanno determinati parametri predefiniti e sono impostati per essere eseguiti quando tali parametri sono soddisfatti. Le capacità di una blockchain sono notevolmente migliorate dall'aggiunta degli smart contracts, grazie alla loro maggiore adattabilità e diversità.

Le applicazioni degli smart contracts sono molteplici e includono l'industria finanziaria, la sanità, le assicurazioni e qualsiasi altro campo in cui la fornitura di servizi deve essere in qualche modo condizionata dai risultati. I capitoli successivi trattano una serie di applicazioni, la maggior parte delle quali dipende dai contratti digitali per funzionare. Non deve sorprendere che gli smart contracts richiedano sempre un sistema blockchain in grado di supportare gli smart contracts come spina dorsale. Bitcoin, ad esempio, ha il potenziale per aggiungere condizionalità alle transazioni attraverso l'uso di script; tuttavia, Bitcoin è stato progettato fin dall'inizio per non essere "turing-completo". A differenza di Bitcoin, sia Ethereum che Cardano sono sistemi turing-completi.

Utilizzando gli smart contracts, si è in grado di generare ed elaborare contratti di qualsiasi livello di complessità senza la necessità che una terza parte intervenga nel processo. La natura intrigante degli smart contracts deriva dal fatto che possono offrire maggiori livelli di trasparenza. A titolo di esempio, è possibile stipulare un contratto con un'entità non identificata per scambiare un bene di valore con qualcos'altro. I fondi sono garantiti all'interno del contratto e vi rimarranno fino a quando la controparte non soddisferà l'obbligo di consegnare i beni come parte dell'accordo. È possibile trasmetterlo alla rete e convalidarlo se tutte le condizioni sono soddisfatte, compresa la verifica che i beni siano conformi a quanto stabilito nel contratto. In questo modo si garantisce che entrambe le parti ricevano i beni concordati. Ora, nel caso in cui la controparte del contratto non dovesse rispettare la propria parte dell'accordo, i fondi verrebbero sbloccati e rimborsati automaticamente dopo un periodo di tempo prestabilito. Non è necessario che le parti comunichino tra loro per avere la certezza che il contratto sarà rispettato. Poiché gli smart contracts sono essenzialmente solo pezzi di codice di programma scritti da una persona, è inevitabile che contengano errori. Tuttavia, le

piattaforme blockchain e il linguaggio di programmazione degli smart contract che le aziende scelgono di utilizzare possono avere un'influenza significativa sulla tolleranza agli errori.

Una rapida rassegna dei vantaggi degli smart contracts:

- Non è richiesto l'utilizzo di intermediari
- I documenti non vanno persi
- Sicurezza contro le intrusioni informatiche
- La procedura è rapida.
- Meno errori umani

(Rosic, 2020)

### 3.3 Token non fungibili (NFT)

I gettoni non fungibili, o in breve NFT, sono gettoni digitali che fanno parte di una rete blockchain e possono essere praticamente qualsiasi cosa digitale, dalle immagini alla musica e tutto il resto. Gli NFT possono essere creati praticamente con ogni bene digitale immaginabile. Poiché gli NFT non sono fungibili, il proprietario di un NFT ha la piena proprietà dell'asset sottostante, che non può essere replicato o falsificato in alcun modo. Ogni NFT ha una propria impronta digitale unica memorizzata in una rete blockchain, che può essere consultata per confermare la legittimità degli asset. Al momento, la maggior parte dei token non fungibili (NFT) nelle varie reti blockchain è costituita da opere d'arte digitale, che vengono scambiate e distribuite nella rete. In questo momento gli NFT possono essere paragonati a carte da collezione, alcune delle quali sono estremamente rare e altre no. Esistono diversi mercati per i token non fungibili (NFT), ognuno dei quali è specifico per una particolare rete blockchain.

Ci sono diversi fattori che possono influenzare la decisione di una persona di acquistare e detenere NFT. Il valore di alcuni token rari non fungibili (NFT) può aumentare nel tempo, rendendoli adatti all'uso come investimento o anche come forma di conservazione del valore a lungo termine. Alcuni tipi di NFT sono accompagnati da speciali iscrizioni che possono essere utilizzate in una serie di comunità riservate.

Come già accennato, la maggior parte degli NFT attualmente disponibili ha la forma di opere d'arte digitali e sono classificati come oggetti da collezione. Gli NFT, in realtà, possono essere utilizzati in diversi contesti, come identità digitali, passaporti, patenti di guida e così via. Oltre all'impronta digitale unica, gli NFT possono memorizzare metadati che possono essere applicati a diversi casi d'uso, come la creazione di licenze digitali di vario tipo. Gli NFT possono fungere da documenti di prova della proprietà di una serie di beni tangibili, tra cui immobili e veicoli. Gli NFT hanno un'altra qualità interessante: possono essere frazionati, il che crea la possibilità di possedere parti di qualcosa facilmente verificabili. Questo è solo uno dei tanti motivi per cui sono così attraenti. (Gettoni non fungibili (NFT), n.d.) (Clark, 2021) (Sharma, 2021)

### 3.3.1 Breve storia degli NFT

Quando si parla dello sviluppo dei NFT, è importante distinguere tra la nascita dell'idea concettuale e l'effettiva creazione del primo token non fungibile su una blockchain come atto materiale dell'invenzione. Nel 2012, cioè tre anni dopo la nascita dei Bitcoin e tre anni prima della nascita di Ethereum, quest'ultima la piattaforma open source che ospita il maggior volume di conio di NFT, è stato pubblicato un articolo scritto da Meni Rosenfield che introduceva il concetto di "Moneta colorata".

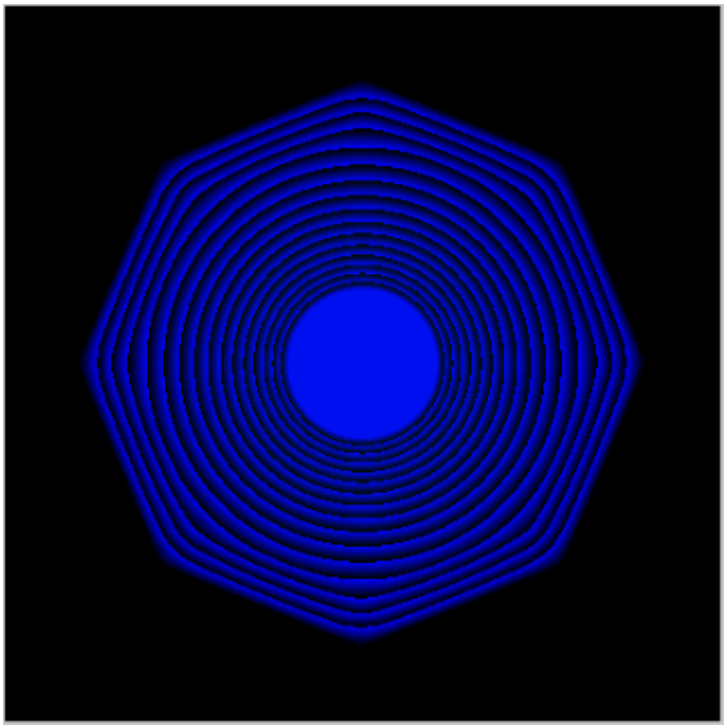
Questo documento è stata la prima pubblicazione di questo tipo. Questa idea è stata sviluppata in relazione alla blockchain utilizzata da Bitcoin ed è nata specificamente per superare alcuni tipi di problemi associati alle monete digitali definite "Fungible Tokens". I gettoni distinti l'uno dall'altro sono da intendersi sotto il termine "gettoni colorati". Il Bitcoin e le altre criptovalute sono definiti "gettoni fungibili" perché un bitcoin vale sempre lo stesso importo di un altro bitcoin, così come un euro è sempre equivalente a un euro. La creazione di risorse crittografiche uniche sarebbe l'obiettivo di Coloured Coin, e l'idea di "unicità", in cui ogni token è distinto dagli altri, è il principio fondamentale alla base dei token non fungibili (NFT).

È qui che il mondo crittografico inizia a porsi il problema di rendere "uniche" le risorse, ed è questo ragionamento che porterà alla nascita degli NFT. Anche se le limitazioni dovute alla blockchain di Bitcoin non hanno permesso lo sviluppo di questo progetto, le Coloured Coins rappresentano la

nascita concettuale delle NFT. Anche se lo sviluppo di questo progetto non è stato possibile a causa delle limitazioni della blockchain Bitcoin.

Il 3 maggio 2014, l'artista digitale Kevin McCoy conia fisicamente il primo token non fungibile nella storia del mondo. Utilizza la sua opera "Quantum", che viene coniata su una blockchain chiamata Namecoin e basata sul modello Bitcoin. L'opera è una rappresentazione digitale di un'immagine che consiste in un ottagono pixelato che cambia colore.

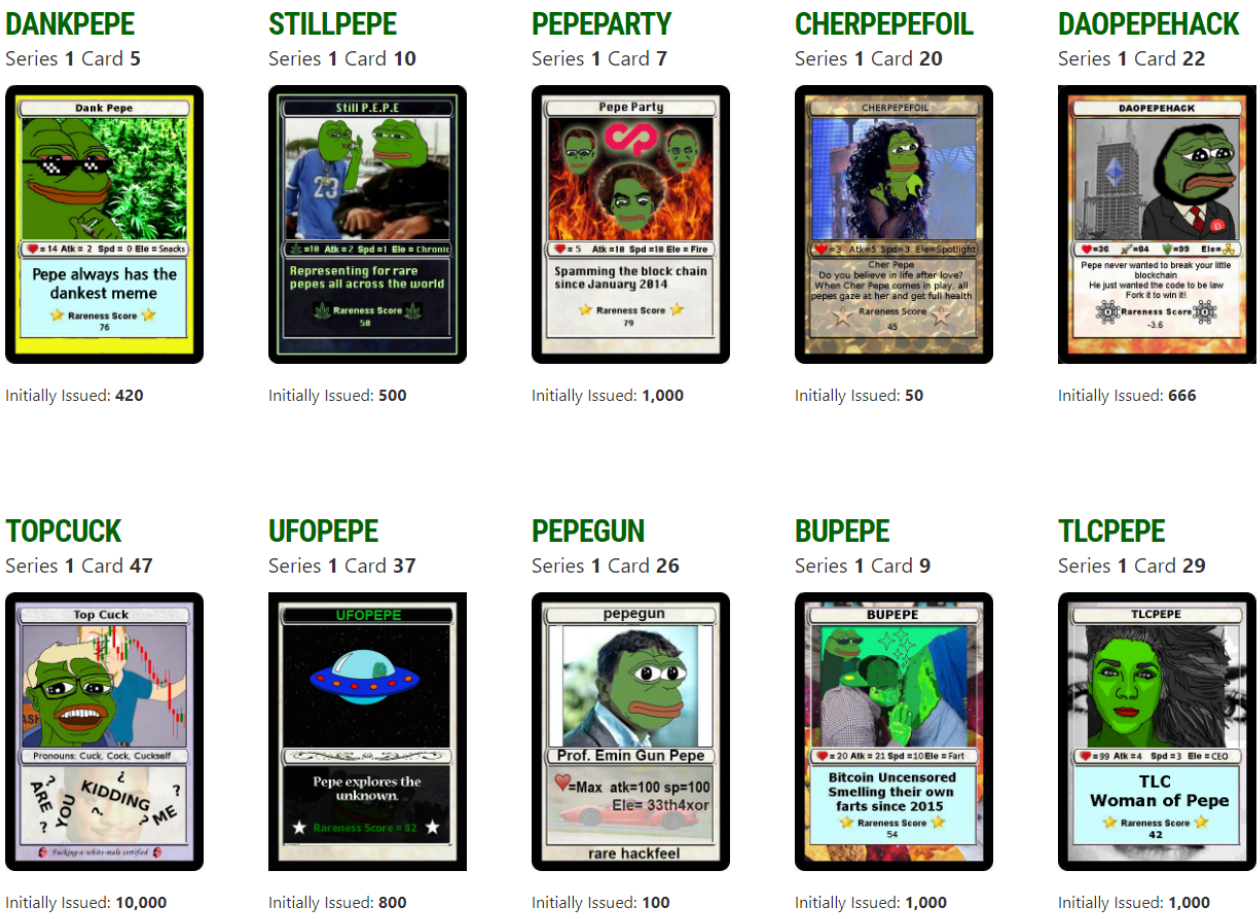
Figura 14. “Quantum” primo NFT mintato da Kevin McCoy



Dopo il completamento di Quantum, è iniziato il conio di una serie di NFT e per facilitare questo processo è stata creata la piattaforma Counterparty, un protocollo che opera sulla blockchain di Bitcoin. Questa piattaforma ha ospitato le varie collezioni di NFT di Rare Pepes nel 2015. A causa dei vincoli imposti dall'infrastruttura di base del Bitcoin, tuttavia, il mercato delle valute non-flat si è spostato su Ethereum, una piattaforma introdotta per la prima volta nel 2015. L'implementazione di Ethereum nel 2017 ha segnato una svolta significativa per i token non fungibili (NFT), in quanto ha stabilito che Ethereum è il leader indiscusso degli NFT.

