Blockchain, Web 3.0 e NFTs: i profili tecnici

Andrea Visconti (Orcid 0000-0001-5689-8575)
Professore Associato di Informatica, Università degli Studi di Milano

Simone Pelizzola
Dottorando di Ricerca in Informatica, Università degli Studi di Milano
DOI: 10.54103/milanoup.150.c178

Abstract: Il lavoro ricostruisce i profili tecnici della blockchain, degli Smart Contracts e degli NFTs quali mattoncini di base per lo sviluppo di nuove forme di commercio e le crittomonete, visto che rappresentano lo strumento di supporto di questi nuovi modelli di business. La natura decentralizzata delle Blockchain permetterà di produrre e negoziare nuovi contenuti digitali attraverso transazioni trasparenti e tracciabili senza la necessità di coinvolgere intermediari. Per questo si sottolinea come gli utenti che sapranno cogliere le nuove opportunità legate alla finanza decentralizzata (DeFi), al metaverso e alle nuove tecnologie avranno un vantaggio competitivo nell'evoluzione del World Wide.

The work reconstructs the technical profiles of Blockchain, Smart Contracts and NFTs as essential building blocks for developing new forms of commerce and cryptocurrencies, representing the fundamental tool to support these new business models. The decentralized nature of Blockchains will allow new digital content to be produced and traded through transparent and traceable transactions without the need to involve intermediaries. For this reason, it is underlined that users who can seize the new opportunities linked to decentralized finance (DeFi), the Metaverse and new technologies will have an essential competitive advantage in the evolution of the World Wide Web.

1. Introduzione alla Blockchain

Il concetto di blockchain nasce nel 2008, quando Nakamoto [1] ne ha introdotto la struttura come mezzo per garantire in modo sicuro e affidabile le transazioni di monete virtuali, in particolare di Bitcoin. A seguito dell'implementazione pratica del modello del 2009 e al suo successo, lo schema ha riscosso sempre maggiori attenzioni ed è stato applicato in diversi ambiti dove c'è

grande necessità di sistemi per conservare e garantire proprietà e autenticità di dati e/o transazioni.

Il modello di blockchain proposto da Nakamoto aveva lo scopo di creare un sistema di scambio di risorse economiche (Bitcoin) che rispettasse elevati standard di sicurezza senza necessitare di un organo centrale di controllo, gestione e verifica di patrimoni e transazioni, ruolo solitamente ricoperto dalle banche. L'idea sottostante questo schema, ripreso negli altri casi di blockchain, consiste nel rappresentare i dati in catene blocchi in cui ogni anello dipende dal blocco precedente. Diversi casi di blockchain si basano su differenti tecniche per collegare i blocchi, per verificare l'autenticità degli stessi e per effettuare transazioni in modo coerente con la struttura.

Il sistema Bitcoin presentato in [1], ad esempio, consiste in un insieme di monete elettroniche, ognuna delle quali corrisponde a una catena di firme digitali. Ogni volta che una moneta viene trasferita, il vecchio possessore aggiunge alla catena un estratto cifrato (hash) dell'identificativo precedente della moneta e di un identificativo (chiave pubblica) del nuovo possessore, firmandolo digitalmente. Diventa facile, in questo modo, verificare una catena di transazioni.

Questo modello presenta due principali questioni relative alla sicurezza. La prima riguarda la possibilità che un utente esterno o interno al sistema provi a modificare una transazione passata, la seconda riguarda l'eventualità in cui il possessore di una moneta provi a venderla a due utenti diversi, comportando dunque la necessità di approvare le transazioni.

Il primo problema è strettamente correlato al metodo di collegamento dei blocchi, nel caso in esempio alla sicurezza della funzione di hash utilizzata, mentre per il secondo problema sono state proposte e implementate diverse soluzioni.

