

Tesi di laurea triennale

Dipartimento di Impresa e Management

Corso di laurea in Economia e Management

Cattedra: Statistica applicata ed econometria

Titolo:

“Il futuro dei play to earn: analisi in serie storiche dei NFT”

Relatore:

Prof. Giorgia Riveccio

Candidato:

Alessandra Luciano

Matr. 255171

Anno Accademico 2022-2023

Sommario

INTRODUZIONE	5
CAPITOLO PRIMO	6
LA TECNOLOGIA BLOCKCHAIN	6
1.1 DEFINIZIONE E FUNZIONAMENTO	6
1.2 CARATTERISTICHE	7
1.2.1 <i>DECENTRALIZZAZIONE</i>	7
1.2.2 <i>CONSENSO</i>	7
1.2.3 <i>IMMUTABILITA'</i>	9
1.2.4 <i>TRASPARENZA</i>	10
1.3 ARCHITETTURA DELLA BLOCKCHAIN	11
1.4 LA CRITTOGRAFIA COME SINONIMO DI SICUREZZA	12
1.4.1 <i>CRITTOGRAFIA A CHIAVE SIMMETRICA</i>	12
1.4.2 <i>CRITTOGRAFIA A CHIAVE ASIMMETRICA</i>	13
1.4.3 <i>CRITTOGRAFIA E FIRMA DIGITALE</i>	13
1.5 TIPOLOGIE DI BLOCKCHAIN	14
1.6 AMBITI DI APPLICAZIONE DELLA BLOCKCHAIN	15
1.7 RIVOLUZIONE DEL CONCETTO DI BLOCKCHAIN	17
1.7.1 <i>ETHEREUM</i>	17
1.7.2 <i>SMART CONTRACT</i>	18
1.7.3 <i>DApp</i>	20
1.8 GLI ORACOLI: IL PONTE TRA BLOCKCHAIN E MONDO REALE	21
CAPITOLO SECONDO	24
TOKEN NON FUNGIBILI	24
2.1 TOKEN E TOKENIZZAZIONE	24
2.2 LA DISTINZIONE TRA TOKEN DI UTILITA' E TOKEN DI SICUREZZA	25
2.3 FUNGIBLE E NON-FUNGIBLE TOKEN	25
2.4 ETHEREUM REQUEST FOR COMMENT	26
2.5 STORIA DEGLI NFT	27
2.6 CARATTERISTICHE NFT	29
2.7 FORMATO	30
2.8 FUNZIONAMENTO	30
2.9 CATEGORIE	33
CAPITOLO TERZO	35
SERIE STORICHE E GAME	35
3.1 UTILIZZO DELLA BLOCKCHAIN NEL GAMING	35
3.2 STRUMENTI PER LA COMPrensIONE DEL FENOMENO	36

3.3	SERIE STORICHE, APPROCCIO STOCASTICO E VARIABILI CASUALI.....	36
3.5	OPERATORE RITARDO E OPERATORE DIFFERENZA.....	38
3.6	STAZIONARIETA' E INVERTIBILITA'	39
3.7	FUNZIONE DI AUTOCORRELAZIONE GLOBALE E PARZIALE: AUTOCOVARIANZA STANDARD.....	40
3.8	MODELLI STATISTICI	41
3.8.1	WHITE NOISE: $\epsilon_t \sim WN(0, \sigma^2)$	41
3.8.2	MODELLI AUTOREGRESSIVI $AR(p)$	42
3.8.3	MODELLI MOVING AVERAGE $MA(q)$	44
3.8.4	MODELLO AUTOREGRESSIVO MOVING AVERAGE $ARMA(p, q)$	45
3.9	PROCEDURA BOX-JENKINS	45
3.9.1	IDENTIFICAZIONE.....	45
3.9.2	STIMA	47
3.9.3	LA VERIFICA	49
3.10	METODI ALTERNATIVI	49
3.11	LE PREVISIONI	50
3.11.1	PREVISIONI PER MODELLI AR	51
3.11.2	PREVISIONI PER MODELLI MA	51
3.11.3	PREVISIONI PER MODELLI $ARMA$	52
3.11.4	ERRORE DI PREVISIONE.....	52
3.12	MODELLO $ARIMA$	53
3.13	VERIFICA DELLA STAZIONARIETA'	53
3.14	OUTLIERS E LEVEL CHANGES.....	54
CAPITOLO QUARTO.....		56
ANALISI IN SERIE STORICHE DEI PLAY TO EARN		56
4.1	AXIE INFINITY.....	56
4.1.1	ANALISI IN SERIE STORICHE UAW	56
4.1.2	ANALISI IN SERIE STORICHE NUMERO DELLE TRANSAZIONI.....	59
4.1.3	ANALISI IN SERIE STORICHE DEL VOLUME.....	62
4.2	GODS UNCHAINED	63
4.2.1	ANALISI IN SERIE STORICHE UAW	64
4.2.2	ANALISI IN SERIE STORICHE TRANSAZIONI.....	67
4.2.3	ANALISI IN SERIE STORICHE VOLUME	69
4.3	SANDBOX.....	72
4.3.1	ANALISI IN SERIE STORICHE UAW	72
4.3.2	ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI	74
4.3.3	ANALISI IN SERIE STORICHE VOLUME	75
4.4	ALIENS WORLD.....	77
4.4.1	ANALISI IN SERIE STORICHE UAW	78
4.4.2	ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI	80
4.4.3	ANALISI IN SERIE STORICHE VOLUME	83

4.5	DECENTRALAND.....	85
4.5.1	ANALISI IN SERIE STORICHE UAW.....	85
4.5.2	ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI.....	87
4.5.3	ANALISI IN SERIE STORICHE VOLUME.....	89
4.6	SPLINTERLANDS.....	91
4.6.1	ANALISI IN SERIE STORICHE UAW.....	92
4.6.2	ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI.....	94
4.6.3	ANALISI IN SERIE STORICHE VOLUME.....	97
4.7	QUANTO SONO CORRELATI I VIDEOGAMES?.....	98
4.7.1	CORRELAZIONE VIDEOGAME: UAW.....	98
4.7.2	CORRELAZIONE VIDEOGAME: TRANSAZIONI.....	99
4.7.3	CORRELAZIONE VIDEOGAME: VOLUME.....	100
	CONCLUSIONI.....	101
	BIBLIOGRAFIA.....	102
	SITOGRAFIA.....	103

INTRODUZIONE

Negli ultimi anni, il mondo dei videogiochi è stato sconvolto da una rivoluzione tecnologica che ha portato alla creazione di nuovi modelli di business basati sulla blockchain e sui non-fungible token. La blockchain, infatti, rappresenta una tecnologia innovativa che consente la creazione di registri digitali sicuri e immutabili, che possono essere utilizzati per registrare transazioni, tracciare e garantire la sicurezza di ciascun dato registrato al suo interno.