Il 2015 ha segnato l'inizio dell'era dei Rare Pepes, che sono i precursori dei moderni PFP. Si tratta delle immagini seriali che hanno reso NFT famosa come CryptoPunk o Bored Ape Yacht Club (BAYC). Le Rare Pepes sono gettoni non fungibili emessi sotto forma di carte commerciali, che sono essenzialmente carte da collezione costruite inizialmente su Counterparty. Ci sono un totale di 1.774 risorse distribuite in 36 serie diverse, e tutti i soggetti delle serie sono basati su "Pepe" la rana, un personaggio che ha fatto il suo debutto nel 2005 nel fumetto intitolato Boy's Club.

Figura 15. Esempio di Rare Pepes




Nel 2021, tuttavia, quando gli NFT erano all'apice della popolarità, questi asset furono spostati su Ethereum utilizzando il protocollo Emblem Vault, in modo da poter essere venduti sulla piattaforma Open Sea per cifre esorbitanti. Il 2021 è stato anche l'anno di lancio di Ethereum.

Una delle principali differenze tra i PFP**,** come i CryptoPunk e i BAYC, ed i Rare Apes è che i primi sono espressione di arte generativa, mentre i secondi sono realizzati con Photoshop. Ovvero, nei Rare Apes ogni immagine è stata creata con Photoshop singolarmente. Gli PFP, invece, sono generati da un algoritmo, in cui l'artista crea i singoli elementi e poi un software li assembla, generando casualmente varianti di NFT. Ciò contrasta con il processo utilizzato per creare Rare Apes, in cui ogni immagine è stata creata individualmente in Photoshop.

Figura 16. Esempio di arte PFP (Bored Ape Yatch Club NFTs)

In conclusione, il 2021 è stato l'anno degli NFT. È stato l'anno in cui il volume degli scambi ha raggiunto picchi estremamente elevati, con esempi di artisti digitali venduti per milioni di dollari, come Beeple e Pak. La partecipazione di importanti case d'asta come Sotheby's e Christie's, che ora sono anche responsabili della gestione delle aste di NFT, è uno dei fattori che ha contribuito alla recente crescita del mercato dei token non fungibili. Anche la tecnologia alla base degli asset

crittografici è progredita nel corso del tempo. Un esempio è The Merge di Pak, un'immagine che è stata suddivisa in migliaia di NFT. Se un proprietario possiede più di un asset, gli NFT si combinano automaticamente in un singolo gettone non fungibile più grande. (Chi ha inventato gli NFT (Non Fungible Token)?, 2022)

# Capitolo 4: Possibili applicazioni

## 4.1 Web 3.0

Il termine "Web 3.0" si riferisce al processo di decentramento del web così come è attualmente inteso. Il principio centrale del Web 3.0 è l'idea che le reti debbano essere rese più aperte, senza fiducia e senza permessi. Questo obiettivo può essere raggiunto rendendo lo sviluppo e i software open-source; la decentralizzazione e l'eliminazione della necessità di terze parti fidate e governanti possono essere realizzate senza fiducia e senza permessi. Le blockchain sono comunemente considerate sinergiche con il futuro sviluppo del web 3.0. Ad esempio, abbiamo appreso dalla DeFi e dalle DAO che questi protocolli possono essere visti come la realizzazione delle ideologie del web 3.0. Poiché la decentralizzazione è una componente fondamentale del web 3.0, si ritiene che le blockchain abbiano queste sinergie. (Vermaak, 2022) (Fabric Ventures, 2019)

### 4.1.1 Evoluzione del Web

All'inizio degli anni '90 sono state rese disponibili le prime applicazioni Web1 commerciali. A quel tempo, ciò che oggi chiamiamo "Internet" era costituito solo da pagine Web statiche. Internet era di "sola lettura", cioè gli utenti potevano solo recepire le informazioni disponibili. All'epoca, le destinazioni online più popolari erano siti web come Britannica Online e Yahoo piuttosto che piattaforme di social media come Facebook o Netflix. L'infrastruttura tecnologica era fornita rispettivamente da IP, HTTP, URI e HTML. A seguito dello scoppio della bolla delle dot-com nel 2000, molte aziende di Internet sono fallite. Nonostante questa battuta d'arresto, le menti brillanti del mondo tecnologico concentrarono la loro attenzione sull'ulteriore sviluppo di innovazioni come JavaScript, HTML5 e CSS3. La conseguenza è stata la lenta ma costante ascesa del Web2.

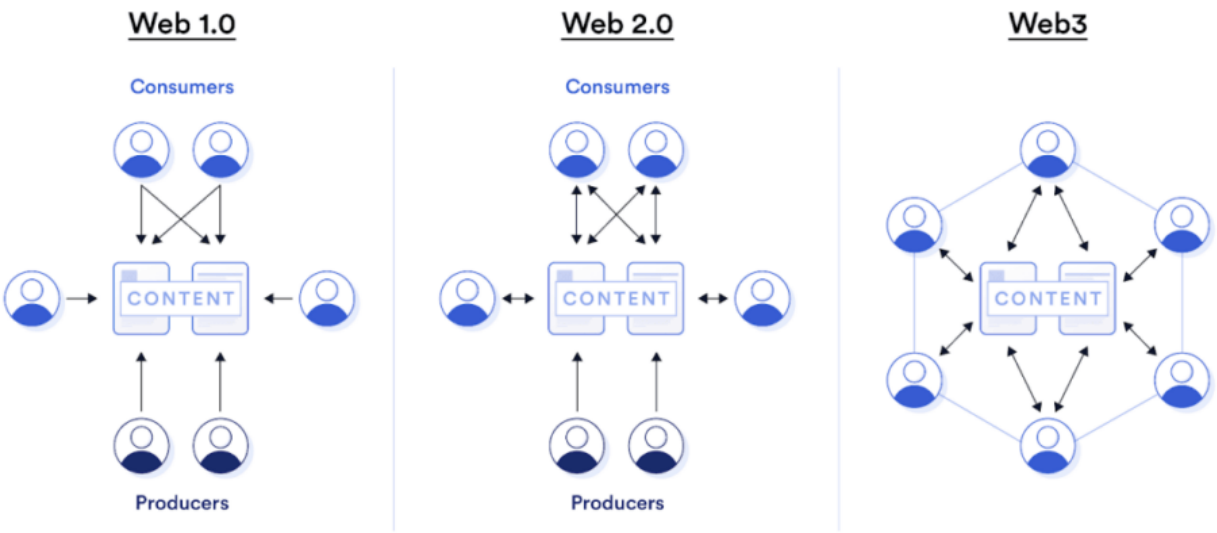
Gli utenti mettono i loro dati a disposizione dei fornitori di servizi come le piattaforme di social media, le piattaforme di e-commerce o i fornitori di pagamenti, consentendo così il funzionamento di queste applicazioni. Mentre il Web1 si concentrava principalmente sulla trasmissione di informazioni, il Web2 è più attento all'interazione. Gli utenti del Web2 non sono più considerati solo clienti, ma anche prodotti. Facebook è una buona illustrazione di questo concetto perché, a differenza degli utenti dei siti Web1, gli utenti di Facebook possono accedere allo stesso sito web

ma vedere contenuti completamente diversi. Il motivo è che Facebook riceve dati diversi dai due utenti e, di conseguenza, visualizza feed diversi per ciascuno di essi, ognuno dei quali contiene contenuti pubblicitari o post unici.

Il Web2 ha portato a cambiamenti significativi nei modi in cui le persone comunicano e interagiscono tra loro. Paghiamo le cose con l'online banking e varie piattaforme fintech, facciamo telefonate con WhatsApp, acquistiamo su Amazon e soggiorniamo in case altrui prenotate con Airbnb. Il Web2 ha indubbiamente migliorato il nostro tenore di vita e ci ha fornito maggiori comodità, ma ci ha anche posto di fronte a nuove sfide. L'architettura server-client alla base del Web2 garantisce che le società private centralizzate continuino a controllare e possedere i dati. Di conseguenza, queste società hanno un enorme potere monopolistico e rendono difficile l'ingresso sul mercato di potenziali concorrenti erigendo barriere all'ingresso. L'intero sistema bancario e finanziario, oltre a tutte le altre applicazioni del Web 2, sono sotto il controllo di società centralizzate.

I libri mastri distribuiti, il cui tipo più comune è la blockchain, sono destinati a prendere il posto dell'infrastruttura centralizzata server-client come mezzo con cui il Web3 intende minare il potere di mercato degli attori centralizzati coinvolti nel settore. Pertanto, anziché memorizzare tutti i dati su un unico server, essi saranno dispersi su più server collegati a una rete informatica decentralizzata. Per questo motivo, le entità centralizzate, che prima fungevano da intermediari, diventeranno obsolete.

Figura 17. Differenze tra Web1.0, Web2.0 e Web 3.0



Ecco un esempio di ciò: I server centralizzati dei rispettivi fornitori di servizi bancari sono utilizzati da chiunque desideri inviare denaro da una banca all'altra nell'era moderna. Eseguendo effettivamente la transazione, le banche svolgono il ruolo di intermediari. L'utente deve fornire tutti i dati rilevanti alle banche partecipanti e deve avere fiducia che queste ultime elaborino correttamente la transazione. La banca, come ci si aspetterebbe, riscuote una commissione per l'utilizzo di questo servizio. Questa è l'attività bancaria che utilizza il Web2.

Nel Web3, si ha la possibilità di inviare la transazione tramite una blockchain decentralizzata, come quella utilizzata per il Bitcoin. Utilizzando la matematica e una quantità significativa di potenza di calcolo, questa blockchain fornisce una verifica indipendente che la transazione è stata completata con precisione. A differenza del Web2, le banche non sono più necessarie come intermediari. Inoltre, ciò indica che l'utente mantiene il controllo sui propri dati e, poiché non c'è un attore centrale che trae profitto dalla transazione, non ci sono commissioni che l'utente deve pagare. In altre parole, il Web3 dovrebbe restituire all'utente la sovranità dei dati e i diritti di proprietà. (cryptostudio.com, 2022)

### 4.1.2 Sfide del Web 3.0

Il Web3 è ancora agli inizi e rimangono molte domande senza risposta. Poiché la velocità di elaborazione dei dati di una rete decentralizzata è significativamente più lenta di quella di una rete centralizzata (Web2), la scalabilità tecnologica è un ostacolo significativo, proprio come lo era in passato per il Web1. Le transazioni Bitcoin, ad esempio, richiedono molto più tempo per essere completate rispetto a quelle elaborate attraverso le reti di Visa o Mastercard. L'esperienza utente offerta dalle applicazioni Web3 non è attualmente all'altezza di quella offerta dalle applicazioni Web2. Per molti utenti, ottenere un prestito attraverso una piattaforma Web3 è più difficile che farlo attraverso una società di tecnologia finanziaria o una banca Web2. A ciò si aggiunge la questione della reale decentralizzazione del Web3. Almeno per il momento, la funzionalità del Web3 continua a dipendere dall'infrastruttura del Web2. Se i fornitori di infrastrutture come Amazon Web Services dovessero fallire, anche la maggior parte delle applicazioni del Web3 smetterebbe di essere accessibile. Un gran numero di applicazioni decentralizzate sono finanziate anche da società di capitale di rischio, che detengono un gran numero di token e hanno quindi potere decisionale

all'interno della rete. Uniswap, uno scambio di criptovalute, e Compound Finance, un protocollo di prestito di criptovalute, sono due esempi di questo tipo di servizi.

### 4.2 dApps

Le dApp, nella loro forma più elementare, sono applicazioni che funzionano come altri programmi, ma non fanno capo a un unico amministratore. Finché un'applicazione non dipende da un server centrale per i suoi dati o le sue funzionalità, può essere considerata un'applicazione decentralizzata (dApp). La maggior parte delle applicazioni decentralizzate (dApp) sono costruite per operare su blockchain perché queste ultime offrono un'infrastruttura decentralizzata su cui è possibile costruire. Nonostante sia teoricamente possibile per un'applicazione operare al di fuori della catena, come nel caso di alcune applicazioni di tracciamento o raccolta dati su blockchain, ciò non è attualmente una realtà. D'altra parte, questo tipo di applicazioni off-chain hanno quasi sempre un server centralizzato che le supporta, motivo per cui non possono essere considerate applicazioni decentralizzate (dApp).