1.1. Struttura della blockchain

In [2] gli autori descrivono la blockchain come composta da tre strati essenziali, uno di rete, uno di dati e uno di applicazioni. I dati sono chiaramente la parte essenziale della blockchain, attorno ai dati ruota il concetto stesso di questo schema. Questo strato è costituito dai blocchi, dalle tecniche che ne garantiscono la sicurezza e dai collegamenti tra essi. Lo strato della rete rappresenta, invece, tutto ciò che è relativo alle interazioni che coinvolgono gli elementi di una blockchain. Coinvolge, ad esempio, l'insieme dei protocolli adottati per lo scambio di dati o i metodi utilizzati per garantire unicità alle transazioni e approvarle all'interno della struttura (protocolli di consenso). Infine, lo strato delle applicazioni è composto dai prodotti che fanno uso della struttura della blockchain, dunque l'insieme delle aree di applicazione di questa tecnologia e le diverse varianti adattate ai vari bisogni di mercato.

Lo strato dei dati

La struttura dei dati di una blockchain segue il modello proposto da Nakamoto [1] e sfrutta alcune classi di algoritmi di importanza fondamentale per la crittografia.

I dati: i dati memorizzati nella blockchain sono transazioni, registrazioni di movimenti e modifiche che riguardano l'oggetto di interesse della struttura. Nel caso dei Bitcoin rappresentano i possessori di una moneta virtuale e tutti i passaggi precedenti che hanno portato alla situazione presente.

I blocchi: i blocchi sono strutture dati che contengono le informazioni di cui sopra. Solitamente un blocco ha un'intestazione in cui sono presenti le informazioni che identificano la blockchain, degli hash che rappresentano il blocco precedente nella catena e la catena stessa, un'indicazione temporale, ad esempio l'istante dell'ultima modifica, delle informazioni utili all'autenticazione del blocco. Oltre all'intestazione, c'è il corpo del blocco che contiene l'insieme delle transazioni.

La blockchain: la blockchain, letteralmente catena di blocchi, è l'insieme dei blocchi di dati, organizzati in modo tale che la struttura sia immutabile nella pratica. Per ottenere questo risultato si fa uso di funzioni hash, algoritmi crittografici che estraggono un dato di lunghezza fissa partendo da un dato di input qualsiasi, e che soddisfano alcune proprietà che rendono computazionalmente difficile risalire al dato originario. In particolare, ogni blocco sarà caratterizzato dall'hash dei blocchi precedenti, garantendo la sicurezza della struttura poiché un cambiamento a metà della catena avrà influenza su tutto il seguito. Per risparmiare memoria si adotta la struttura di Merkle Tree, un albero di hash dei blocchi in cui l'hash di una foglia dipende solo dagli hash dei suoi figli e dall'hash della radice dell'albero. In questo modo, avendo a disposizione le foglie finali, si può verificare l'integrità dell'intera catena.

Firma digitale: per tenere traccia degli utenti coinvolti nelle transazioni, l'hash di un blocco coinvolge anche, come suo input, la firma digitale dell'utente che effettua la transazione. Questa firma è l'output di una funzione asimmetrica, o one-way function, cioè una funzione matematica la cui funzione inversa è computazionalmente molto complessa da valutare in assenza di un parametro segreto, ma che soddisfa una qualche proprietà molto semplice da verificare, dimostrandone l'autenticità. Queste funzioni sono molto comuni in crittografia e garantiscono la sicurezza di una cifratura.

Lo strato di rete

Lo strato di rete è caratterizzato da due aspetti principali. Il primo è l'organizzazione degli utenti e come essi interagiscono con la blockchain, il secondo è dato dalle tecniche che garantiscono l'autenticazione e la verifica di validità dei blocchi da parte degli utenti.

Per quanto riguarda l'organizzazione degli utenti, distinguiamo le blockchain in tre grandi categorie [3, 4]. Le *blockchain pubbliche* sono totalmente decentralizzate e seguono il modello peer to peer (P2P). In questi casi, gli utenti utilizzano e sviluppano i nodi della rete allo stesso tempo, hanno quindi tutti il controllo, seppur dietro comune approvazione, della rete. Di conseguenza, ogni utente ha anche una parte di controllo, solitamente proporzionale alla quantità di risorse impiegate, riguardo l'approvazione di una transazione.