In particolare, il fenomeno dei play to earn, ha attirato l'attenzione di milioni di giocatori in tutto il mondo, promettendo la possibilità di guadagnare denaro reale attraverso l'acquisizione ed il commercio di oggetti virtuali all'interno del videogioco. Ciò è reso possibile in quanto, ogni asset virtuale presente all'interno del videogioco viene registrato sulla blockchain come NFT, motivo per cui diventa unico ed irripetibile. Una volta avvenuta la registrazione all'interno della blockchain del videogame, è possibile lo scambio ed il commercio non solo all'interno del game stesso, ma anche su piattaforme esterne dedicate definite market place.

Il mondo dei videogiochi play to earn è ancora relativamente nuovo e poco conosciuto, e molte domande rimangono ancora senza risposta. Ad esempio, quali sono i fattori che influenzano il successo di questi nuovi business model? Quali sono le dinamiche di mercato che guidano la domanda e l'offerta di oggetti virtuali all'interno dei games? E quali sono le possibilità di guadagno per i giocatori che partecipano a questi sistemi? La presente tesi si propone l'analisi in serie storiche di variabili d'interesse come numero di portafogli attivi, numero delle transazioni e volume di queste ultime di alcuni videogiochi play to earn. In particolare, si cercherà di identificare i principali fattori al fine di comprendere meglio non solo il loro funzionamento attraverso l'utilizzo di blockchain e NFT, ma anche la possibilità di guadagno che essi offrono ai giocatori.

Tuttavia, per poter comprendere come un'analisi in serie storiche viene effettuata, è necessaria l'esplorazione nel dettaglio della teoria delle serie storiche. Si cercherà dunque di identificare e spiegare i modelli maggiormente appropriati a ciascuna serie storica costruita, nonché la loro applicazione ai dati relativi i videogames d'interesse.

In conclusione, lo scopo della tesi è l'analisi del settore dei play to earn nonché l'identificazione delle ragioni per cui questi ultimi rappresentano una vera e propria rivoluzione nell'industria dei videogames.

Tuttavia, per una profonda comprensione del fenomeno è necessaria la conoscenza della blockchain, l'analisi temporale e in cross-section degli NFT e l'utilizzo di metodologie statistiche per l'analisi delle serie storiche, elementi coinvolti ed alla base degli obiettivi dei prossimi capitoli di questo elaborato. IL lavoro di tesi si concluderà con l'analisi empirica di alcuni NFT GAME e l'utilizzo dei modelli AutoRegressive Integrated Moving Average (ARIMA) per l'analisi della loro evoluzione temporale.

CAPITOLO PRIMO

LA TECNOLOGIA BLOCKCHAIN

1.1 DEFINIZIONE E FUNZIONAMENTO

La Blockchain, conosciuta genericamente come Distributed Ledger Technologies (DLT)¹, è un registro digitale genericamente pubblico, e dunque talvolta può essere anche privato, all'interno del quale possono essere registrate informazioni, da transazioni ad interi programmi. Le informazioni contenute all'interno della blockchain dipendono dalla tecnologia utilizzata. Una blockchain, dunque, è una particolare tipologia di database distribuito e condiviso fra i nodi di una rete di computer che memorizza informazioni e le organizza in unità di archiviazione; le unità di archiviazione vengono definite blocchi e queste ultime sono collegate tra di loro.

All'interno di ciascun blocco sono contenute delle informazioni ben precise: se ci trovassimo di fronte una transazione, il blocco contenebbe dati relativi il destinatario, il mittente, l'importo trasferito e una firma digitale che garantisce l'autenticità della transazione.

Per distribuito e condiviso intendiamo un ledger all'interno del quale vi è un'architettura peer-to-peer: i nodi sono equivalenti in quanto possono rivestire la veste di client ma anche di server verso gli altri nodi terminali della rete².

Attraverso l'organizzazione del registro in blocchi, è possibile la creazione di una sequenza temporale irreversibile: ogni blocco, dopo esser stato compilato, viene definitivamente chiuso con una firma digitale immutabile e viene collegato all'ultimo blocco presente nella catena.

Nel dettaglio, se venissero elaborate transazioni all'interno della blockchain, queste transazioni verrebbero raggruppate e aggiunte ad un nuovo blocco: all'interno di quest'ultimo vi è un riferimento al blocco precedente; grazie a questo riferimento, chiamato hash³, i due blocchi sono direttamente collegati tra loro e, il sistema così descritto, consente la creazione di una catena di blocchi.

Questa peculiare caratteristica dell'hash, in grado di collegare ogni blocco a quello precedente, rende i blocchi già aggiunti alla blockchain immutabili e sicuri. Non possono, dunque, essere modificati retroattivamente. L'immutabilità dei blocchi della blockchain dipende dal fatto che, qualora voglia esser modificato un blocco ormai aggiunto alla sequenza, bisognerebbe modificare anche tutti gli altri blocchi precedenti essendoci dei

¹ DTL: l'insieme dei sistemi digitali che consentono lo scambio sicuro e trasparente di dati e valore tra più parti.

² Rete: può anche essere definita come "network" per il quale intendiamo una serie di macchine connesse tra loro che scambiano reciprocamente delle informazioni.

³ Hash: funzione matematica che prende in input un dato e lo converte in un valore di lunghezza fissa definito "hash".

riferimenti in ognuno che permettono il loro collegamento. Inoltre, la modifica diviene impossibile in quanto la potenza di calcolo richiesta è estremamente elevata.

1.2 CARATTERISTICHE

1.2.1 DECENTRALIZZAZIONE

I sistemi tradizionali vengono definiti centralizzati: ciò significa che esiste un ente di controllo che regola le attività svolte all'interno del sistema. L'esempio più rappresentativo è quello in cui il soggetto è la banca e l'oggetto è rappresentato dalle transazioni. Affinché una transazione venga approvata e abbia dunque esito positivo, viene effettuato un controllo da parte dell'ente centrale, il quale controlla se effettivamente ci sia il denaro da trasferire e in caso di riscontro positivo, approva la transazione. La blockchain al contrario è un sistema decentralizzato: non esiste un ente di controllo e dunque i suoi compiti decisionali e di controllo vengono trasferiti alla rete distribuita.