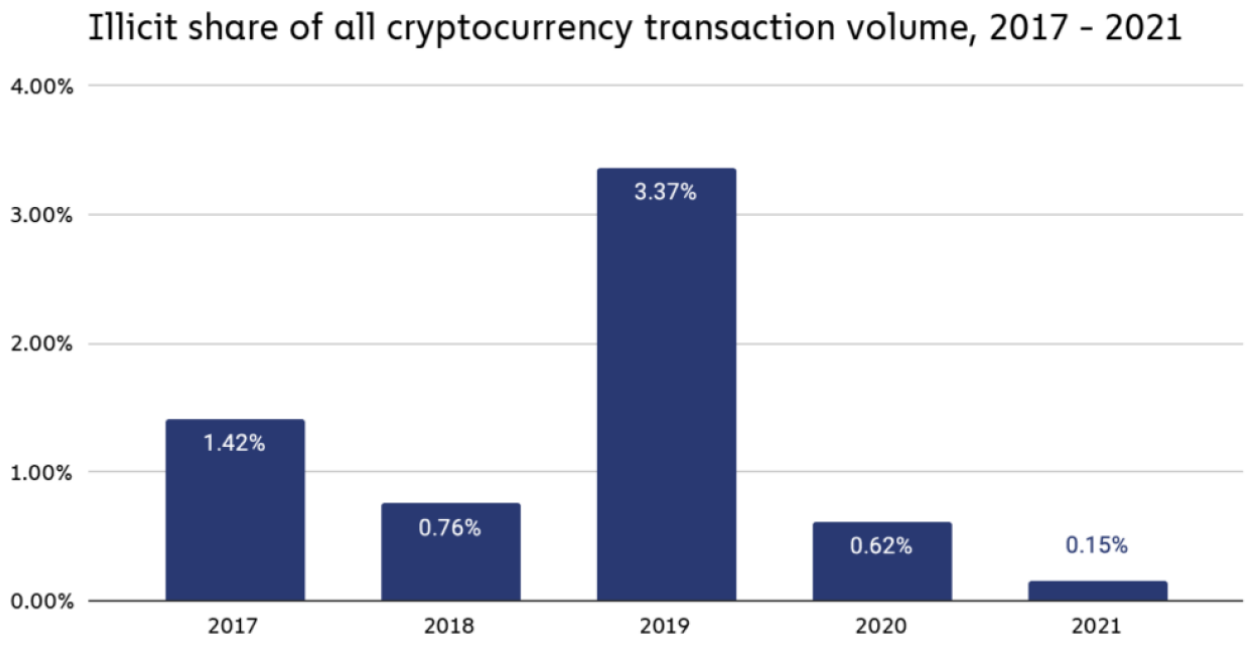
Le dApp presentano aspetti positivi e negativi; tra gli aspetti positivi vi sono la trasparenza, la coerenza e le prestazioni. Prendendo come esempio una soluzione finanziaria decentralizzata, è possibile trasferire beni per un valore di milioni di dollari sulla catena senza che nessuno nella rete si informi sulla transazione. È lecito supporre che l'applicazione elaborerà il trasferimento nello stesso modo in cui lo farebbe qualsiasi altro trasferimento, in quanto è possibile che questi trasferimenti avvengano quasi istantaneamente e a costi molto bassi. D'altra parte, queste applicazioni decentralizzate (dApp) sono come tutte le altre applicazioni: sono programmate dall'uomo, il che significa che esiste la possibilità di bug e violazioni della sicurezza, che potrebbero causare la perdita di fondi. Dato che la rete è decentralizzata, non esistono vere e proprie autorità che possano emettere un rimborso all'utente. Questo rende quantomeno discutibili alcune delle soluzioni dApp e DeFi. A causa della natura delle blockchain in generale, il debug e l'aggiornamento di un'applicazione decentralizzata (dApp) possono essere piuttosto impegnativi. Poiché la stragrande maggioranza dei nodi dovrebbe acconsentire a ogni aggiornamento, sarebbe molto più difficile da implementare rispetto a un aggiornamento standard dell'applicazione. Al momento, accedere alle applicazioni decentralizzate (dApp) non è semplice come scaricare

un'applicazione tradizionale. Per molte soluzioni di applicazioni decentralizzate sono necessari un portafoglio adeguato e un browser web che supporti un connettore esterno per le dApp. (Che cosa sono le dApp? è stato pubblicato da Cointelegraph nell'anno n.d.)

### 4.3 Atti illeciti

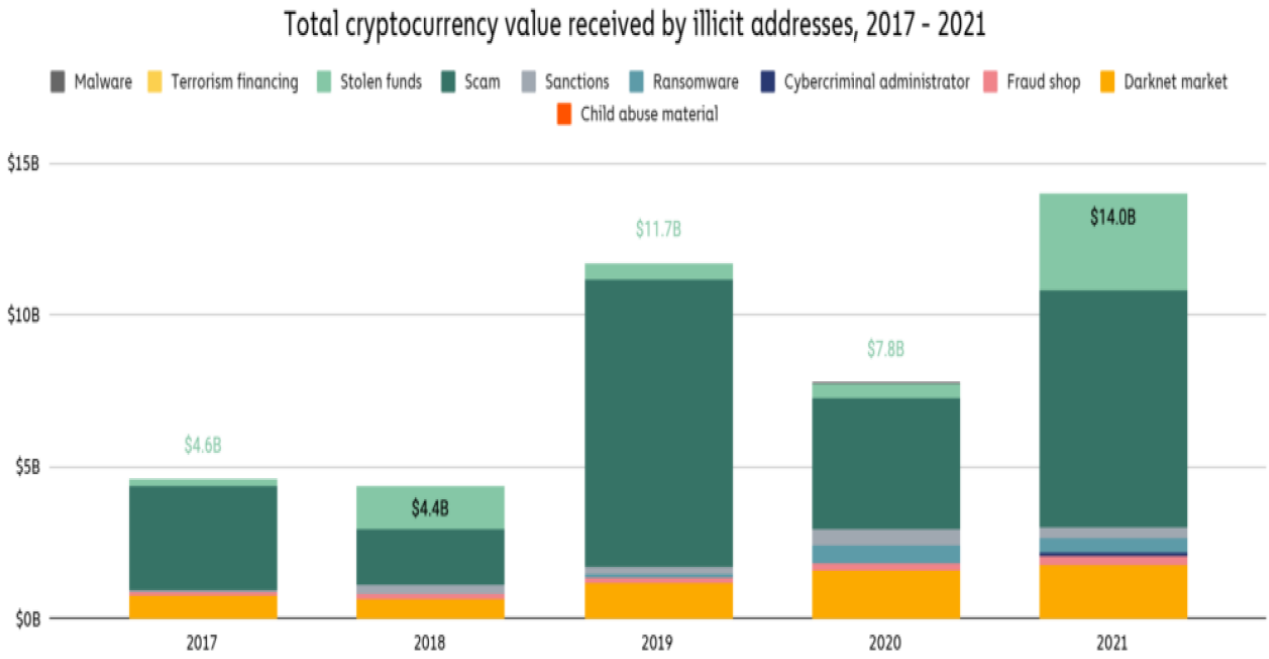
Quando si parla di soluzioni decentralizzate, in cui non esiste alcun tipo di autorità centrale e ogni transazione viene effettuata in pratica in completo anonimato, è necessario parlare di atti illegali. È vero che le criptovalute sono spesso collegate all'uso di atti illegali e ci sono casi in cui, ad esempio, gli aggressori di ransomware chiedono pagamenti in criptovalute. Questo è un esempio di come le criptovalute siano spesso collegate ad atti illegali. Tuttavia, contrariamente a quanto molti credono, le attività illegali costituiscono solo una piccola percentuale dell'uso complessivo delle criptovalute (si stima che nel 2021 saranno lo 0,15%, come mostrato nella Figura 14).

Figura 18. Grafico che mostra la porzione illecita del volume totale di transazioni per le criptovalute 2017-2021 (Tendenze della criptocriminalità per il 2022, 2022)



Questo non significa necessariamente che l'ammontare del valore utilizzato per condurre attività illegali in criptovalute stia diminuendo; piuttosto, come mostrato nella Figura 15, indica che l'ammontare totale dell'uso legittimo delle criptovalute sta aumentando.

Figura 19. Grafico che mostra il valore totale delle criptovalute inviate a indirizzi illeciti nel periodo 2017-2021 (Tendenze della criptocriminalità per il 2022, 2022)




Un altro aspetto da mettere in luce è il fatto che la stragrande maggioranza delle attività illegali associate alle criptovalute sono in realtà truffe e furti di fondi. La stragrande maggioranza delle attività illegali si svolge specificamente nei protocolli DeFi, il che non sorprende se si considera che il volume delle transazioni DeFi è aumentato del 912% nel 2021. (Tendenze della criminalità legata alle criptovalute per il 2022, 2022)

### 4.4 DeFi

La finanza decentralizzata, nota anche come DeFi, è una soluzione finanziaria innovativa che si avvale della tecnologia blockchain. Offre agli individui la possibilità di funzionare in un certo senso come la propria banca. I protocolli DeFi, ad esempio, consentono agli utenti di svolgere attività come prestare criptovalute in cambio di interessi, prendere in prestito fondi con criptovalute che fungono da garanzia, acquistare assicurazioni, negoziare derivati e attività, possedere un conto di risparmio che offre tassi di interesse tipicamente superiori a quelli offerti dalle banche convenzionali, fornire liquidità per ottenere rendimenti e molte altre attività.

Attualmente, Ethereum è la criptovaluta più dominante sul mercato in termini di TVL (Total Value Locked). Oggi, nel gennaio 2022, si stima che il TVL di Ethereum si aggiri intorno ai 115 miliardi di dollari USA. (Ethereum, 2022)

Ci sono molti motivi per cui la DeFi è un'alternativa interessante per la detenzione e la gestione di beni, tra cui i seguenti:

- Gli utenti mantengono il controllo del proprio denaro e dei propri beni, quindi non è necessario inviare il proprio denaro a terzi.
- Indipendentemente dall'entità della transazione, le commissioni sono ridotte al minimo e le transazioni vengono completate rapidamente.
- I tassi di interesse sono tipicamente più alti di quelli offerti dalle istituzioni finanziarie tradizionali.
- Anonimato, in quanto i protocolli DeFi non richiedono ai loro utenti o clienti di rivelare la propria identità o di raccogliere informazioni sull'utente.
- Senza fiducia, i protocolli DeFi funzionano esattamente come programmati, senza possibilità di errori causati dall'uomo o da altre complicazioni.
- I protocolli Defi sono disponibili 24 ore su 24, 365 giorni all'anno; non ci sono orari d'ufficio per Defi; Defi opera ininterrottamente.
- Se mettiamo in banca gli unbanked, le persone che non hanno un conto bancario avranno accesso a servizi finanziari che altrimenti non avrebbero.

(Guida completa alla finanza decentralizzata, n.d.) (Cos'è la DeFi?, n.d.) (Sharma, 2022)

### 4.5 Organizzazione autonoma decentralizzata (DAO)

L'acronimo "DAO" sta per "Organizzazione Autonoma Decentralizzata". Si tratta di un tipo di organizzazione in cui i membri della comunità detengono l'autorità rispetto a una leadership centrale. Le DAO possono svolgere un'ampia gamma di funzioni, tra cui filantropia, investimenti, raccolta di fondi, gestione di progetti e molte altre.

L'organizzazione autonoma decentralizzata (DAO) può funzionare correttamente solo con un insieme limitato di caratteristiche, a causa della mancanza di un controllo centralizzato. Un'organizzazione autonoma decentralizzata (DAO) deve avere un insieme di regole che definiscono il funzionamento di un token DAO. I token emessi dalla DAO possono essere utilizzati dai membri della comunità dell'organizzazione per una serie di scopi, tra cui il voto, la partecipazione ad attività, l'abilitazione di funzioni e così via. I token sono un tipo di criptovaluta che può essere scambiata con altre criptovalute e, di conseguenza, avrà valore in futuro. Il valore sarà determinato dal grado di adozione del progetto e dalla sua popolarità.