Le *blockchain private* sono caratterizzate da un'autorità centrale che determina chi può accedere al sistema e ne autentica l'ingresso. Inoltre, il permesso di modifica e di operare transazioni può essere sottoposto al vaglio dell'autorità centrale.

Esistono, infine, soluzioni ibride, ad esempio le *blockchain di consorzio*, nelle quali parte del ruolo dell'autorità centrale del caso privato è ricoperto da un insieme ridotto di utenti che devono autorizzare (all'unanimità o no) le transazioni, oppure approvare l'ingresso di un nuovo utente o entrambe le cose. Altri casi ibridi sono quelli in cui parte delle informazioni sono accessibili a tutta la rete, mentre altre sono tenute private per i singoli utenti.

In base al tipo di rete adottato possono cambiare i modelli utilizzati per approvare le transazioni (i protocolli di consenso), come vedremo nella Sezione 1.2.

Applicazioni della blockchain

In seguito all'implementazione di successo di una blockchain in Bitcoin, sempre più applicazioni di questo modello sono sorte, nei più disparati ambiti [10, 11]. Le caratteristiche di questa tecnologia, quindi l'immutabilità della struttura, la possibilità di non avere un garante centrale, l'essere una struttura distribuita, dove le transazioni vengono trasmesse a tutti i nodi, in alcuni casi per approvazione, rendono la blockchain un oggetto versatile e sicuro dove salvare e condividere dati e transazioni. Per queste ragioni le applicazioni comprendono monete digitali, contratti, servizi finanziari, tracciabilità di filiere produttive, comunità di agenti o di utenti, IoT e molti altri. Ne vedremo ora alcuni più nel dettaglio.

- *Crittovalute*: l'esempio più classico di utilizzo della blockchain è sicuramente il caso delle crittovalute, come Bitcoin, poi seguita da molti altri casi simili. Seppur costruiti utilizzando protocolli di consenso diversi, questi esempi sono tutti basati sull'utilizzo della struttura della blockchain per dimostrare la proprietà di una moneta digitale e registrarne le transazioni.
- *Proprietà smart:* le blockchain possono essere utilizzate per certificare il possesso di beni materiali o per depositare contratti che garantiscono l'acquisizione di un particolare bene materiale sotto certe condizioni.
- *Tracciabilità di filiere produttive:* certificare la qualità dei prodotti che vengono messi in commercio è un aspetto importante per le aziende che li producono, così com'è importante evitare che il sistema di controlli non venga raggirato. Per questo motivo, stanno emergendo sempre più aziende che

forniscono soluzioni blockchain per la registrazione dei documenti di certificazione di qualità della filiera produttiva di diversi prodotti. In questo modo, si ha la garanzia che ogni lotto registrato e segnalato nella documentazione registrata attraverso la blockchain rispetti gli standard qualitativi richiesti.

– *Informatica medica:* la registrazione e autenticità di referti medici ed esiti di esami è di fondamentale importanza per i pazienti e per le strutture mediche. Per questo motivo, diverse soluzioni sono state proposte, e alcune anche implementate, per creare strutture blockchain in cui inserire questi documenti.

Si trovano innumerevoli altri esempi di proposte teoriche e pratiche di applicazione della blockchain nei campi dell'IoT, delle telecomunicazioni, dei big data, della privacy, della finanza e non solo, che sfruttano il meglio possibile le potenzialità di sicurezza e condivisione garantite da questa tecnologia.

1.2. Protocolli di consenso

In una blockchain pubblica o ibrida si pone il problema di come assicurarsi che le transazioni registrate siano valide e, conseguentemente, di quali catene di hash fidarsi per effettuare una transazione, poiché qualche utente malevolo potrebbe provare ad approfittare dell'assenza di un'autorità che tiene tutto sotto controllo, ad esempio, provando a vendere più volte una risorsa in suo possesso. Solitamente per validare una transazione occorre l'approvazione di un certo numero di utenti, come proposto in [1], la quale viene concessa in base a criteri specifici. Questi algoritmi di verifica sono chiamati *protocolli di consenso* e ne sono stati sviluppati di diversi tipi [2, 4, 5].