Nello specifico, gli scambi che avvengono tra i nodi del network vengono segnati all'interno del registro, ovvero ledger, che non risiede in un unico punto centrale, ma viene decentralizzato attraverso i blocchi che formano la catena. Quest'ultima viene replicata tra tutti i nodi che fanno parte del sistema: non è dunque necessario l'affidamento ad un ente centrale in quanto la fiducia dei nodi risiede nel sistema stesso. Tale sistema permette inoltre la soppressione dell'ente centrale, la cui funzione tipica è quella dell'intermediazione: l'ente centrale ha il compito di registrare le transazioni che avvengono tra le parti. Talvolta però, l'intermediazione da parte dell'ente centrale può creare all'interno del sistema un punto di vulnerabilità, anche definito "point of failure". Infatti, qualora l'ente venisse compromesso, entrambe le parti subirebbero dei danni.

Se all'interno di un sistema decentralizzato alcune delle informazioni o transazioni all'interno di un blocco venissero corrotte, tutti gli altri blocchi ai quali quest'ultimo è collegato, dimostreranno che all'interno dell'ultimo blocco le informazioni sono false e dunque non verranno accettate.

Affinché le informazioni contenute nel blocco vengano validate, è necessario raggiungere il consenso.

1.2.2 CONSENSO

La possibilità di registrare transazioni all'interno del registro digitale è determinata dal consenso della maggioranza dei partecipanti alla rete. Tale consenso, a seconda di quanto preveda la blockchain utilizzata, può essere prevalentemente raggiunto in due modi differenti. Tali sistemi vengono definiti: "proof of work" e

“proof of stake”⁴. Seppure nella maggior parte dei casi il consenso all’interno del ledger viene raggiunto grazie il loro utilizzo, la scelta dell’algoritmo dipende dalle esigenze specifiche della piattaforma, ma in ogni caso possono essere utilizzati, e vengono utilizzati, anche in altre tipologie di blockchain.

PoW e PoS differiscono l’uno dall’altro date le loro differenti caratteristiche ma ambedue nascono per assolvere alla medesima funzione e dunque il raggiungimento dello stesso scopo: la risoluzione del cosiddetto “Problema dei generali bizantini”.

Il problema dei generali bizantini appartiene prevalentemente al mondo del calcolo distribuito: viene immaginato uno scenario i cui protagonisti sono nove generali bizantini, ciascuno a capo di una parte dell’esercito.

I generali si trovano in una situazione di incertezza in quanto tutti i generali circondano una città, ma solo alcuni vogliono attaccarla. Il fine ultimo tuttavia, non è l’attacco, bensì l’accordo tra tutti i generali affinché tutti agiscano nel medesimo modo. Tutti i generali esprimono il proprio parere: quattro sono favorevoli all’attacco, quattro alla ritirata, mentre l’ultimo comunica ai primi di essere favorevole all’attacco, ai secondi invece, di essere concorde alla ritirata.

Il gruppo che ha ricevuto il voto favorevole all’attacco procederà con quest’ultimo; gli altri generali, avendo contrariamente ricevuto la comunicazione che il nono generale preferisce la ritirata, non attaccheranno. La situazione è ulteriormente aggravata dal fatto che i generali non sono fisicamente nello stesso luogo e dunque le comunicazioni avvengono esclusivamente tramite messaggi che tuttavia, possono non arrivare o addirittura falsificare le decisioni prese dal gruppo di comando.

Tale situazione è analoga a quella in cui opera la blockchain: i generali rappresentano i nodi terminali, i traditori i nodi malevoli, i messaggeri il mezzo con cui avviene la comunicazione.

Il ledger, dunque, deve assicurare il raggiungimento del consenso anche qualora ci si venga a trovare nel contesto analogo sopra quello appena descritto. Ed è proprio questa la ragione per cui sono stati ideati i due algoritmi di consenso riassumibili con i termini “PoW” e “PoS”.

Il “proof of work” prevede che i blocchi vengano minati: tale tecnica viene comunemente conosciuta come mining⁵ e i suoi protagonisti sono i miners.

I miners, dunque, hanno il compito di unire ogni nuovo blocco a quello precedente: attraverso complessi calcoli algoritmici e un lungo processamento di dati, calcolano un lungo codice definito hash. Se quest’ultimo rappresenta la soluzione alla problematica che viene presentata e dunque è l’output attraverso cui il nuovo blocco può essere unito a quello precedente, quest’ultimo viene aggiunto alla rete.

I miners, dunque, hanno principalmente due compiti: processare e convalidare i dati o transazioni e coniare nuova moneta. Il conio di nuova moneta avviene nel momento in cui miners processano e convalidano la

⁴ Proof of Work e Proof of Stake: due algoritmi utilizzati dalle blockchain per validare le transazioni e garantire la sicurezza in rete.

⁵ Mining: in italiano “estrazione”, è il processo di validazione e creazione dei blocchi utilizzato all’interno del PoW.

transazione: anche i miners hanno incentivi nello svolgere correttamente il loro lavoro nel sistema. Tali incentivi sono rappresentati da una remunerazione, pagata dai soggetti che intendono realizzare ad esempio la transazione, che avviene sottoforma di moneta della blockchain definita gas tax. La base sulla quale tale sistema fa leva e dunque è possibile la realizzazione dell'hash, è la potenza di calcolo e dunque hardware ed elettricità che comportano elevati costi.

Differente è il secondo sistema attraverso cui viene raggiunto il consenso, ovvero il "proof of stake".

Quest'ultimo è un metodo alternativo di validazione di informazioni e transazioni. I protagonisti all'interno del sistema sono i validators e, affinché possano assolvere il compito di approvazione di informazioni e transazioni, e dunque di minting⁶, devono possedere degli asset, ovvero la moneta prevista all'interno della blockchain e depositarla presso quest'ultima. In base a quanta moneta il soggetto deposita, quest'ultimo avrà maggiori probabilità di essere remunerato con la commissione che i soggetti pagano per la transazione da aggiungere al blocco. Una volta scelto attraverso un calcolo algoritmico randomico il soggetto che verrà remunerato, il nuovo blocco viene aggiunto alla catena. Inoltre, qualora un validator approvi una transazione fraudolenta, quest'ultimo perderà la quota precedentemente depositata presso la blockchain.