Un "token di governance" è tipicamente utilizzato per scopi di voto in progetti che danno ai membri della comunità la possibilità di influenzare la direzione dello sviluppo futuro. In un certo senso si tratta di un sistema DAO, che viene utilizzato in questo momento per un progetto di sviluppo. Esiste la possibilità di avere dei "gettoni di utilità", che vengono utilizzati per consentire agli utenti di eseguire un qualche tipo di azione, come la modifica del proprio lotto di terreno nel Metaverso o qualcosa di simile. Il token DAO è più che altro una generalizzazione che potrebbe essere utilizzata come minimo per la governance, ma ha anche il potenziale per includere usi di utilità. (Cos'è un'organizzazione autonoma decentralizzata e come funziona una DAO?, n.d.) (Decentralized Autonomous Organizations (DAOs), n.d.) (Hackl, 2021) (Governance Token, n.d.) (Cos'è un'organizzazione autonoma decentralizzata e come funziona una DAO?, n.d) (I diversi tipi di token di criptovaluta spiegati, 2020)

### 4.6 Logistica

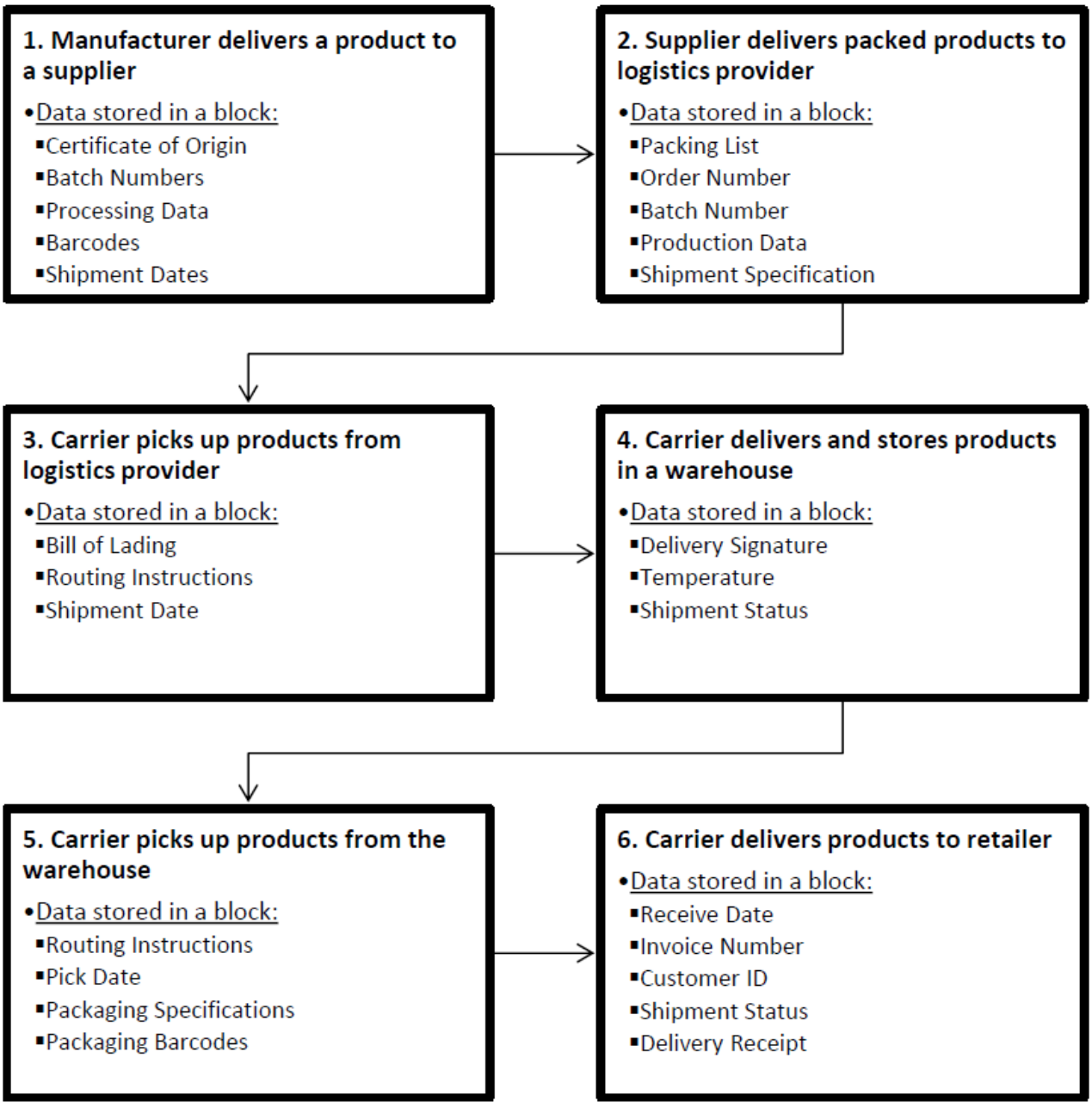
La logistica, che può avere catene di fornitura molto complicate e diverse parti e fasi coinvolte nel processo end-to-end, può utilizzare la tecnologia blockchain in diverse aree, come rendere la catena di fornitura più trasparente, più veloce e di conseguenza più efficiente, fornire una migliore tracciabilità e persino nella gestione dei pagamenti a tutte le parti coinvolte. Attualmente, la catena di approvvigionamento logistico è afflitta da una notevole quantità di lavoro manuale, da una mancanza di trasparenza che si traduce in una tracciabilità inadeguata, che poi si traduce in una serie di problemi, e così via.

L'uso della tecnologia blockchain per creare una rete condivisa per tutti i partecipanti alla catena di approvvigionamento sarebbe una soluzione a quasi tutti i problemi descritti in questo articolo. Inoltre, sono stati fatti molti progressi in termini di maggiore fiducia, visibilità, efficienza, qualità e così via. La tecnologia blockchain e i contratti intelligenti hanno il potenziale per automatizzare un'ampia gamma di processi, tra cui i pagamenti, i trasferimenti di proprietà, le ispezioni dei carichi e molti altri. Se considerati insieme, questi fattori hanno il potenziale di ridurre i costi delle transazioni, eliminare il rischio di errori umani e velocizzare il lavoro manuale.

Importanti aziende come DHL, FedEx e Walmart hanno implementato o stanno prototipando diverse soluzioni legate alla blockchain nelle loro catene di fornitura. Queste soluzioni mirano a migliorare la trasparenza e l'efficienza. (PwC, n.d.) (Higgins, 2021) (Higgins, 2021)

Questo è un esempio di come una blockchain potrebbe essere utilizzata in un'azienda di logistica, nonché di come e quali informazioni vengono memorizzate in una blockchain. L'esempio è presentato in modo semplice.

Figura 20. Esempio di utilizzo della tecnologia Blockchain nel settore della logistica (Globaltranz, 2018)



### 4.7 Il futuro della finanza 3.0

Gli amministratori delegati e altri leader del settore bancario si sono incontrati per discutere dell'impatto che le nuove tecnologie e innovazioni avranno sui servizi finanziari. Tra queste, la creazione di nuovi modelli operativi decentralizzati e il Web 3.0, la terza generazione di Internet.

Fin dalla sua nascita, Internet ha subito una serie di cambiamenti significativi, passando da un'esperienza prevalentemente di sola lettura e statica a una decisamente più dinamica, interattiva e decentralizzata. Le fondamenta del Web 3.0 sono attualmente poste dagli sviluppi della finanza decentralizzata (DeFi), della tecnologia blockchain, delle criptovalute e dei libri contabili distribuiti. La capitalizzazione di mercato totale delle criptovalute ha raggiunto i 2.200 miliardi di dollari nel dicembre 2021, mentre il valore totale bloccato nei protocolli DeFi è aumentato di oltre il 1000% rispetto all'anno precedente. Questa crescita è dovuta alla crescente adozione della DeFi.

Il settore dell'economia che si occupa di servizi finanziari sta accelerando la sua transizione al Web 3.0. Nel corso degli ultimi tre decenni, i progressi della tecnologia Internet sono stati pressoché continui. Negli anni '90, la prima generazione del World Wide Web, nota come Web 1.0, offriva agli utenti contenuti e informazioni statici e ospitati su server web. A questa è seguita una versione migliorata del Web 2.0, nota anche come "Social Web". Questa versione ha permesso di creare contenuti generati dagli utenti, piattaforme di social media, capacità interattive e interoperabilità; tuttavia, presenta anche sfide per quanto riguarda il controllo e la proprietà dei dati. Il Web 3.0, noto anche come Web semantico, è la prossima rivoluzione di Internet, ancora in fase di sviluppo. Il Web 3.0 si baserà sulla convergenza di tecnologie emergenti come blockchain, intelligenza artificiale (AI), apprendimento automatico e realtà aumentata, tra le altre. I dati decentralizzati, un ambiente più trasparente e sicuro, l'intelligenza cognitiva delle macchine e il design tridimensionale saranno alcune delle caratteristiche che lo definiranno.

Nel corso degli ultimi anni Internet ha subito una transizione verso il Web 3.0. Il Web 3.0 è incentrato su dati decentralizzati, più aperti e alimentati dalla tecnologia dei libri mastri distribuiti (DLT), dall'intelligenza artificiale e dall'apprendimento automatico (ML). Si prevede che il Web 3.0 vedrà la convergenza di diverse tecnologie, come la blockchain per migliorare la proprietà e il controllo dei dati e la DeFi. È possibile che la capacità di discernere e valutare le informazioni con l'aiuto dell'IA e dell'analisi contestualizzata porti a risultati più pertinenti, a un'esperienza cliente più

iper-personalizzata e a un migliore processo decisionale. L'uso della realtà aumentata e virtuale potrebbe favorire una maggiore convergenza tra il mondo online e quello fisico, nonché la progettazione tridimensionale di Internet e di siti web interattivi.

Nuove aziende sono nate come risultato diretto del rapido sviluppo di Internet e delle tecnologie finanziarie. È sempre più necessario che le istituzioni innovino i propri servizi e modelli di business e abbraccino questi progressi che hanno il potenziale di rimodellare il futuro del denaro, dei pagamenti e degli asset digitali. Questa esigenza è alimentata dal fatto che vi è una crescente domanda di innovazione dei servizi e dei modelli di business da parte delle istituzioni.

Nella sua ricerca di diventare un centro finanziario globale e un hub tecnologico di primo piano, Singapore considera gli sviluppi delle tecnologie emergenti come le blockchain e le criptovalute come elementi essenziali per il futuro del settore. L'influenza che il Web 3.0 avrà sui servizi finanziari è stato uno dei principali argomenti di discussione del recente fintech festival 2021. Il festival ha messo in luce le nuove innovazioni che stanno rimodellando i modelli operativi e di business dei servizi finanziari verso la decentralizzazione, le valute digitali e i progressi dell'IA, tra le altre cose, mentre il settore avanza.

Heng Swee Keat, vice primo ministro di Singapore e ministro coordinatore delle politiche economiche, ha delineato i tre approcci che possono essere adottati per ottenere la massima quantità di risultati innovativi. "In primo luogo, ottenere una trazione sulle tecnologie che hanno il potenziale per apportare un cambiamento di passo. In secondo luogo, sviluppando i fattori di mercato appropriati per garantire la scalabilità delle innovazioni. In terzo luogo, raddoppiando l'uso dell'innovazione per migliorare la vita delle persone", ha dichiarato in occasione di un festival che ha celebrato il fintech. Nel suo discorso, ha illustrato i molti modi in cui l'IA può facilitare il progresso sociale ed economico e ha annunciato il lancio del programma nazionale di IA nel settore finanziario. Il programma include la piattaforma di intelligenza artificiale NovA! per l'analisi dei rischi finanziari, sviluppata grazie a una partnership tra banche e società fintech del Paese.

Oltre al budget di 500 milioni di SGD (365,8 milioni di dollari) già annunciato, Singapore stanzierà altri 180 milioni di SGD (131,69 milioni di dollari) per accelerare la ricerca fondamentale e traslazionale sull'intelligenza artificiale. Ha continuato dicendo che "il potenziale dell'IA è enorme" e che "è fondamentale garantire che venga utilizzata in modo etico".

Le banche sono state costrette a valutare e strategizzare i futuri modelli di business e ruoli a seguito dell'adozione diffusa del Web 3.0 e degli sviluppi tecnologici. Secondo Piyush Gupta, CEO di DBS, l'importanza del 5G sta crescendo e la capacità di avere contemporaneamente larghezza di banda e latenza rende possibile il mondo Meta. Ha affermato che la tecnologia blockchain rende possibile la verifica dell'identità. Nel mondo di oggi, dove tutto è guidato dai dati, il concetto di identità autonoma è più importante che mai. Fornisce ai clienti una prova di valore e allo stesso tempo adempie a un obbligo per le banche e le altre istituzioni finanziarie. Esse stanno cercando di collegare il paradigma del regolamento delle transazioni in una catena. Le prospettive più idealistiche del Web 3.0, che egli ha definito il terzo livello o il selvaggio west, sono state messe alla prova da lui stesso. Ha sottolineato che gli individui non hanno bisogno di intermediari o istituzioni, il che aprirebbe la strada all'implementazione dei contratti intelligenti. "Il problema di questa linea di ragionamento è che quando si passa alla fase successiva, si inizia a mettere in discussione la necessità o meno di autorità di regolamentazione o di una banca centrale. Fino al punto di non avere più bisogno di una nazione, di uno Stato o di un organo di governo." Gupta ha continuato: "Inizia a non essere una questione di tecnologia, ma piuttosto di politica e filosofia sociale".

Secondo Mike Wells, group chief executive di Prudential, le persone vedranno molti più dati e i consumatori avranno un maggiore controllo e la possibilità di implementare la personalizzazione; tuttavia, avranno bisogno di assistenza. Ha discusso la possibilità che il settore bancario tradizionale diventi obsoleto in futuro. Ha affermato che le aziende tradizionali potrebbero essere stravolte in modo tale da cambiare il loro ruolo e le loro capacità, ma non il loro valore. Helen Wong, Group Chief Executive di OCBC Bank, ha affermato che le criptovalute sono un valore di stoccaggio accompagnato da rischi. Ha citato esempi di contro come il crypto token e come il suo valore sia sceso nel tempo.