Un protocollo di consenso deve essere efficace e consistente, dunque deve approvare ogni istanza corretta, anche in caso di presenza di utenti malevoli nel sistema.

Presentiamo di seguito alcuni tra i più diffusi protocolli di consenso.

– *Proof of Work (PoW):* questo è il modello proposto in [1] per Bitcoin e si basa sull'ipotesi che la maggior parte della potenza di calcolo coinvolta nella rete sia onesta. In questo protocollo, per istanziare un blocco (minare un Bitcoin ad esempio), è necessario risolvere un problema computazionalmente molto complicato ma facile da verificare, ad esempio invertire un particolare hash (cioè, trovare un input il cui hash rispetti determinate condizioni). Verificare che l'hash rispetti le condizioni è semplice, di conseguenza è altrettanto semplice fidarsi della bontà della creazione del blocco. Man mano che nuovi blocchi vengono istanziati e avvengono transazioni, la catena si allunga e si complica, rendendo sempre più complesso computazionalmente andare a interferire sul blocco di partenza. Per far fallire questo protocollo occorre essere in possesso della maggioranza della potenza di calcolo del sistema, in modo tale da riuscire a operare sui

blocchi più rapidamente di quanto la catena si riesca ad espandere, poiché a ogni espansione della catena corrisponde un identificativo temporale che autentica il nuovo stato della catena. La sicurezza di questo modello, in alcuni casi, come Bitcoin, dove allungare la catena garantisce un vantaggio economico, si basa anche sul fatto che più la catena si allunga più diventa computazionalmente complesso modificarla malevolmente, tanto che risulta più conveniente usare la propria potenza di calcolo per creare nuovi blocchi piuttosto che modificarne di vecchi.

– *Proof of Stake (PoS):* questo modello, adottato recentemente da Ethereum [6] in sostituzione del PoW, è applicabile in sistemi abbastanza diffusi e conferisce potere decisionale a chi possiede tante risorse. In particolare, ogni volta che una transazione viene proposta o un nuovo blocco viene aggiunto alla catena, viene chiesto a tutti o a una porzione selezionata casualmente degli utenti di approvare o rifiutare la modifica. Nel caso in cui una transazione venga confermata, gli utenti che l'hanno approvata ricevono un compenso mentre chi approva una transazione giudicata irregolare viene penalizzato. Il peso di ogni voto dipende dalla quantità di risorse del sistema possedute (o messe in gioco per quella singola transazione) dall'utente, così come l'entità della ricompensa o della penalizzazione. In questo modo, per poter intervenire malevolmente è necessario avere una quantità di risorse talmente elevata da rendere più remunerativo il comportamento onesto, tenendo conto di ricompense e penalizzazioni.
– *Practical Byzantine Fault Tolerance (PBFT):* questo protocollo è stato sviluppato espressamente per essere efficace nel caso in cui nella rete siano presenti utenti malevoli il cui comportamento non è prevedibile, ed è stato proposto per la prima volta in [7]. Questo modello consiste nel richiedere l'approvazione di una transazione agli altri utenti, la quale viene confermata nel momento in cui il numero di voti positivi ricevuti supera una certa soglia (o in alcuni casi il peso dei votanti favorevoli). Il protocollo PBFT è efficace nel momento in cui il numero degli utenti malevoli (o il loro peso) non supera la soglia di approvazione. Uno svantaggio di PoW rispetto a questi ultimi protocolli è che un blocco nuovo nel primo caso non è sicuro, ma lo diventa sempre più man mano che nuovi blocchi vengono collegati dopo di esso, mentre negli altri casi una volta che un'operazione è validata è definitivamente confermata.
– *Proof of Elapsed Time (PoET):* PoET è stato proposto da Intel [8] come alternativa a PoW evitando la necessità di minare i blocchi, risparmiando tempo di computazione, ma un'analisi teorica approfondita di questo modello è ancora oggi in fase di sviluppo [9]. Il protocollo consiste in un ambiente affidabile che controlla l'esecuzione delle transazioni assegnando a ogni utente che lo interroga un tempo di attesa dopo il quale potrà essere aggiunto un nuovo blocco. Quando un nuovo blocco viene aggiunto

alla catena, si verifica che il blocco sia valido e consistente con lo stato precedente e che il tempo di attesa associato sia passato. Quando il proprio tempo di attesa scade si aggiunge il nuovo blocco ricevuto alla catena e si trasmette il risultato alla rete.