Entrambi i sistemi mirano a garantire la sicurezza delle informazioni e transazioni approvate non essendoci un ente centralizzato che assolva a tale funzione. Tuttavia, tali sistemi comportano anche dei rischi, in particolare quello che viene definito come attacco al 51%.

Se un unico miner o un unico validator possiedono, il primo il 51% della potenza di calcolo, il secondo il 51% degli asset presenti all'interno della blockchain, le informazioni o transazioni all'interno del blocco potrebbero essere falsificate.

1.2.3 IMMUTABILITA'

Il sistema blockchain viene definito sicuro per determinate e specifiche caratteristiche dei blocchi che lo compongono.

Ogni blocco contiene il proprio hash, oltre che quello del blocco precedente. Tale affermazione vale per tutti i blocchi presenti all'interno della blockchain eccezion fatta per il blocco genesis⁷ che non contiene l'hash del blocco precedente. Se uno dei blocchi venisse compromesso, quest'ultimo non contenebbe più al suo interno lo stesso hash del blocco precedente a cui è collegato. A sua volta, tutti i blocchi successivi a quello manomesso non saranno validi perché non memorizzeranno più un hash valido del blocco precedente. Pertanto, la modifica di un blocco renderà non validi tutti i blocchi successivi. Dunque, una volta inserito un nuovo blocco

⁶ Minting: in italiano "coniazione", è il processo di validazione utilizzato nelle blockchain basate sull'algoritmo PoS.

⁷ Blocco genesis: il primo blocco nella costruzione della blockchain.

all'interno della catena, nessuna delle parti può modificare o alterare tale blocco, a meno che non venga invalidata l'intera struttura.

I blocchi validi verranno pian piano aggiunti alla struttura che, più nello specifico, viene definita "Albero di Merkle".

Di seguito, viene riportata la struttura dell'albero di Merkle.

Figura 1.1, Alberi di Merkle.

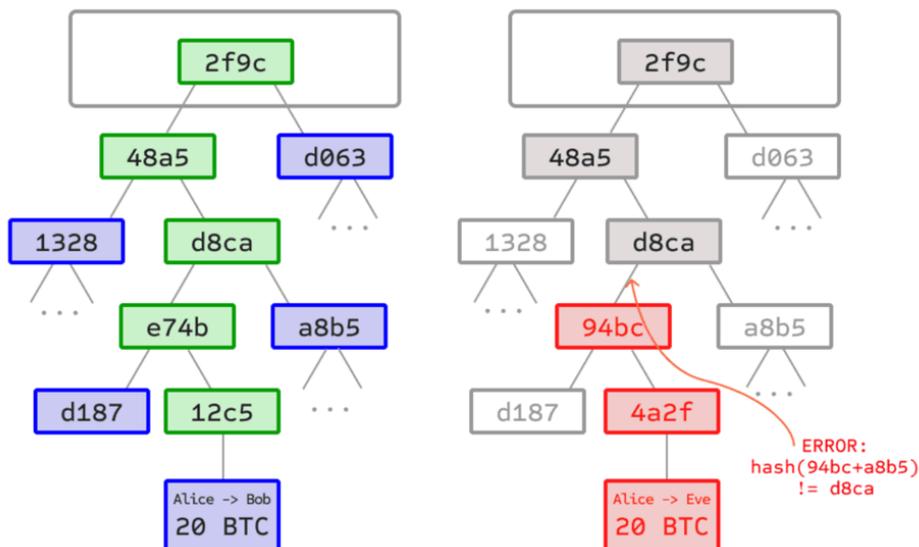


Grafico riportato dal Whitepaper di Ethereum, <https://ethereum.org/it/whitepaper/>.

A sinistra viene riportato un piccolo numero di nodi in un albero di Merkle per fornire una prova della validità di un ramo, mentre a destra viene mostrato un tentativo di manipolazione di una parte dell'albero, che causerà incoerenze ai livelli superiori della catena.

In ciascun momento possono essere aggiunti nuovi blocchi di informazioni, tuttavia, come appena visto, non possono essere rimossi o modificati i blocchi precedentemente aggiunti alla catena. Tale caratteristica non è altro che un corollario di come i blocchi vengono aggiunti alla catena una volta raggiunto il consenso tramite il PoW o il PoS.

1.2.4 TRASPARENZA

Grazie alla sua architettura distribuita e alla condivisione di dati fra tutti i partecipanti della rete, la blockchain è un sistema altamente trasparente. In particolare, ogni transazione all'interno di una blockchain registrata in modo permanente e immutabile, e le informazioni contenute in ciascun blocco sono accessibili a tutti i partecipanti della rete. Ciò significa che ogni transazione è verificabile e tracciabile, e che le informazioni registrate nella blockchain sono sempre disponibili per la verifica e l'analisi. Questa trasparenza consente di creare un sistema di monitoraggio e verifica dei dati più affidabile e trasparente. Ad esempio, nella blockchain

pubblica di Bitcoin, tutte le transazioni sono visibili a tutti i partecipanti della rete, e ogni nodo della rete ha una copia identica del registro delle transazioni. Questo rende difficile manipolare le transazioni o contraffare la blockchain.

E proprio per la trasparenza che caratterizza la blockchain, quest'ultima ha numerose applicazioni pratiche, ad esempio nel settore finanziario, nella supply chain e nella gestione dei dati sensibili. Inoltre, la tecnologia blockchain consente di garantire la veridicità dei dati senza la necessità di affidarsi a un intermediario o ad una unità centrale, aumentando la sicurezza e la fiducia nell'intero sistema.

1.3 ARCHITETTURA DELLA BLOCKCHAIN

La blockchain ha una propria architettura ed è dunque articolata in molteplici livelli. Il primo livello è rappresentato dall'infrastruttura, poi vi è un livello dei dati, livello di rete, livello di consenso e infine, il livello applicativo. Un blockchain layer è una parte dell'architettura il cui fine ultimo è quello di assolvere determinati compiti, derivanti dal livello a cui fa riferimento.

Esistono varie tipologie di layer, classificati dal più semplice al più complesso.