Un ostacolo significativo per le istituzioni finanziarie è la proliferazione di dispositivi interconnessi e di ecosistemi ampliati, oltre alle enormi quantità di dati che devono essere consolidati e archiviati. È scontato che i dati saranno un bene essenziale che le istituzioni finanziarie dovranno imparare a monetizzare meglio per ottenere una crescita futura. Il Web 3.0 consente alle istituzioni finanziarie di innovare i propri prodotti e servizi, secondo Jacquelyn Tan, amministratore delegato e

responsabile dei servizi finanziari personali del gruppo, Group Retail di UOB. Sono in grado di adattarsi rapidamente alle preferenze in continua evoluzione dei loro clienti e di offrire di conseguenza un'esperienza altamente personalizzata. È assolutamente necessario che le banche non solo investano nell'innovazione tecnologica, ma modifichino anche il modo in cui i clienti interagiscono fisicamente con le banche per ottenere un'attività bancaria omnicanale senza soluzione di continuità. La capacità di iper-personalizzare l'esperienza bancaria digitale in base alle impronte digitali dei clienti e di integrare gli stili di vita dei consumatori riunisce il mercato bilaterale in una rete più ampia. Per avere relazioni bancarie più contestualizzate, le istituzioni finanziarie devono ora ripensare i percorsi dei clienti utilizzando la convergenza senza soluzione di continuità di tecnologie chiave, la realtà virtuale e l'intelligenza artificiale aumentata.

Secondo Mark Smith, amministratore delegato di Digital Realty, è davvero necessario che le aziende sfruttino in modo aggressivo le interazioni abilitate dal digitale piuttosto che quelle fisiche, perché i clienti si aspettano che le aziende forniscano loro un'esperienza digitale completa. La localizzazione dei dati sta acquisendo importanza a causa delle politiche legali e normative che richiedono l'archiviazione locale dei dati. Una forte intensità di gravità dei dati è stata osservata a Singapore, in Giappone, Corea e Australia, e questa intensità è raddoppiata ogni anno. L'importanza delle normative sulla privacy dei dati aumenta la possibilità che l'aggregazione dei dati basata sul consenso porti dei vantaggi. I consumatori otterranno il controllo e la proprietà dei propri dati attraverso l'iniziativa Singapore Financial Data Exchange (SGFinDex), nonché il potere di decidere quando acconsentire alla condivisione dei propri dati. Il recente lancio della seconda fase dell'SGFinDex da parte dell'Autorità Monetaria di Singapore (MAS) e dello Smart Nation and Digital Government Group (SNDGG) consente ai cittadini di visualizzare le informazioni finanziarie consolidate dei loro investimenti detenuti presso il deposito centrale.

"Sono convinto che la tecnologia permetta di immaginare qualsiasi cosa", ha dichiarato Han Kwee Juan, amministratore delegato e responsabile della strategia e della pianificazione di DBS; "Tuttavia, è necessario che un ecosistema si unisca per risolvere un vero punto dolente". Han Kwee Juan ha inoltre dichiarato che DBS ha condotto prove con il 5G, l'Internet delle cose (IoT) e sta utilizzando il cloud privato.

L'open banking sta guadagnando slancio grazie all'aumento consistente dell'uso delle interfacce di programmazione delle applicazioni (API) e del cloud banking. Ciò ha permesso di combinare obiettivi commerciali e progressi tecnologici per sviluppare nuovi modelli commerciali. Le banche hanno iniziato a specializzarsi, non dovendo più operare come un'unica entità. Il Banking as a service (BaaS) è un modello che offre agli istituti finanziari la possibilità di concentrarsi su scala, apertura e coinvolgimento dei clienti. Secondo Chuck Davis, direttore commerciale di Temenos, le banche e le altre istituzioni finanziarie stanno adottando il cloud computing e utilizzano il software-as-a-service (SaaS) per creare esperienze iper-personalizzate per i clienti utilizzando le interfacce di programmazione delle applicazioni (API). In questo modo, i vari operatori del settore sono in grado di scalare le proprie operazioni e di rispondere più rapidamente alle tendenze emergenti del mercato.

Le nuove aziende che stanno costruendo i loro modelli di business sulla vendita diretta ai clienti hanno registrato una crescita significativa. "Se si vuole far parte della rivoluzione digitale, si tratta di utilizzare la tecnologia per migliorare la produttività", ha dichiarato Kevin O'Leary, presidente di O'Leary Ventures. Nel contesto dei servizi finanziari, questo si riferisce alle criptovalute. Si tratta di un software che rende i mercati finanziari globali più efficienti, con meno attriti e costi, oltre che più trasparenti e conformi. I volumi totali e il market cap delle criptovalute hanno registrato una tendenza al rialzo negli ultimi due anni e si prevede che raggiungeranno un massimo di 2,83 trilioni di dollari nel novembre 2021. Alla fine dell'anno, il valore totale del mercato era di 2.200 miliardi di dollari. Oggi esistono migliaia di criptovalute diverse, ma il Bitcoin è il leader del mercato con un margine significativo, detenendo quasi il 39% del market cap totale.

Il termine "finanza decentralizzata" (abbreviato in "Defi") è utilizzato per indicare gli asset digitali, nonché gli smart contract finanziari, i protocolli e le applicazioni decentralizzate (DApp). Defi, che si basa anche sulla tecnologia distributed ledger e blockchain, è un'alternativa decentralizzata al tradizionale sistema finanziario centralizzato. Lo fa eliminando la necessità di intermediari e ponendo l'accento sulle reti peer-to-peer. L'espressione "valore totale bloccato in Defi", che descrive la somma di denaro che viene attualmente elaborata attraverso i vari protocolli DeFi, ha registrato un notevole incremento nel corso degli ultimi due anni.

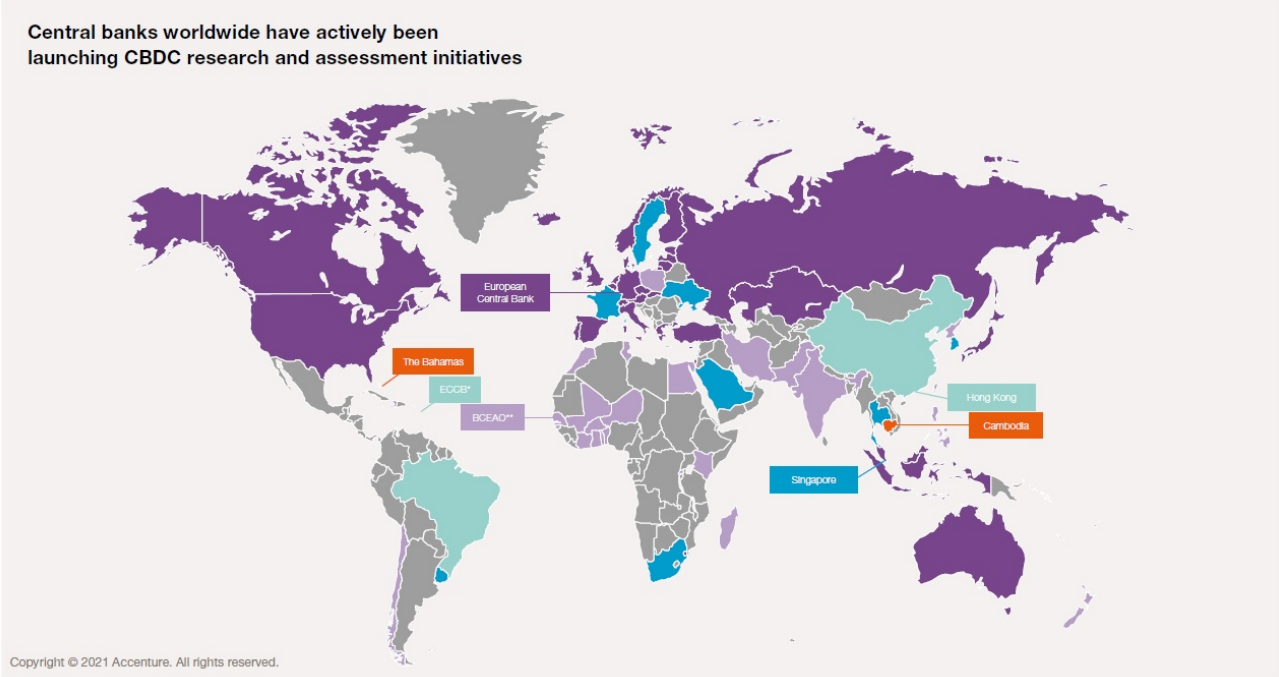
Il mercato sta studiando le possibilità offerte dalla tecnologia blockchain e c'è una crescente domanda di applicazioni legittime delle criptovalute. Tuttavia, la Distributed Ledger Technology (DLT) è ancora nelle prime fasi di sviluppo e deve affrontare sfide quali l'interoperabilità, la scalabilità e le normative. Inoltre, le criptovalute destano preoccupazioni dal punto di vista normativo e molti Paesi stanno studiando la possibilità di emettere le proprie valute digitali (CBDC). Nel mese di ottobre, le Bahamas hanno fatto la storia introducendo la prima CBDC al mondo progettata per uso generale; si chiama Sand Dollar. Ad oggi, nove Paesi, tra cui la Nigeria e i Paesi dei Caraibi orientali, hanno lanciato le CBDC, mentre altri 87 Paesi stanno studiando e testando le acque di questo mercato.

Secondo Ravi Menon, direttore generale dell'Autorità monetaria di Singapore (MAS), l'anonimato delle criptovalute ha reso possibile il loro utilizzo in transazioni illegali, come l'alimentazione di ransomware e il riciclaggio di denaro. La Monetary Authority of Singapore non approva l'uso di criptovalute o token come investimenti per attività al dettaglio. Secondo Menon, i prezzi dei token delle criptovalute non si basano su alcun fondamento economico, rendendoli vulnerabili a oscillazioni selvagge causate da attività speculative. Secondo Menon, la tecnologia blockchain e i token crittografici sono potenzialmente in grado di apportare molti benefici, tra cui pagamenti internazionali più rapidi e meno costosi e il finanziamento del commercio; tuttavia, affinché ciò avvenga, è necessario che abbiano un valore più stabile e un supporto credibile. Secondo Menon, "il MAS vede un grande potenziale nei CBDC all'ingrosso". D'altra parte, non ci sono argomenti convincenti né a favore né contro la vendita di CBDC nei punti vendita al dettaglio a Singapore.

Le CBDC sono anche oggetto di studio da parte di alcuni Paesi per l'utilizzo nelle transazioni finanziarie internazionali. Ad esempio, la Reserve Bank of Australia, la Banca Centrale della Malesia, la Monetary Authority of Singapore e la Reserve Bank sudafricana, insieme alla Banca dei Regolamenti Internazionali, stanno collaborando a un progetto chiamato Project Dunbar per studiare la fattibilità dell'utilizzo delle CBDC per i regolamenti internazionali. Questo esperimento potrebbe rendere più facile e meno costoso effettuare pagamenti attraverso i confini internazionali. Tuttavia, per avere successo, tali progetti richiederanno una maggiore partecipazione da parte di altre nazioni, una migliore governance e la risoluzione delle sfide derivanti dal fatto che le diverse giurisdizioni hanno norme e regolamenti differenti. Patrick Njoroge, governatore della Banca

Centrale del Kenya, e Serey Chea, assistente del governatore della Banca Nazionale della Cambogia, hanno discusso del partenariato pubblico-privato, delle potenziali applicazioni delle CDBC e della necessità di una maggiore collaborazione. Non possiamo farcela da soli". Secondo Njoroge, "è necessario lavorare a stretto contatto con altre istituzioni e banche centrali che hanno una mentalità simile".

Figura 21. Mappa dell'adozione delle CBDC nel mondo




| | | |
|---|---|---|
| 32 | Interest | Countries declaring interest and doing initial internal research to explore CBDC feasibility. |
| 35 | Research | Countries that published CBDC research reports and/or conducted early PoCs. |
| 19 | Experimentation | Countries that started experimenting and piloting CBDC with limited number of parties. |
| 2 | Implementation | Countries preparing their CBDC for a full-scale launch. |
| 2 | Launched | Countries that officially launched a CBDC. |

Nel frattempo, il panorama dei pagamenti globali sta subendo un rapido cambiamento ed è urgente sfruttare il Web 3.0 per alimentare la successiva fase di sviluppo. I clienti hanno determinate aspettative per quanto riguarda la velocità, il prezzo, la convenienza e la trasparenza dell'esperienza di pagamento, e le banche devono sviluppare il pagamento incorporato come parte di un percorso

integrato per soddisfare tali aspettative. Secondo Michael Miebach, Chief Executive Officer di Mastercard, per il Web 3.1 è necessario un commercio senza soluzione di continuità. Il pagamento deve essere ridotto al punto da non essere visto, e dobbiamo soddisfare tutte le nostre esigenze in modo intuitivo. Ha sottolineato che la questione dell'identità nel commercio senza attriti è di estrema importanza, mentre l'identità digitale rappresenta un significativo passo avanti.

Le banche stanno studiando nuovi modelli per incorporare la finanza nei pagamenti. Per raggiungere il massimo grado possibile di accessibilità economica, è necessario ampliare i partenariati pubblico-privato. È necessaria una maggiore collaborazione e lo sviluppo di soluzioni per collegare Paesi e regioni al fine di facilitare le transazioni finanziarie internazionali. Sono in corso nuovi accordi a livello bilaterale che stanno entrando in vigore. Recentemente, la Monetary Authority of Singapore (MAS) e la Banca Centrale delle Filippine (Bangko Sentral ng Pilipinas, o BSP) hanno firmato un accordo per facilitare i pagamenti interoperabili tra Singapore e le Filippine.