Numerosi protocolli differenti da quelli presentati sono stati adottati in diverse blockchain, come DPOS, Ripple, Stellar, Threshold Relay, Proof of Authority (PoA), Proof of Burn (PoB), Proof of Activity, Proof of Space, Proof of Luck e molti altri.

1.3. Sicurezza della blockchain

Per quanto la struttura della blockchain sia il più possibile a prova di utenti malevoli, c'è la possibilità che l'integrità di una catena sia messa a rischio. Sono stati sviluppati, infatti, diversi attacchi [12], che minano la stabilità di una blockchain in base alle sue caratteristiche.

Un primo esempio è l'"attacco di maggioranza", o del 51%, in cui un utente malevolo controlla più di metà della potenza di calcolo della rete. In questo caso l'attaccante può essere in grado di modificare transazioni passate, biforcare una catena facendo poi approvare la propria versione o rifiutare transazioni valide, facendo pesare il proprio voto o allungando una catena di blocchi più rapidamente di un'altra o ancora invertendo un blocco prima che il resto della rete riesca ad accodarne di nuovi.

Un altro tipo di strategia malevola è quella del "minatore egoista", in cui un utente riesce a costruirsi in privato una catena più lunga di una già esistente biforcandola a un certo punto. Inserendola poi nel sistema e trasmettendola agli altri nodi, se il protocollo di consenso è adatto, potrebbe soppiantare il ramo originale ed essere accettata dal sistema.

La "doppia spesa" consiste, invece, nel creare due transazioni che riguardano lo stesso blocco, tentando di far apparire come precedente la versione malevola, in cui un bene viene trasferito all'utente di partenza o un suo alleato. Se la rete accetta la versione malevola, il truffatore potrebbe riuscire a effettuare un acquisto senza effettivamente spendere risorse, poiché a causa dei tempi di esecuzione all'interno della blockchain la transazione potrebbe venire considerata valida prima della conferma della rete.

Infine, il sistema blockchain e i server in cui vengono memorizzati portafogli digitali, profili di utenti, documenti e dati fanno sempre affidamento su funzioni crittografiche per garantire sicurezza e privacy. Di conseguenza queste infrastrutture si portano dietro tutte le vulnerabilità di cui questi algoritmi sono, o potrebbero essere in futuro, suscettibili.

2. Web 3.0, Wallets e Smart Contracts

La parola Web che tutti noi conosciamo si riferisce all'inizio dell'era digitale e alla prima fase di nascita della rete, nella quale gli utenti utilizzavano semplici browser per navigare pagine internet prevalentemente statiche scritte in HTML. In questo periodo, l'interazione fra gli utenti era molto limitata, ma la possibilità di rendere pubbliche informazioni che in precedenza risiedevano solo su libri, supporti cartacei o supporti digitali personali ha portato a uno stravolgimento tecnologico. Questa possibilità di condividere informazioni, memorizzate in una maniera centralizzata ma accessibili da tutti, si è sviluppata in una seconda fase, detta anche Web 2.0. I social media, le app, i blog, i podcast hanno avuto un grande sviluppo, rivoluzionando il mondo della comunicazione. Nonostante la diffusione su larga scala delle nuove tecnologie, permane il problema della gestione delle informazioni che sono memorizzate in maniera centralizzata su uno o più server e non sono aggiornate automaticamente quando ripetute su più piattaforme. La successiva evoluzione del Web mira a risolvere queste problematiche oltre che a introdurre nuovi paradigmi informatici. Il *Web 3.0* fa riferimento allo sviluppo di nuove tecnologie quali la Blockchain, gli Smart Contracts, le Criptovalute, l'intelligenza artificiale etc. La possibilità di memorizzare le informazioni in maniera decentralizzata fornirà un insieme di nuove possibilità alle persone che sapranno cogliere e sfruttare questo valore aggiunto.