Il layer 0 è un'infrastruttura di base che consente il trasferimento di dati e l'integrazione della blockchain con le reti tradizionali. Successivamente il layer 0, un livello più avanzato è rappresentato dal layer 1. In particolare, questa tipologia di layer, si occupa della gestione dei dati, composizione dei blocchi e crittografia, protocolli di rete e di consenso e gestione ed esecuzione delle transazioni. I layer 1, nel caso in cui si vogliano apportare alla blockchain dei cambiamenti, richiedono delle modifiche strutturali e dunque l'intervento diretto sul software. Ad esempio, qualora si voglia modificare il meccanismo di consenso della piattaforma, verranno apportate delle modifiche seguendo dei meccanismi specifici: hard fork o soft fork. Il primo richiede un aggiornamento obbligatorio da parte di tutti i nodi della rete in quanto la versione della blockchain che verrà rilasciata non è più compatibile con la versione precedente; il secondo invece, non richiede l'aggiornamento da parte di tutti i peers della rete in quanto la modifica del protocollo è compatibile con la versione blockchain precedente.

I layer 1 tuttavia, hanno un limite: la scalabilità. Per scalabilità viene intesa la capacità della piattaforma di supportare tutte le transazioni che avvengono al suo interno, rimanendo efficiente ed evitando la congestione, ed è proprio da qui che nasce il trilemma della blockchain, introdotto da Vitalik Buterin.

Il trilemma introduce una problematica relativa tali tipologie di layer: la difficoltà delle blockchain di assicurare simultaneamente scalabilità, decentralizzazione e sicurezza. Viene spiegato che, in genere, le blockchain possono raggiungere in modo efficiente solo due di questi obiettivi, sacrificando inevitabilmente il terzo. Solitamente, ogni blockchain layer 1 cerca di assicurare sicurezza e decentralizzazione, e questo comporta, talvolta, problemi di scalabilità.

Per risolvere le difficoltà che emergono proprio da quest'ultimo punto, possono essere apportate due tipologie di modifiche all'interno della piattaforma: on-chain⁸ ed off-chain⁹. Il presupposto delle modifiche on-chain è che venga interamente modificata la piattaforma, per quelle off-chain non è richiesta la modifica dell'intera piattaforma bensì l'introduzione dei layer 2.

Una delle possibili soluzioni dello sfruttamento dei layer 2 è la side chain, grazie a cui viene sfruttata una blockchain parallela: viene utilizzata una rete di elaborazione secondaria che si integra con la blockchain principale.

Infine, è stato anche introdotto il termine layer 3, possibile soluzione ai problemi legati alla scalabilità, ma che differisce dal layer 2 per il livello più avanzato. Questo concetto, ad oggi, è ancora in fase di sviluppo e dunque è astratta la sua applicazione all'interno dei ledger.

1.4 LA CRITTOGRAFIA COME SINONIMO DI SICUREZZA

La crittografia¹⁰ è una componente fondamentale della blockchain perché consente di garantire la sicurezza e l'integrità dei dati all'interno della rete. Tale tecnica viene comunemente utilizzata ogni qual volta un soggetto voglia inviare delle informazioni ad un altro: se il messaggio viene crittografato, vuol dire che l'intento principale del mittente è che il solo destinatario possa essere in grado di leggerlo e dunque di decriptarlo. Tale tecnica presuppone che le due parti abbiano preventivamente concordato la chiave di decriptazione del messaggio. In particolare, ci sono due tecniche di crittografia comunemente utilizzate nella blockchain: la crittografia a chiave simmetrica e la crittografia a chiave pubblica.

1.4.1 CRITTOGRAFIA A CHIAVE SIMMETRICA

La crittografia a chiave simmetrica è una tecnologia crittografica in cui mittente e destinatario utilizzano la stessa chiave per crittografare e decrittografare i dati. Questa tecnologia, oltre che essere definita a chiave simmetrica, viene anche comunemente conosciuta come a chiave segreta.

Nella crittografia a chiave segreta, le due parti, ovvero mittente e destinatario, devono preventivamente accordarsi sulla chiave da utilizzare per rendere la comunicazione sicura. Il ruolo svolto dalla chiave all'interno

⁸ On-chain: informazioni direttamente gestite sulla blockchain.

⁹ Off-chain: informazioni gestite al di fuori della blockchain.

¹⁰ Crittografia: tecnica per la rappresentazione di un messaggio in una forma tale che le informazioni in esso contenute possano essere decriptate e dunque decifrate solo dal destinatario del messaggio stesso.

di questa tipologia di crittografia è quello di essere utilizzata dal mittente per crittografare i dati contenuti dal messaggio, prima ancora di essere inviato al destinatario.

Un punto a favore di questa tipologia di tecnologia è la velocità: essendo utilizzata la stessa chiave per il processo di crittografia e decrittografia, lo stesso viene eseguito in modo efficiente e veloce. Lo descritto vantaggio, tuttavia, può talvolta rappresentare anche una minaccia al sistema; tale problema è legato alla ripartizione della chiave segreta. Mittente e destinatario devono anticipatamente accordarsi sulla chiave segreta, garantendo che nessun terzo riesca ad intercettarla durante il trasferimento.

1.4.2 CRITTOGRAFIA A CHIAVE ASIMMETRICA

Più generalmente conosciuta come crittografia a chiave pubblica, tale tecnologia utilizza una coppia di chiavi: una pubblica ed una privata.

Mentre la chiave pubblica è, come dice la parola stessa, resa disponibile a tutti, quella privata è nota solo al proprietario della chiave.

Al fine di crittografare i dati del messaggio, il mittente utilizza la chiave pubblica; mentre il destinatario può decrittografare i dati crittografati utilizzando la chiave privata in suo possesso e solo a lui nota.

La crittografia a chiave pubblica è efficace per garantire sicurezza e privacy nella comunicazione online, come la trasmissione di dati sensibili alla base dell'utilizzo della blockchain, si pensi alle informazioni di pagamento o credenziali di accesso.

Il vantaggio principale di tale tecnologia risiede nel fatto che non viene richiesta la condivisione della stessa chiave segreta tra le parti, ma viene richiesta la generazione di una coppia di chiavi che differiscono tra loro. Inoltre, tale tecnologia è molto più resistente alle violazioni di sicurezza rispetto la crittografia a chiave simmetrica: ciò, è dato dal fatto che la chiave privata non viene mai trasmessa o condivisa con altri soggetti, ma viene tenuta segreta dal proprietario.