Il presidente e amministratore delegato di Salesforce, Marc Benioff, ha dichiarato che "non c'è niente di più importante della fiducia". Questo si riferisce alla fiducia che Salesforce ha nei confronti di tutti i suoi stakeholder, compresi i clienti, i dipendenti, i partner e gli azionisti pubblici. A seguito della pandemia, si è verificata una maggiore convergenza tra tecnologie fisiche e digitali, nonché un cambiamento nel modo di operare in remoto. A causa di questi fattori, oggi si pone un'enfasi maggiore sulla sicurezza, sull'identità digitale, sulla fiducia zero e sulla sicurezza dei dati. Integrando reti blockchain di nodi decentralizzati in grado di convalidare transazioni crittograficamente protette, l'architettura decentralizzata del Web 3.0 affronta questioni quali la fiducia degli utenti, la privacy e la trasparenza. In questo modo, i clienti non devono affidarsi a un'unica entità centralizzata per soddisfare le loro esigenze.

Secondo Oki Matsumoto, amministratore delegato di Money Group, il Web 3.0 è una rete affidabile che ha il potenziale per stabilire una nuova nazione nel cyberspazio. L'azienda opera in questo Paese utilizzando diversi modelli di business, come l'implementazione di contratti intelligenti. Un'applicazione decentralizzata (app) che esegue la logica aziendale in risposta a eventi è nota come smart contract. La sua esecuzione può essere il risultato del trasferimento di fondi, della fornitura di servizi, dello sblocco di contenuti protetti dalla gestione dei diritti digitali o di altre forme di manipolazione dei dati. È possibile utilizzarlo per garantire la protezione della privacy,

facilitando il rilascio selettivo di dati protetti dalla visione di parti non autorizzate, al fine di soddisfare una particolare richiesta.

Le discussioni hanno anche messo in luce l'importanza di avere una governance sull'IA, di gestire i modelli e di mantenere la sicurezza dei dati. Durante un'intervista, Ben King, Chief Security Officer di Okta per l'Asia e il Pacifico (APAC) e per l'Europa, il Medio Oriente e l'Africa (EMEA), ha dichiarato che "vedremo più "zero trust" e l'utilizzo di questo concetto nella strutturazione dei programmi di sicurezza". L'uso di più metodi di autenticazione diventerà sempre più comune. È probabilmente il controllo più potente di cui disponiamo e nel prossimo futuro assisteremo a un maggior numero di applicazioni di password-less. L'uso dell'apprendimento automatico (ML) per analizzare grandi insiemi di dati sta diventando sempre più comune nel campo della sicurezza. Poiché i nostri avversari utilizzano l'apprendimento automatico, abbiamo bisogno di macchine in grado di reagire in pochi secondi. Secondo King, "questo è un dibattito che sta crescendo rapidamente, perché si può perdere un umano nel loop se la macchina sta combattendo un'altra macchina".

Il ciclo del cambiamento è innegabilmente immutabile, ma la velocità con cui avviene si è indubbiamente accelerata a seguito della pandemia. L'evoluzione del settore dei servizi finanziari continuerà a essere guidata, in futuro, dal Web 3.0 e dalla transizione verso la decentralizzazione, la capacità di monetizzare i dati in modo efficace, le valute digitali e le collaborazioni più forti tra ecosistemi per un servizio incentrato sul cliente. (Aggarwal & Salangsang, 2022)

# Capitolo 5: Metaverso

Tra le infinite applicazioni del Web 3.0 e della Blockchain, una in particolare potrebbe avere un impatto rivoluzionario sulla nostra concezione di realtà. Tale è la potenzialità del Metaverso, un mondo virtuale ed interconnesso che sfrutta ed integra tutte le funzionalità del Web 3.0.

## 5.1 Cos'è il Metaverso?

Il Metaverso è un mondo virtuale tridimensionale online, aperto, condiviso e persistente che offre alle persone la possibilità di connettersi tra loro in ogni momento della loro vita. Le persone saranno in grado di lavorare, interagire socialmente, condurre affari, giocare e persino creare all'interno del Metaverso perché si tratta di una rete altamente scalabile e persistente di mondi virtuali interconnessi, incentrata sull'interazione in tempo reale.

Per immergere completamente l'utente nel mondo della realtà virtuale, il Metaverso utilizzerà tecnologie di virtualizzazione e di avanguardia come la realtà aumentata, la realtà virtuale e i sensori aptici. Si potrà, ad esempio, utilizzare per organizzare una conferenza in realtà mista nel proprio luogo di lavoro virtuale tramite l'utilizzo di un visore Oculus. In questo spazio virtuale potrete finire i vostri compiti, giocare a giochi basati sulla blockchain e gestire il vostro portafoglio di criptovalute semplicemente entrando nella tecnologia del Metaverso. Ciò significa che l'utente può interagire in tempo reale con un mondo che è sempre presente e al quale ha accesso costante e illimitato in qualsiasi momento lo desideri.

Oltre ai social media e ai videogiochi, il Metaverso conterrà anche economie, identità digitali, governi decentralizzati e altri tipi di reti e strutture. La tecnologia blockchain utilizzata dal Metaverso può essere un'ottima soluzione per le criptovalute. Essa apre la strada alla creazione di una digitalizzazione fondata su una serie di valute digitali e oggetti virtuali (NFT). Il Metaverso beneficerà anche dello sviluppo di portafogli di criptovalute come Trust Wallet e MetaMask, attualmente in fase di sviluppo. Inoltre, le reti blockchain hanno il potenziale per essere utilizzate nello sviluppo di reti di governance affidabili e aperte.

Al giorno d'oggi, il denaro e gli oggetti di valore creati dai consumatori continuano a contribuire allo sviluppo di un Metaverso unico e unificato. Le più grandi aziende tecnologiche del mondo stanno lavorando attivamente per plasmare il corso del futuro. Inoltre, la decentralizzazione delle criptovalute consente anche ai membri di minor rilievo di partecipare all'espansione del Metaverso. La combinazione di tutte queste qualità rende la tecnologia blockchain una possibilità interessante per guidare questa innovazione.

Secondo molti sostenitori, la versione ideale del "Metaverso" per il futuro consisterebbe in un'unica piattaforma unificata che consentirebbe agli utenti di connettere le proprie personalità, identità e servizi della piattaforma, il che porterebbe alla creazione di più mondi a cui gli utenti avrebbero accesso. Paragonabile a un mondo che contiene molti mondi più piccoli, ognuno dei quali può scegliere di entrare, uscire o addirittura creare. L'esistenza di una definizione di identità digitale, di proprietà digitale, di valute digitali e della trasferibilità universale dei beni digitali sono tutti fattori importanti che devono essere soddisfatti prima di poter stabilire un'economia pienamente funzionale in un mondo virtuale.

Il modo in cui le persone imparano, studiano, interagiscono e persino incontrano nuovi amici potrebbe essere radicalmente sconvolto dall'introduzione del Metaverso. (Talin, 2022) (Blockchain Council, 2022)

### 5.2 Realtà Virtuale

Dopo aver introdotto il concetto di Metaverso e aver accennato al suo funzionamento, è bene parlare della tecnologia che ci permetterà di godere a pieno di questa nuova realtà. Uno dei principali strumenti che ci consentiranno un'esperienza davvero immersiva all'interno di questo mondo digitale è la realtà virtuale (VR).

Una persona è in grado di interagire con un ambiente artificiale tridimensionale (3-D), visivo o sensoriale, proprio attraverso l'uso della tecnologia VR, creata grazie all'uso della modellazione e della simulazione al computer. L'utente è immerso in un ambiente generato dal computer e progettato per simulare la realtà attraverso l'uso di dispositivi interattivi. Questi dispositivi possono essere indossati sotto forma di occhiali, cuffie, guanti o tute e inviano e ricevono informazioni. Un

utente che indossa un casco dotato di schermo stereoscopico guarda immagini animate di un ambiente simulato mentre partecipa a una tipica esperienza di realtà virtuale. I sensori di movimento rilevano i movimenti dell'utente e regolano di conseguenza la visualizzazione sullo schermo, in genere in tempo reale (nell'istante in cui avviene il movimento dell'utente). In questo modo si crea l'illusione di "essere lì", ovvero di essere in telepresenza. Di conseguenza, l'utente è in grado di navigare attraverso una serie di stanze simulate, sperimentando punti di vista e prospettive mutevoli che sono credibilmente collegati ai suoi spostamenti e passi. L'utente è persino in grado di prendere e manipolare gli oggetti che vede nell'ambiente virtuale se indossa dei guanti dotati di dispositivi di force-feedback che forniscono la sensazione del tatto e che vengono indossati dall'utente.

Figura 22. Esempio di visore per realtà virtuale (Oculus Quest)

A Jaron Lanier si deve il merito di aver coniato il termine "realtà virtuale" nel 1987. La sua ricerca e la sua ingegneria hanno contribuito con una serie di prodotti alla nascente industria della realtà virtuale (VR) in quel periodo. Il coinvolgimento di vari settori del governo federale degli Stati

Uniti, in particolare il Dipartimento della Difesa, la National Science Foundation e la National Aeronautics and Space Administration, è stato un fattore unificante nelle prime fasi della ricerca e dello sviluppo tecnologico della realtà virtuale (VR) negli Stati Uniti (NASA). I progetti finanziati da queste agenzie e portati avanti nei laboratori di ricerca universitari hanno prodotto un ampio bacino di personale di talento in campi quali la grafica computerizzata, la simulazione e gli ambienti in rete. Inoltre, questi progetti hanno creato collegamenti tra il lavoro accademico, militare e commerciale. (Henry E. Lowood, 2022)

### 5.2.1 Differenze tra realtà virtuale e realtà aumentata

L'idea della realtà virtuale è ancora estranea a un numero significativo di persone, nonostante la tecnologia che ne è alla base risalga a diversi decenni fa. I termini "realtà virtuale" e "realtà aumentata" vengono spesso confusi l'uno con l'altro, il che è piuttosto comune.

La distinzione più importante tra i due è che la realtà virtuale (VR) crea il mondo in cui gli utenti si immergono tramite un headset o casco dedicato. Si tratta di un'esperienza completamente immersiva e tutto ciò che vediamo è una componente di un ambiente costruito artificialmente con immagini, suoni e così via. Nel campo della realtà aumentata (AR), invece, il nostro mondo funge da sfondo al quale vengono sovrapposti elementi virtuali come immagini, oggetti e simili. Poiché tutto ciò che vediamo è nel suo ambiente naturale, è possibile che a questo punto non siano assolutamente necessarie le cuffie. L'illustrazione più evidente e diffusa di questa idea è attualmente fornita da Pokémon Go.

Tuttavia, esiste anche la cosiddetta realtà mista, che è una combinazione di entrambe le realtà. Questa tecnologia ibrida permette di vedere oggetti virtuali nel mondo reale e di costruire un'esperienza in cui il fisico e il digitale sono quasi impossibili da distinguere.

### 5.3 La nuova economia virtuale del Metaverso

Il Metaverso non è solo un regno di gioco immaginario o il mondo ideale di uno scrittore di fantascienza. Non è nemmeno limitato alle aziende del settore tecnologico, ma è un'economia completamente nuova. Anche le aziende più tradizionali, come ristoranti come McDonald's e rivenditori come Nike, si stanno preparando a far sì che il Metaverso diventi un luogo in cui sarà possibile costruire una vita virtuale, fare shopping, giocare, incontrare amici, partecipare a concerti e lavorare. Poiché il Metaverso è ancora agli albori, per la maggior parte delle aziende non esiste un percorso ovvio verso la redditività; tutti sono in competizione tra loro per trovare l'oro per primi.

La mia previsione è che, con il superamento del Web 2.0 e l'ingresso di un numero maggiore di persone in comunità più ampie e ricche di contenuti generati dagli utenti, Internet diventerà meno stratificato. Sembra che il Metaverso si stia preparando a continuare a rompere i confini delle piattaforme e a riunire in un nuovo mondo decentralizzato ecosistemi che prima erano compartimentati.

L'economia on-demand sta rapidamente emergendo come risultato delle nuove dinamiche economiche in atto nel Metaverso. Qualsiasi azienda o creatore che voglia fare affari nel Metaverso dovrà avere una mentalità digitalmente avanzata e dare priorità alle esigenze del cliente.

Il Metaverso promette un'era in cui la creatività guiderà l'economia. Questo perché gli esperti di un'ampia varietà di settori potranno portare con sé le proprie competenze. L'assenza di regolamenti "reali" e di concorrenti consolidati significa che c'è una barriera all'ingresso significativamente più bassa, che attrae i creatori o gli studenti che sono agili e adattabili. Il Metaverso non si limita in alcun modo al regno dell'arte o del divertimento, ma ha il potenziale per trasformare completamente il modo in cui svolgiamo il nostro lavoro, introducendo avatar ultra-realistici e sale riunioni virtuali piene di persone provenienti da tutto il mondo.