Un portafogli digitale, o *wallet*, è uno strumento che permette agli utenti di interagire con le blockchain fornendo servizi quali la conservazione delle chiavi pubbliche e private, la gestione delle transazioni, la visualizzazione delle proprie crittomonete etc. In base alla modalità di gestione delle chiavi private degli utenti, i wallet possono essere catalogati in *hardware wallet* e in *software wallet*. I primi conservano le chiavi private su un dispositivo hardware esterno e gestito dall'utente. I secondi utilizzano un software locale o remoto per l'archiviazione delle proprie chiavi. Entrambe le soluzioni forniscono opportune interfacce grafiche (programmi, siti web, app) per la gestione delle chiavi necessarie per accedere ai servizi forniti dalle blockchains.

Gli *Smart Contracts*, programmi decentralizzati che sfruttano le caratteristiche intrinseche di specifiche blockchain, consentono di eseguire operazioni in maniera automatica senza la necessità di avere intermediari fidati. Queste operazioni, che si basano su meccanismi di transizione di stato, consentendo l'implementazione di funzionalità più o meno complicate sfruttabili in tutti quei settori dove gli attori in gioco hanno interessi contrastanti e non si fidano l'uno dell'altro. Le istruzioni, i parametri e lo stato di uno Smart Contract sono informazioni pubbliche e garantiscono la trasparenza dell'esecuzione di tutte le operazioni. Inoltre, per ridurre il rischio di frodi, le regole stabilite a priori all'interno di uno Smart Contract non possono essere modificate durante l'esecuzione dello

stesso, impedendo quindi che un partecipante disonesto possa interferire con il sistema all'insaputa degli altri.

Tutte le operazioni eseguite dagli Smart Contracts devono a loro volta essere memorizzate per tener traccia dei cambiamenti in atto. Questo compito è affidato alle blockchain che, grazie alla loro struttura distribuita, suddividono il carico computazionale tra i partecipanti della rete e garantiscono l'immutabilità delle transazioni.

Gli Smart Contracts, inizialmente introdotti con la Blockchain Ethereum, sono generalmente considerati un elemento fondamentale per lo sviluppo della finanza decentralizzata (DeFi) e per tutte le applicazioni legate ai non-fungible token (NFT).

3. Asset digitali e NFTs

Un *asset digitale* è un oggetto materiale o un contenuto immateriale rappresentato attraverso una sorgente binaria e che include i diritti per il suo utilizzo. Nel Web esistono diversi tipi di contenuti digitali:

- contenuti digitali generati dagli utenti con un valore economico potenziale – User-Generated Content (UGC);
- contenuti digitali professionali, generati da esperti o aziende per i quali si presta maggiore attenzione al diritto d'autore – Professional-Generated Content (PGC). Per i contenuti a pagamento, la dilagante pirateria può causare un danno economico considerevole al proprietario dell'asset, alla piattaforma che gestisce i contenuti e anche ai potenziali acquirenti;
- contenuti digitali generati impiegando l'intelligenza artificiale – Artificial Intelligence-Generated Content (AIGC). Il processo di creazione di questi contenuti è automatizzato e spesso gestito o modellato degli utenti.

Un asset digitale può essere associato a un *Non-Fungible-Token* (NFT), cioè un identificatore digitale univoco registrato su una blockchain, utilizzato per certificare la proprietà e l'autenticità dell'asset. Gli NFTs non possono essere copiati, sostituiti o suddivisi, ma possono essere trasferiti dal proprietario, consentendone la vendita e lo scambio. Gli NFTs possono contenere riferimenti a opere d'arte, foto, video, audio etc. e differiscono dalle crittovalute per le loro proprietà intrinseche. Infatti, gli NFTs sono unici e non possono essere scambiati con altri simili. Questa caratteristica li rende adatti a proteggere la proprietà intellettuale.