1.4.3 CRITTOGRAFIA E FIRMA DIGITALE

La crittografia e le firme digitali sono tecniche crittografiche fondamentali per garantire la sicurezza e l'integrità dei dati sulla blockchain. In particolare, la crittografia viene utilizzata per proteggere i dati delle transazioni, mentre le firme digitali vengono utilizzate per garantire l'autenticità delle transazioni sulla blockchain, nonché l'identità di un utente.

La firma digitale funziona esattamente come una e propria firma reale, l'unica differenza è che non è manuale in quanto viene utilizzata la matematica.

Per proteggere i dati della transazione, la blockchain utilizza l'algoritmo di crittografia asimmetrica, anche noto come crittografia a chiave pubblica.

Una firma digitale viene creata utilizzando la chiave privata del mittente della transazione e verificata utilizzando la chiave pubblica del mittente. In questo modo la firma digitale garantisce che la transazione sia stata effettivamente eseguita dal proprietario della chiave privata. In particolare, per garantire la sicurezza e l'integrità delle firme digitali, la blockchain utilizza un determinato algoritmo, meglio noto come hash SHA-256; questo algoritmo crea un valore hash univoco. Viene quindi creata una firma digitale in base all'hash della transazione, quindi qualsiasi modifica alla transazione invalida la firma digitale.

La firma digitale, premesso che la chiave privata rimanga tale, garantisce autenticazione, integrità e non ripudio. Più esattamente, una firma valida dimostra inequivocabilmente che il messaggio sia stato mandato dal mittente al quale è associata la specifica chiave privata, ogni manipolazione subita dal messaggio successivamente la firma, invalida il messaggio stesso e, infine, posta la propria firma, quest'ultima non può essere negata in un secondo momento.

1.5 TIPOLOGIE DI BLOCKCHAIN

BLOCKCHAIN PUBBLICHE (Public Blockchain)

Questo tipo di blockchain è aperto a chiunque desideri partecipare senza alcuna restrizione. Tutti i partecipanti alla blockchain pubblica hanno accesso alle transazioni e possono verificarne la validità. Bitcoin ed Ethereum sono esempi di blockchain pubbliche.

BLOCKCHAIN PRIVATE (Private Blockchain)

A differenza delle blockchain pubbliche, le blockchain private sono riservate a un gruppo specifico di utenti, solitamente aziende o organizzazioni. L'accesso alla blockchain è limitato e controllato dal proprietario della blockchain.

BLOCKCHAIN CONSORTILI (Consortium blockchain)

Le blockchain consortili sono simili alle blockchain private, ma coinvolgono diverse organizzazioni. In questo caso, le organizzazioni coinvolte collaborano per gestire la blockchain e stabilire le regole che la governano.

BLOCKCHAIN IBRIDE (Hybrid blockchain)

Questo tipo di blockchain combina elementi di blockchain pubblici e privati. In una blockchain ibrida, una transazione è visibile a tutti i partecipanti, mentre le altre transazioni sono riservate a specifici gruppi di utenti.

BLOCKCHAIN FEDERATE (Federate Blockchain)

Una blockchain federata coinvolge un insieme predefinito di nodi di rete il cui compito è verificare e confermare le transazioni. Questo tipo di blockchain è stato utilizzato in contesti aziendali in cui è necessario garantire un elevato livello di sicurezza e controllo.

BLOCKCHAIN AUTORIZZATE (Permissioned blockchain)

Le blockchain autorizzate richiedono ai partecipanti di accedere per utilizzare la blockchain. Questo tipo di blockchain viene spesso utilizzato nella governance o in contesti finanziari in cui la sicurezza e il controllo sono fondamentali.

BLOCKCHAIN SENZA PERMESSO (Permissionless blockchain)

Tutti possono accedere alla blockchain senza autorizzazione senza alcuna restrizione. Questo tipo di blockchain viene utilizzato principalmente per creare criptovalute per la gestione di contratti intelligenti.

1.6 AMBITI DI APPLICAZIONE DELLA BLOCKCHAIN

Blockchain è stato originariamente sviluppato per alimentare la criptovaluta Bitcoin, ma ad oggi la sua tecnologia viene applicata in più e diversi ambiti e, di fatto, quest'ultima ha molte potenziali applicazioni oltre alle criptovalute. Ad esempio, la blockchain può essere utilizzata per registri immutabili di beni di proprietà, tenere traccia di cibo e forniture mediche, gestire identificatori digitali, creare sistemi di voto elettronico sicuri e trasparenti e altro ancora.

DeFi

L'obiettivo principale della DeFi¹¹ è creare un sistema decentralizzato, aperto e trasparente, la cui creazione è resa possibile grazie all'implementazione della blockchain. La tecnologia può tracciare le transazioni che avvengono internamente, eliminando in particolare la necessità di intermediari finanziari.

VIDEOGIOCHI

Gli oggetti virtuali in-game possono essere autenticati in modo univoco e posseduti dagli utenti, il che consente una proprietà e uno scambio sicuri e trasparenti di oggetti virtuali.

IDENTITA' DIGITALE

¹¹ DeFi: Decentralized Finanza ovvero Finanza Decentralizzata.

Tradizionalmente, le identità digitali sono state gestite da terze parti centralizzate, con conseguenti problemi di sicurezza e privacy. Blockchain offre un approccio innovativo: agli utenti viene concesso il controllo sulle proprie informazioni personali e possono condividerle solo con soggetti autorizzati. Inoltre, la falsificazione dei dati diventa molto complessa in quanto si tratta di un registro pubblico e condiviso.

PROPRIETA' INTELLETTUALE

La registrazione consente di certificare l'autenticità e l'originalità di opere protette da diritto d'autore, invenzioni e prodotti brevettati, nonché marchi registrati.

SUPPLY CHAIN

Le piattaforme blockchain possono essere utilizzate per la creazione di un registro immutabile di transazioni all'interno di una catena di approvvigionamento. Il loro utilizzo, inoltre, rende possibile la riduzione dei costi di transazione e garantisce la provenienza dei prodotti.

CRIPTOARTE

Grazie l'avvento della blockchain, è stato altresì rivoluzionato il mondo della criptoarte. Grazie la tecnologia blockchain, è possibile verificare l'autenticità dell'opera, registrata sulla blockchain attraverso un codice univoco il cui scopo è l'identificazione stessa dell'opera. Ulteriore motivo per cui la blockchain sta invadendo anche il mondo dell'arte è rappresentato dalla possibilità di monetizzazione dell'opera stessa: l'artista può direttamente interfacciarsi e dunque compiere la vendita della propria opera senza la necessità di intermediari, rappresentati nel caso specifico da case d'asta o gallerie d'arte.