Dopo tutta l'eccitazione che ha circondato i token non fungibili (NFT) e i valori degli asset digitali, il mercato speculativo indica che ci sarà un gran numero di aziende che falliranno, ma ci sarà anche un ristretto numero di aziende che emergeranno vittoriose. La mia previsione è che gli attributi di arte e divertimento che contribuiscono al valore creato dagli asset digitali come gli NFT lasceranno il posto all'incorporazione di più funzioni di utilità nel prossimo futuro.

La scommessa sulle monete per ottenere un reddito passivo è uno dei nuovi modi in cui gli asset digitali come le criptovalute e gli NFT stanno generando nuove vie di guadagno. Alcuni innovatori stanno addirittura "annidando" gli NFT incorporando vari tipi di asset digitali nel codice dei loro NFT.

I proprietari terrieri virtuali possono guadagnare rendite e canoni di locazione in modo analogo alle dinamiche delle proprietà tradizionali e degli immobili, grazie all'uso di termini predeterminati negoziati con gli affittuari e applicati da contratti intelligenti. Gli investitori hanno l'opportunità di guadagnare dividendi passivi in aggiunta alle royalties che possono essere guadagnate dai creatori quando gli NFT sono venduti o rivenduti sui mercati secondari.

Le organizzazioni autonome decentralizzate (DAO), che rappresentano un gruppo di individui che collaborano a un compito aderendo a un insieme di regole codificate, sono un altro tipo di asset digitale che possiede un potenziale significativo. La prossima generazione di servizi finanziari decentralizzati potrebbe essere creata dalle DAO, che assumono il ruolo di prestatori di denaro comunitari attraverso l'uso del crowdsourcing.

La nuova economia dovrà offrire un movimento finanziario onnipresente, definito dal cliente, piuttosto che dai limiti delle istituzioni finanziarie tradizionali. Ciò sarà necessario affinché la nuova economia abbia successo.

I consumatori hanno la possibilità di definire le proprie regole all'interno di una rete finanziaria decentralizzata che si costruisce da sola grazie alla finanza decentralizzata, nota anche come DeFi. Questa rete non potrà essere modificata e non ispirerà fiducia perché verificherà le transazioni senza bisogno dell'intervento umano. Poiché la DeFi offre una più ampia varietà di scelte finanziarie, il sistema risultante sarà più adatto all'uso che se ne intende fare, con conseguenti minori costi e maggiori rendimenti per tutte le parti coinvolte. Una maggiore divulgazione di tutte le informazioni rilevanti sarà l'inevitabile conseguenza di una maggiore simmetria informativa.

Quando vengono effettuati tra un produttore e un consumatore, i pagamenti in moneta digitale sono illimitati, non richiedono alcuna conversione e avvengono quasi immediatamente. Il trasferimento di denaro avverrà nei mercati online, dove gli utenti si riuniranno per conversare liberamente e scambiarsi reciprocamente beni e trasferimenti monetari. La facilità d'uso porterà a un'economia più

inclusiva, in cui la barriera alla partecipazione dovrebbe gradualmente diminuire fino a diventare onnipresente. Questo sarà possibile grazie alla facilità d'uso.

D'altra parte, oggi sono in circolazione migliaia di criptovalute diverse e il loro numero è in rapida crescita. L'ampiezza e la difficoltà di scegliere una strategia di investimento per il proprio denaro guadagnato duramente potrebbero scoraggiare molte persone dall'impegnarsi nel commercio virtuale.

Il Metaverso sarà caratterizzato da nuove pipeline di dati generate da una struttura decentralizzata. Queste pipeline avranno maggiori livelli di interattività e saranno in grado di acquisire dati in tempo reale in una varietà di ambienti virtuali. Il processo di aggregazione dei dati dovrebbe evolversi in un processo in cui la proprietà individuale è centralizzata. Si spera che l'apprendimento automatico porti a un ciclo di feedback istantaneo che ottimizzi immediatamente la realtà virtuale dell'utente in tempo reale.

L'utente ha ora un maggiore controllo sulla propria privacy, poiché la proprietà dei dati sta iniziando a spostarsi. In breve tempo, i dati si trasformeranno in un bene indipendente soggetto a maggiori controlli e la portabilità dei dati emergerà come modello successivo. Chi decifrerà il segreto dei sistemi analitici quasi istantanei richiesti dominerà il mercato fornendo ai clienti esperienze curate e coinvolgenti.

Sarà affascinante osservare come la nostra concezione dell'economia e il modo in cui viene determinato il valore continueranno a cambiare come risultato del Metaverso. Per costruire solide fondamenta per un ecosistema di successo devono emergere altre utilità e molti sistemi finanziari e fornitori di servizi tradizionali potrebbero non essere in grado di tenere il passo con il ritmo del cambiamento. La creazione del sistema economico Metaverso porterà a trasformazioni graduali nel settore finanziario, che si manifesteranno come ondate di innovazione sia continue che improvvise.

I leader delle aziende dovrebbero iniziare a pensare a come i loro marchi possano connettersi con particolari comunità Metaverso per suscitare fiducia e fedeltà nei loro clienti. Sperimentare con i propri strumenti e beni virtuali personali è una mossa intelligente in questo momento. Dovreste iniziare a sottoporre i vostri avatar a dei test e a studiare come creare eventi virtuali e contenuti ludici.

Non c'è dubbio che verranno create nuove norme per affrontare la natura mutevole del panorama digitale, in particolare per quanto riguarda lo sviluppo dei sistemi DeFi. Tuttavia, una cosa è certa: il Metaverso è arrivato e la nostra società tradizionale non sarà più la stessa. L'unica cosa che ci resta da fare è capire come i due mondi diversi possano coesistere.

Per avere successo nel mondo virtuale, non basta la creatività. Le aziende che vorranno avere successo nel Metaverso dovranno adottare una mentalità incentrata sull'utente e innovare sulla base di un modello commerciale decentralizzato e trasparente. Guardate quanto velocemente si stanno sviluppando questi settori grazie al fatto che le nuove generazioni sono cresciute con Internet e gli smartphone. Se la vostra azienda è in grado di catturare l'attenzione della generazione che è cresciuta insieme al Metaverso in una fase iniziale, potreste assistere a una rapida espansione.

# Conclusione

Questa tesi ha esaminato i potenziali usi della tecnologia blockchain e ha sottolineato la rilevanza e il valore della tecnologia. La tesi riconosce che l'applicabilità della tecnologia blockchain va ben oltre la moneta virtuale bitcoin. In realtà, questa tesi dimostra che il bitcoin è un uso piuttosto negativo di questa tecnologia, dato che consente agli utenti di spostare denaro e operare in modo anonimo, portando a usi sospetti. Diversi altri usi della tecnologia blockchain sono discussi nel corso di questa tesi utilizzando la letteratura attuale.

L'industria finanziaria può trarre vantaggio dalla tecnologia blockchain in diversi modi. Quando gli intermediari non necessari e costosi vengono eliminati da più processi, la tecnologia può ridurre i costi e aumentare l'efficienza. La tecnologia blockchain riduce i rischi quando un numero minore di beni è coinvolto nelle transazioni. Grazie alla natura distribuita delle blockchain pubbliche, la trasparenza aumenta e la sicurezza è garantita quando le informazioni non possono essere alterate. Le blockchain private hanno recentemente acquisito popolarità, in particolare nel settore bancario, in quanto consentono l'archiviazione di informazioni sensibili e la gestione dei permessi di accesso ai record.

Nella loro ricerca, Malinova e Park (2016) hanno analizzato il trading di titoli basato su blockchain e hanno scoperto che la tecnologia blockchain può essere utilizzata per modificare le strutture di mercato. Pinna e Ruttenberg (2016), invece, sostengono che i contratti intelligenti hanno il potenziale per sostituire una serie di attività attualmente svolte da intermediari post-trade obbligatori nei mercati finanziari.

Come si può notare, la tecnologia blockchain consente oggi un'ampia varietà di applicazioni nel settore finanziario e presto ne consentirà molte altre. Poiché la tecnologia blockchain è ancora nelle prime fasi di sviluppo, è impossibile prevedere quali tipi di applicazioni saranno implementate e in che misura. È inoltre essenziale notare che alcuni servizi possono essere più adatti alla tecnologia blockchain rispetto ad altri.

Poiché la tecnologia blockchain è una tecnologia relativamente nuova, c'è abbastanza spazio per ulteriori studi sull'argomento. Questa tesi ha inoltre esaminato le implicazioni della tecnologia blockchain nell’ambito del Metaverso e le rivoluzioni che potrebbe portare. Il modo in cui la realtà

virtuale e il Metaverso influenzeranno la vita degli "esseri umani normali" è un argomento di studio interessante. Si tratta, a mio avviso, di un tema davvero entusiasmante e attuale, che tuttavia è stato limitato da questa tesi.

Prima di poter assistere ad una diffusione su larga scala di questa tecnologia ci vorrà ancora del tempo, in modo da consentire alla tecnologia di svilupparsi ulteriormente e di ideare nuove funzioni e possibili applicazioni. Per il momento possiamo concludere che sia la blockchain che il Metaverso saranno presto parte della nostra quotidianità e rivoluzioneranno molti ambiti della nostra vita.

## Bibliografia


Malinova, K. and Park, A. (2016). Market Design with Blockchain Technology by Katya Malinova, Andreas Park :: SSRN. *Market Design with Blockchain Technology by Katya Malinova, Andreas Park :: SSRN*. [online]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2785626.

The Economist. (2015). The trust machine | The Economist. *The trust machine | The Economist*. [online]. Available from: https://www.economist.com/leaders/2015/10/31/the-trust-machine.

The Economist. (2016). Hype springs eternal | The Economist. *Hype springs eternal | The Economist*. [online]. Available from: https://www.economist.com/finance-and-economics/2016/03/19/hype-springs-eternal.

Times, F. (2016). Blockchain can create financial sector jobs as well as kill them | Financial Times. *Blockchain can create financial sector jobs as well as kill them | Financial Times*. [online]. Available from: https://www.ft.com/content/3a9ef8d8-33d5-11e6-bda0-04585c31b153.

Blog, E.F. (2015). On Public and Private Blockchains | Ethereum Foundation Blog. *Ethereum Foundation Blog*. [online]. Available from: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

Sheldon, R. (2021). A timeline and history of blockchain technology. *WhatIs.com*. [online]. Available from: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology.

Javatpoint. History of Blockchain - Javatpoint. *www.javatpoint.com*. [online]. Available from: https://www.javatpoint.com/history-of-blockchain.

Academy, B. (2019). History of Blockchain | Binance Academy. *Binance Academy*. [online]. Available from: https://academy.binance.com/en/articles/history-of-blockchain?ref=AZTKZ9XS&utm_source=BinanceTwitter&utm_medium=GlobalSocial&utm_campaign=GlobalSocial.

Deloitte US. (2016). Making blockchain real for customer loyalty programs | Deloitte US. *Deloitte United States*. [online]. Available from: https://www2.deloitte.com/us/en/pages/financial-services/articles/making-blockchain-real-customer-loyalty-rewards-programs.html.

Aggarwal & Salangsang, N.& D. (2022). How DeFi and Web 3.0 will shape the future of finance- The Asian Banker. *How DeFi and Web 3.0 will shape the future of finance- The Asian Banker*. [online]. Available from:

https://www.theasianbanker.com/updates-and-articles/decentralised-finance-and-web-3.0-shaping-the-future-of-financial-services.

Studio, C. (2020). Web 3.0 Explained Simply: Definition & Examples. *Web 3.0 Explained Simply: Definition & Examples*. [online]. Available from: https://www.cryptostudio.com/crypto-abc/web3/?utm_term=web%203.0&utm_campaign=Search+-+EN+-+Web3&utm_source=adwords&utm_medium=ppc&hsa_acc=5931252456&hsa_cam=17273574137&hsa_grp=139282006960&hsa_ad=598173251689&hsa_src=g&hsa_tgt=kwd-296468071419&hsa_kw=web%203.0&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjw6_CYBhDjARIsABnuSzo489Rvjw1WkerNEFuLMTttB-fzaHfFiliKXvPGRj0ES7puCuaVfXUaAo3IEALw_wcB.

Britannica. (2016). virtual reality - Education and training. *Encyclopedia Britannica*. [online]. Available from: https://www.britannica.com/technology/virtual-reality/Education-and-training.

IBERDROLA, I. Virtual Reality, the technology of the future - Iberdrola. *Iberdrola*. [online]. Available from: https://www.iberdrola.com/innovation/virtual-reality#:~:text=Virtual%20Reality%20(VR)%20is%20a,Virtual%20Reality%20headset%20or%20helmet..

Blockchain Council. (2022). Metaverse Vs. Virtual Reality: A Detailed Comparison -. *Metaverse Vs. Virtual Reality: A Detailed Comparison* -. [online]. Available from: https://www.blockchain-council.org/metaverse/metaverse-vs-virtual-reality/.

Kilzi, M. (2022). Council Post: The New Virtual Economy Of The Metaverse. *Forbes*. [online]. Available from: https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/20/the-new-virtual-economy-of-the-metaverse/?sh=b8fd23346d83.