Gli NFTs possono essere negoziati utilizzando appositi Smart Contracts. Ogni volta che avviene un acquisto o uno scambio su una piattaforma informatica, il creatore dell'NFT può guadagnare delle royalties. Negli ultimi anni, lo scambio di NFTs è aumentato in maniera considerevole e gli stessi sono stati utilizzati anche come investimenti speculativi.

Gli NFTs sono utilizzati in diversi ambiti quali:

- attività ludiche: gli NFTs consentono agli utenti di possedere determinati componenti di un gioco promuovendo di conseguenza il suo sistema economico. Questo andrà a vantaggio sia degli sviluppatori, sia dei giocatori che, teoricamente, possono guadagnare delle royalties ogni volta che un loro asset digitale viene venduto/acquistato;
- eventi virtuali: gli NFTs sono legati al processo di emissione di biglietti univoci per determinati eventi virtuali. Grazie agli Smart Contracts è possibile scambiare in maniera trasparente questi biglietti senza richiedere l'intervento di terzi;
- beni digitali collezionabili: gli NFTs sono utilizzati nel processo di trasformazione di oggetti collezionabili in formati digitali. Essi consentono agli artisti di trasferire proprietà e contenuti a terzi senza avvalersi di intermediari, assicurandosi la ricezione di una quota predeterminata delle royalties ogni volta che l'asset viene scambiato su una piattaforma;
- Metaverso: gli NFTs sono utilizzati nel Metaverso sfruttando le caratteristiche descritte nei punti precedenti, ma anche per lo scambio di beni e proprietà virtuali (appezzamenti di terreno, edifici, dispositivi indossabili...) da cui gli utenti possono trarre profitti, per esempio affittando spazi virtuali per attività o eventi.

Gli NFTs necessitano di un registro distribuito sottostante – i.e. la Blockchain – per conservare informazioni e transazioni relative alla negoziazione degli stessi attraverso una rete peer-to-peer. Questo registro distribuito deve possedere una serie di caratteristiche fondamentali quali la sicurezza, la completezza e la disponibilità delle informazioni, in modo da consentire la creazione e lo scambio degli NFTs fra gli utenti della rete.

Il processo di generazione di un NFT può avvenire in due modi: NFT creato dal proprietario, NFT creato dall'acquirente. Nel primo caso, un NFT viene generato e poi venduto seguendo questo processo:

1. Digitalizzazione di un NFT: il proprietario dell'NFT, dopo aver verificato che le informazioni in suo possesso sono corrette, inizia il processo di creazione di un NFT digitalizzando i dati grezzi in un formato appropriato.
2. Archiviazione di un NFT: il proprietario dell'NFT memorizza i dati grezzi in un database esterno oppure all'interno della blockchain. In questo secondo caso, si dovrà pagare un corrispettivo in crittomente per l'attività di memorizzazione dei dati.
3. Firma di un NFT: il proprietario dell'NFT firma la transazione e la invia a uno Smart Contract.
4. Creazione e commercio di un NFT: dopo che lo Smart Contract riceve tutte le informazioni del caso, inizia il processo di creazione dell'asset digitale con la registrazione dell'NFT sulla blockchain, dando inizio alla possibile attività di negoziazione.

Nel secondo caso, viene generato un modello di NFT che ogni utente può personalizzare e riempire di determinati contenuti seguendo questo processo:

1. Creazione del modello: l'ideatore del progetto genera un modello tramite Smart Contract, definendo regole e caratteristiche di base degli NFTs.
2. Personalizzazione degli NFTs: una volta trovato un acquirente, un NFT può essere personalizzato attraverso una serie di funzionalità aggiuntive, per esempio selezionandole da un database definito al momento della creazione del modello.
3. Creazione e commercio degli NFTs: il processo di creazione e negoziazione inizia con la registrazione dello stesso sulla Blockchain. Tutte le procedure sono condotte attraverso Smart Contracts. Gli NFTs creati verranno memorizzati in modo persistente on-chain quando la procedura di consenso sarà completata.