SERVIZI DIGITALI

Tra i servizi digitali resi possibili grazie la blockchain vi è senz'altro la possibilità di effettuare pagamenti online: la trasparenza della blockchain e l'assenza di intermediari consentono non solo la riduzione dei costi di transazione, ma anche l'efficienza dell'intero sistema.

SCAMBIO DI MONETA

La blockchain consente lo scambio di moneta fra i vari peers connessi alla rete. La moneta oggetto di scambio viene definita criptovaluta e il suo nome, o il suo prezzo reale, può variare in base alla blockchain all'interno della quale viene effettuato lo scambio. Grazie la tecnologia blockchain, le transazioni vengono effettuate in modo sicuro e sono sempre tracciabili in quanto la loro registrazione, una volta avvenuta, non può essere modificata.

INVESTIMENTI FINANZIARI

Date le caratteristiche proprie della blockchain e dunque tracciabilità, verificabilità e immutabilità di ciò che viene registrato al suo interno, la tecnologia si sta diffondendo anche per quanto concerne il mondo della finanza, più nello specifico per gli investimenti finanziari. Molti investitori compiono investimenti acquistano le criptovalute, il cui prezzo però è molto volatile e dunque il suo valore reale può mutare facilmente. Inoltre, il loro rischio è aumentato dalla deregolamentazione delle criptovalute, per le quali non sono ancora state ideate norme volte a regolarne l'acquisto o la vendita. Oltre gli investimenti in criptovalute, è possibile investire anche in token, nonché asset digitali presenti sulla blockchain, e soprattutto grazie l'utilizzo degli smart contract.

1.7 RIVOLUZIONE DEL CONCETTO DI BLOCKCHAIN

Nonostante l'idea della blockchain sia nata anteriormente la creazione di Bitcoin nel 2008, la sua creazione si fa risalire a Satoshi Nakamoto, pseudonimo con il quale viene indicato il creatore o i creatori di Bitcoin in quanto è stato proprio quest'ultimo a trovare un ambito di applicazione per la blockchain. Con l'introduzione di Bitcoin, la blockchain veniva esclusivamente utilizzata per la registrazione di transazioni. Le sue potenzialità, dunque, erano ancora ignote. Appena 5 anni più tardi la creazione di Bitcoin, e dunque nel 2013, grazie un giovane canadese, Vitalik Butarin, gli ambiti di applicazione della blockchain vennero estesi con la piattaforma di Ethereum, in grado di andare ben oltre le singole transazioni tra le parti e di prevedere al suo interno smart contract e DApp.

1.7.1 ETHEREUM

La blockchain di Ethereum è una piattaforma open-source, di seconda generazione, che utilizza la tecnologia blockchain per creare e gestire applicazioni decentralizzate e smart contract.

Ethereum utilizza un sistema di ledger distribuito per mantenere un registro immutabile di tutte le transazioni e i dati relativi alle applicazioni create sulla piattaforma, quindi decentralizzazione, immutabilità e trasparenza sono da sempre le caratteristiche che lo contraddistinguono come blockchain. Inoltre, la criptovaluta utilizzata all'interno della piattaforma è l'Ether, criptovaluta nativa di Ethereum.

La blockchain di Ethereum funziona come le altre blockchain, ma ha alcune caratteristiche specifiche. Innanzitutto, Ethereum nasce utilizzando l'algoritmo di consenso "proof of work"; tuttavia, è recentemente passato, più nello specifico nel 2022, all'algoritmo "proof of stake" per convalidare le transazioni e creare nuovi blocchi nella blockchain. Ogni nodo della rete Ethereum ha una copia completa del libro mastro distribuito della blockchain, che viene costantemente aggiornato in tempo reale man mano che vengono

effettuate nuove transazioni. Ogni transazione sulla rete Ethereum viene registrata in un blocco, verificata e aggiunta alla blockchain da validatori dedicati.

Affinché un utente possa utilizzare la piattaforma Ethereum, è necessario che quest'ultimo costruisca un proprio wallet. Il wallet può essere paragonato ad una porta di accesso in quanto gestisce gli indirizzi dei nodi: vi è all'interno una chiave privata, dalla quale viene generato un indirizzo privato, identificativo dell'utente. Proprio da quest'ultimo, viene generato un indirizzo pubblico al quale l'utente può decidere o meno di associare il proprio identificativo. Ciò permette all'utente di interfacciarsi con la piattaforma e gli altri utenti presenti all'interno di essa senza la necessità di fornire i propri dati.

La blockchain di Ethereum offre anche la possibilità di creare e gestire applicazioni decentralizzate e contratti intelligenti ed è proprio questa la grande novità. Prima dell'avvento di Ethereum, ciascuna blockchain veniva sviluppata in funzione del suo scopo. Dunque, un sistema che abbia come oggetto unicamente quello delle transazioni, poteva assolvere solo a tale funzione. Ethereum, a differenza delle blockchain precedenti, permette di implementare al proprio interno contratti intelligenti, codici sorgente e, più in generale, qualsiasi tipologia di dato o informazione. Proprio per le loro potenzialità, hanno acquistato grande fama gli smart contract, ovvero codici informatici autonomi che consentono di automatizzare e verificare l'esecuzione degli accordi tra le parti senza bisogno di intermediari o terze parti. La grande innovazione di questa tecnologia sta nella creazione di applicazioni complesse come nuovi strumenti finanziari o addirittura giochi. Attraverso l'implementazione di contratti intelligenti, Ethereum può essere definito come una piattaforma di scambio decentralizzato; quindi, è un'applicazione costruita come un contratto intelligente che consente agli utenti di controllare i fondi mentre scambiano i propri asset con altri utenti della stessa rete.

1.7.2 SMART CONTRACT

L'idea degli smart contract è stata introdotta nel 1994 da Nick Szabo, rappresentante della corrente dei cyberpunk, nel lavoro intitolato "Smart Contracts" dove è data la seguente definizione: "A smart contract is a computerized transaction protocol that executes the terms of a contract¹²."

La creazione della blockchain Ethereum e l'implementazione al suo interno dei contratti intelligenti hanno aumentato notevolmente l'utilizzo di Ethereum stesso ed esteso gli ambiti in cui può essere utilizzata.