Blockchains, 101. (2020). A Guide To Merkle Trees - 101 Blockchains. *101 Blockchains*. [online]. Available from: https://101blockchains.com/merkle-trees/.

Republic, T. (2021). Cryptocurrency and blockchain jobs listings skyrocket in 2021 | TechRepublic. *Cryptocurrency and blockchain jobs listings skyrocket in 2021 | TechRepublic*. [online]. Available from: https://www.techrepublic.com/article/listings-for-cryptocurrency-and-blockchain-jobs-skyrocket-in-2021/.

Academy, B. (2021). What Is a 51% Attack? | Binance Academy. *Binance Academy*. [online]. Available from: https://academy.binance.com/en/articles/what-is-a-51-percent-attack.

Academy, B. (2020). Who Is W Scott Stornetta? *Bit2Me Academy*. [online]. Available from: https://academy.bit2me.com/en/who-is-w-scott-stornetta/.

Developer, B. Transactions — Bitcoin. *Transactions — Bitcoin*. [online]. Available from: https://developer.bitcoin.org/devguide/transactions.html.

Developer, B. Wallets — Bitcoin. *Wallets — Bitcoin*. [online]. Available from: https://developer.bitcoin.org/devguide/wallets.html.

Team, C. (2022). Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity - Chainalysis. *Chainalysis*. [online]. Available from: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

Team, C. (2022). Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity - Chainalysis. *Chainalysis*. [online]. Available from: https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

Clark, M. (2021). People are spending millions on NFTs. What? Why? *NFTs, explained: what they are and why they're suddenly worth millions - The Verge*. [online]. Available from: https://www.theverge.com/22310188/nft-explainer-what-is-blockchain-crypto-art-faq.

Cointelegraph. Decentralized finance (DeFi): A beginner's guide. *Cointelegraph*. [online]. Available from: https://cointelegraph.com/defi-101/defi-a-comprehensive-guide-to-decentralized-finance.

Cointelegraph. Soft fork vs. hard fork: Differences explained. *Cointelegraph*. [online]. Available from: https://cointelegraph.com/blockchain-for-beginners/soft-fork-vs-hard-fork-differences-explained.

Cointelegraph. What are DApps? Everything there is to know about decentralized applications. *Cointelegraph*. [online]. Available from: https://cointelegraph.com/defi-101/what-are-dapps-everything-there-is-to-know-about-decentralized-applications.

Cointelegraph. What is a decentralized autonomous organization, and how does a DAO work? *Cointelegraph*. [online]. Available from: https://cointelegraph.com/ethereum-for-beginners/what-is-a-decentralized-autonomous-organization-and-how-does-a-dao-work.

ConsenSys. Blockchain for Digital Identity | Real World Blockchain Use Cases | ConsenSys. *ConsenSys*. [online]. Available from: https://consensys.net/blockchain-use-cases/digital-identity/.

Digiconomist. (2022). Bitcoin Energy Consumption Index - Digiconomist. *Digiconomist*. [online]. Available from: https://digiconomist.net/bitcoin-energy-consumption.

Digiconomist. (2022). Ethereum Energy Consumption Index - Digiconomist. *Digiconomist*. [online]. Available from: https://digiconomist.net/ethereum-energy-consumption.

Ethereum Foundation Blog. (2021). Ethereum's energy usage will soon decrease by ~99.95% | Ethereum Foundation Blog. *Ethereum Foundation Blog*. [online]. Available from: https://blog.ethereum.org/2021/05/18/country-power-no-more/.

ethereum.org. Decentralized autonomous organizations (DAOs) | ethereum.org. *ethereum.org*. [online]. Available from: https://ethereum.org/en/dao/#what-are-daos.

ethereum.org. Ethereum Energy Consumption | ethereum.org. *ethereum.org*. [online]. Available from: https://ethereum.org/en/energy-consumption/.

ethereum.org. Non-fungible tokens (NFT) | ethereum.org. *ethereum.org*. [online]. Available from: https://ethereum.org/en/nft/.

Euromoney.com. Blockchain Explained: What is blockchain? | Euromoney Learning. *Blockchain Explained: What is blockchain? | Euromoney Learning*. [online]. Available from: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain.

Fabric Ventures. (31.12.2019). Medium: What is Web 3.0 & Why It Matters. Mersh & Muirhead, M.& R. (2021). What Is Web 3.0 & Why It Matters. Written by Max Mersch and Richard… | by Fabric Ventures | Fabric Ventures | Medium. *Medium*. [online]. Available from: https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b.

Frankenfield & Mansa, J.& J. (2022). What Is Double-Spending in a Blockchain? *Investopedia*. [online]. Available from: https://www.investopedia.com/terms/d/doublespending.asp.

Frankenfield & Khartit, J.& K. (2022). What Is the UTXO Model? *Investopedia*. [online]. Available from: https://www.investopedia.com/terms/u/utxo.asp.

Gensler, G. (2018). MIT 15.S12 Blockchain and Money, Fall 2018. *YouTube*. [online]. Available from: https://www.youtube.com/playlist?list=PLUl4u3cNGP63UUkfL0onkxF6MYgVa04Fn.

Geroni, D. (2020). What is a Public Blockchain? Beginner's Guide - 101 Blockchains. *101 Blockchains*. [online]. Available from: https://101blockchains.com/what-is-a-public-blockchain/.

GlobalTranz. (2018). How Blockchain Technology Can Transform Logistics - Part 1. *GlobalTranz*. [online]. Available from: https://www.globaltranz.com/blockchain-technology-transform-logistics/.

Gulley, A. (2021). Understanding Ethereum. a simple explanation of Ethereum and… | by allan.g | Medium. *Medium*. [online]. Available from: https://allan-gulley.medium.com/understanding-ethereum-819c2096b613.

Hackl, C. (2021). What Are DAOs And Why You Should Pay Attention. *Forbes*. [online]. Available from: https://www.forbes.com/sites/cathyhackl/2021/06/01/what-are-daos-and-why-you-should-pay-attention/?sh=57a87e0c7305.

Hayes, A. (2022). Blockchain Facts: What Is It, How It Works, and How It Can Be Used. *Investopedia*. [online]. Available from: https://www.investopedia.com/terms/b/blockchain.asp.

Hayes, A. (2022). Who Is Satoshi Nakamoto? What Is Their Net Worth? *Investopedia*. [online]. Available from: https://www.investopedia.com/terms/s/satoshi-nakamoto.asp.

Higgins, M. (2021). Council Post: Blockchain In Supply Chain. *Forbes*. [online]. Available from: https://www.forbes.com/sites/forbestechcouncil/2021/11/08/blockchain-in-supply-chain/?sh=743cbffd4e1a.

Hamacher, Hussey, Chipolina. (2021). What Is Cardano (ADA)? | The Beginner's Guide - Decrypt. *Decrypt*. [online]. Available from: https://decrypt.co/resources/cardano.

IBM. What are smart contracts on blockchain? | IBM. *IBM*. [online]. Available from: https://www.ibm.com/topics/smart-contracts.

IBM. What is Blockchain Technology? - IBM Blockchain | IBM. *IBM*. [online]. Available from: https://www.ibm.com/topics/what-is-blockchain.

IBM. Blockchain for Digital Identity and Credentials | IBM. *IBM*. [online]. Available from: https://www.ibm.com/blockchain/identity.

Kapilkov, M. . (2020). Future elections could be held on the Cardano blockchain, says Hoskinson. *Cointelegraph*. [online]. Available from: https://cointelegraph.com/news/future-elections-could-be-held-on-the-cardano-blockchain-says-hoskinson.

Kattwinkel, O. et al. (2020). pub H-BRS | Technical Fundamentals of Blockchain Systems. *pub H-BRS | Technical Fundamentals of Blockchain Systems*. [online]. Available from: https://doi.org/10.18418/978-3-96043-081-0.

Liebkind , J. (2020). How Blockchain Technology Can Prevent Voter Fraud. *Investopedia*. [online]. Available from: https://www.investopedia.com/news/how-blockchain-technology-can-prevent-voter-fraud/.

Lutkevich, B. (2021). What is a Nonce? - Cryptographic Nonce from SearchSecurity. *SearchSecurity*. [online]. Available from: https://www.techtarget.com/searchsecurity/definition/nonce.

MarketDao. (2020). » The Different Types of Cryptocurrency Tokens Explained. *» The Different Types of Cryptocurrency Tokens Explained*. [online]. Available from: https://blog.makerdao.com/the-different-types-of-cryptocurrency-tokens-explained/.

Melinek, J. et al. (2022). Report: VCs Invested $33B in Crypto and Blockchain Startups in 2021 - Blockworks. *Blockworks*. [online]. Available from: https://blockworks.co/report-vcs-invested-33b-in-crypto-and-blockchain-startups-in-2021/.

Non-Interactive Proofs of Proof-of-Work. Non-Interactive Proofs of Proof-of-Work. *Non-Interactive Proofs of Proof-of-Work*. [online]. Available from: https://nipopows.com/.

O'Reilly. Mastering Bitcoin. *O'Reilly Online Learning*. [online]. Available from: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch08.html.

O'Reilly. Mastering Bitcoin. *O'Reilly Online Learning*. [online]. Available from: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch04.html.

O'Reilly. Mastering Bitcoin. *O'Reilly Online Learning*. [online]. Available from: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch05.html.

O'Reilly. Mastering Bitcoin. *O'Reilly Online Learning*. [online]. Available from: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch07.html.

Pate, D.L. (2022). The Top Skills In Demand For 2020—And How to Learn Them. *The Top Skills In Demand For 2020—And How to Learn Them*. [online]. Available from: https://www.linkedin.com/business/learning/blog/top-skills-and-courses/the-skills-companies-need-most-in-2020and-how-to-learn-them.

Polkadot. Polkadot Network. *Polkadot Network*. [online]. Available from: https://polkadot.network/technology/.

Poston, H. (2022). Blockchain and asymmetric cryptography - Infosec Resources. *Infosec Resources*. [online]. Available from: https://resources.infosecinstitute.com/topic/blockchain-and-asymmetric-cryptography/.

Przybilla, D. (2021). Learning Ergo 101 : eUTXO explained for human beings. *Medium*. [online]. Available from: https://dav009.medium.com/learning-ergo-101-blockchain-paradigm-eutxo-c90b0274cf5e.

PwC. (n.d.). PwC: Blockchain in Logistics. https://www.pwc.de/de/strategie-organisation-prozesse-systeme/blockchain-in-logistics.pdf

River Financial. Bitcoin's UTXO Model | River Learn - Bitcoin Technology. *River Financial*. [online]. Available from: https://river.com/learn/bitcoins-utxo-model/.

Rosic, A. (2016). What Are Smart Contracts? [Ultimate Beginner's Guide to Smart Contracts]. *Blockgeeks*. [online]. Available from: https://blockgeeks.com/guides/smart-contracts/.

Sanchez, F. Cardano's Extended UTXO accounting model – built to support multi-assets and smart contracts - IOHK Blog. *IOHK*. [online]. Available from: https://iohk.io/en/blog/posts/2021/03/11/cardanos-extended-utxo-accounting-model/.

Sanchez, F. Cardano's Extended UTXO accounting model – built to support multi-assets and smart contracts (part 2) - IOHK Blog. *IOHK*. [online]. Available from: https://iohk.io/en/blog/posts/2021/03/12/cardanos-extended-utxo-accounting-model-part-2/.

Seth, S. (2022). Public, Private, Permissioned Blockchains Compared. *Investopedia*. [online]. Available from: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

Sharma, R. (2022). Non-Fungible Token (NFT): What It Means and How It Works. *Investopedia*. [online]. Available from: https://www.investopedia.com/non-fungible-tokens-nft-5115211.

Sharma, R. (2022). What Is Decentralized Finance (DeFi) and How Does It Work? *Investopedia*. [online]. Available from: https://www.investopedia.com/decentralized-finance-defi-5113835.

Tardi, C. (2022). Application-Specific Integrated Circuit (ASIC) Miner. *Investopedia*. [online]. Available from: https://www.investopedia.com/terms/a/asic.asp.

Turner (guest), D.M. (2019). Summary of cryptographic algorithms - according to NIST. *Summary of cryptographic algorithms - according to NIST*. [online]. Available from: https://www.cryptomathic.com/news-events/blog/summary-of-cryptographic-algorithms-according-to-nist.

Vermaak, W. (2022). What Is Web 3.0? | CoinMarketCap. *CoinMarketCap Alexandria*. [online]. Available from: https://coinmarketcap.com/alexandria/article/what-is-web-3-0.

Vote Australia. (2022). Blockchain Voting - Vote Australia. *Vote Australia*. [online]. Available from: https://www.voteaustralia.org.au/blockchain_voting.

Wiesflecker, L. (2020). Bitcoin Mempool — Simply explained. *Medium*. [online]. Available from: https://medium.com/coinmonks/bitcoin-mempool-simply-explained-7f76be235e85.

Zhang, S. and Lee, J.-H. (2019). Redirecting. *Redirecting*. [online]. Available from: https://doi.org/10.1016/j.icte.2019.08.001.