In generale, ogni volta che un NFT viene creato o venduto, è necessario inviare alla rete una nuova transazione invocando uno Smart Contract. Dopo che la transazione è stata confermata, i metadati dell'NFT e i dettagli relativi al nuovo proprietario vengono aggiornati e il tutto è registrato in blockchain.

Anche la valutazione della sicurezza dell'intero processo di creazione di un NFT è di vitale importanza, poiché ogni componente può diventare un possibile punto debole, rendendo l'intero sistema vulnerabile agli aggressori. Diversi sono gli scenari d'attacco presi in considerazione. A titolo di esempio, possiamo elencare le tecniche di *spoofing* che sfruttano le capacità di un malintenzionato di fingersi un'altra entità, le tecniche di manomissione dei dati memorizzati in blockchain o di quelli memorizzati esternamente, le tecniche di divulgazione di informazioni che violano la riservatezza dei dati, tecniche di Denial of Service (DoS), che hanno come obiettivo quello di rendere non disponibili le normali funzionalità di un server etc.

3. Conclusioni

La blockchain, gli Smart Contracts, gli NFTs sono i mattoncini di base per lo sviluppo di nuove forme di commercio e le crittomonete sono lo strumento fondamentale che supporta questi nuovi modelli di business. La natura decentralizzata delle blockchain permetterà di produrre e negoziare nuovi contenuti digitali attraverso transazioni trasparenti e tracciabili senza la necessità di coinvolgere intermediari. Gli utenti che sapranno cogliere le nuove opportunità legate alla finanza decentralizzata (DeFi), al Metaverso e alle nuove tecnologie avranno un importante vantaggio competitivo nell'evoluzione del World Wide Web.

This work was supported in part by project MUSA (ECS0000037) under the NRRP MUR program founded by the EU.

Bibliografia

[1] Nakamoto, S. (28/08/2023) *Bitcoin: a peer□to□peer electronic cash system*, https://bitcoin.org/bitcoin.pdf.

[2] Gao, W., Hatcher, W. G. and Yu, W. (2018) "A Survey of Blockchain: Techniques, Applications, and Challenges". *27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou, China, 1-11, doi: 10.1109/ICCCN.2018.8487348.

[3] Feng, Q., He, D., Zeadally, S., Khan, M. K. and Kumar, N. (2019) "A survey on privacy protection in blockchain system". *Journal of Network and Computer Applications*, 126, 45-58.

[4] Islam, S., Islam, M. J., Hossain, M., Noor, S., Kwak, K.-S.and Islam, S. M. R. (2023) "A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues,". *IEEE Access*, 11, 39066-39082, doi: 10.1109/ACCESS.2023.3267047.

[5] Sankar, L. S., Sindhu, M. and Sethumadhavan M. (2017) "Survey of consensus protocols on blockchain applications,". *4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, 1-5, doi: 10.1109/ICACCS.2017.8014672.

[6] Ethereum (28/08/2023) *PoS*: https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/.

[7] Castro, M. and Liskov, B. (1999) "Practical Bizantine Fault Tolerance". *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA.

[8] Costan, V. and Devadas, S. (2017) "Intel SGX explained", *Cryptol. ePrint Arch.,* 2016/086, https://eprint.iacr.org/2016/086.

[9] Bowman, M., Das, D., Mandal, A. and Montgomery, H. (2021) "On Elapsed Time Consensus Protocols", *Cryptology ePrint Arch., 2021/086,* https://eprint.iacr.org/2021/086.

[10] Forte, P., Romano, D. and Schmid, G. (2015) "Beyond Bitcoin – Part I: A critical look at blockchain-based systems", *Cryptol. ePrint Arch., 2015/1164*, https://eprint.iacr.org/2015/1164.

[11] Zheng, Z., Xie, S., Dai, H. N., Chen, X. and Wang, H. (2018) "Blockchain challenges and opportunities: a survey", *Int. J. Web and Grid Services,* 14(4).

[12] Hasanova, H., Baek, U., Shin, M., Cho, K., Kim, M.-S. (2019) "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures". *Int J Network Mgmt*. 29: e2060. https://doi.org/10.1002/nem.2060.