Dalla loro nascita, l'utilizzo su Ethereum è esponenzialmente cresciuto proprio per la loro praticità e facilità di esecuzione. Di seguito, viene riportato il totale dei contratti verificati all'interno della piattaforma Ethereum

¹² N. Szabo, Smart Contracts, 1994.

Figura 1.2, Totale Contratti Verificati su Ethereum per giorno.



Totale Contratti Verificati su Ethereum per giorno¹³, dal 30 Luglio al 6 Marzo, grafico riportato da Etherscan, <https://etherscan.io/>.

Per poter al meglio comprendere l'utilizzo della tecnologia, è necessario approfondire il concetto di smart contract.

Questi ultimi sono programmi informatici in grado di eseguire automaticamente quanto stabilito al loro interno al verificarsi di determinati condizioni, senza necessità dell'intervento umano per la loro esecuzione.

Gli smart contract sono in grado di automatizzare molte attività garantendo correttezza ed integrità grazie alla loro natura decentralizzata e alla crittografia che li protegge.

In pratica, gli smart contract sono scritti in uno specifico linguaggio, definito Solidity, che viene compilato in bytecode, un linguaggio macchina specifico per la blockchain sulla quale viene eseguito.

Proprio quest'ultimo permette di definire regole e condizioni che devono necessariamente essere rispettate per l'esecuzione stessa dell'applicazione.

Più esattamente, Solidity, sviluppato appositamente per le applicazioni blockchain, presenta caratteristiche di sicurezza e di orientamento agli oggetti.

Il linguaggio di programmazione viene utilizzato per la scrittura degli smart contract che gestiscono transazioni di criptovalute, autenticazione, controllo degli accessi e votazioni. Il codice Solidity, inoltre, è simile a

JavaScript o Python, ma include funzionalità specifiche per la blockchain come supporto per le variabili di stato, funzioni di pagamento e strutture di controllo per la gestione dei contratti.

L'esecuzione degli smart contract avviene in modo deterministico e, per tale motivo, è sempre possibile il raggiungimento dello stesso risultato.

Oltre che contenere un codice eseguibile, ciascun smart contract contiene al suo interno la memoria, che permette di gestire e salvare i dati durante l'esecuzione del contratto sulla blockchain.

In generale, dunque, gli smart contract vengono eseguiti in modo autonomo e automatico. Tuttavia, talvolta, è possibile che predavano dei privilegi per gli utenti che interagiscono con quest'ultimi. Più nello specifico, i privilegi rappresentano dei diritti ed autorizzazioni sul contratto per alcuni utenti, i quali avranno accesso a determinate funzionalità o dati all'interno dello smart contract.

Gli sviluppatori dello smart contract determinano il soggetto al quale può eventualmente spettare un determinato privilegio: ad esempio, il programmatore dello smart contract potrebbe avere il massimo livello di privilegio con relativo accesso completo ai dati ed alle funzionalità del contratto, mentre per gli altri potrebbe essere previsto unicamente l'accesso a specifiche funzionalità o dati.

1.7.3 DApp

Non solo Ethereum offre la possibilità di concludere contratti automaticamente al verificarsi di determinate condizioni, ma offre anche l'opportunità di poter implementare delle applicazioni all'interno della piattaforma stessa.

Con il termine DApp, vengono indicate le applicazioni digitali decentralizzate; queste ultime possono unicamente essere costruite sugli smart contract e dunque, sono supportate unicamente da piattaforme, come Ethereum ma non Bitcoin, che prevedono l'utilizzo di tale tipologia di contratti al loro interno e prevedono il supporto di una blockchain.

Ulteriore definizione associata alle DApp è Web3: tale termine sottolinea la distinzione tra il Web2, nonché la versione di Internet maggiormente conosciuta dominata da aziende che offrono servizi in cambio di dati personali, e le app decentralizzate, eseguite su blockchain, che consentono all'utente di non fornire i propri dati personali in quanto, presupposto per il loro utilizzo, è semplicemente la creazione di un indirizzo al quale l'utente è direttamente associato.

La differenza sostanziale tra tali tipologie di applicazioni e quelle tradizionali risiede nel fatto che in quelle tradizionali esiste un'entità centrale che gestisce l'intero sviluppo e funzionamento dell'applicazione mentre quelle decentralizzate sono supportate dalla blockchain.

Le DApp, oltre che essere costituite da smart contract, presentano un'interfaccia utente, definita front-end, scritta in un linguaggio che richiama il back-end.

Il front-end è la parte dell'applicazione che interagisce con l'utente finale e fornisce l'interfaccia grafica dell'applicazione. In una DApp, il front-end comunica con la blockchain e recupera i dati necessari per

mostrare le informazioni all'utente. D'altra parte, il back-end, la parte dell'applicazione non direttamente visibile all'utente, gestisce la logica di business dell'applicazione e la comunicazione con la blockchain. Il back-end di una DApp può essere implementato utilizzando contratti intelligenti sulla blockchain, che contengono la logica di business dell'applicazione e definiscono come l'applicazione interagisce con la blockchain.

L'utilizzo degli smart contract all'interno da parte delle DApp garantisce che quanto previsto dall'applicazione stessa avvenga in modo automatico.

Le DApp sono anch'esse open-source: chiunque può guardare il codice e vedere come funziona e ne consegue che utenti di possano riporre maggiore fiducia nell'applicazione stessa.

Un vantaggio delle applicazioni decentralizzate è che non potranno mai essere offline: talvolta, applicazioni centralizzate quali Facebook o Twitter possono avere un bug¹⁴ o, più in generale, sono maggiormente suscettibili a manipolazioni o hacking.

Le DApp mentre, essendo gestite da centinaia di migliaia di computer in tutto il mondo, non possono risentire di tali problematiche: sarebbe impossibile spegnere o manipolare tutti i nodi che compongono la rete.

Le applicazioni decentralizzate hanno vari ambiti di applicazioni, a partire dalle DeFi sino agli Exchanges, che permettono agli utenti di scambiare i loro stessi token e ancora, videogiochi e marketplace.

Anche all'interno delle Dapp viene utilizzata la crittografia la quale, come già visto, garantisce sicurezza e privacy agli utenti.

Le applicazioni decentralizzate, come indica il termine stesso, non richiedono la presenza di organizzazioni centrali che le gestiscono, ma piuttosto una serie di nodi che assicurano il funzionamento delle stesse.

Sempre attraverso i nodi della rete vengono decise le modifiche o gli aggiornamenti relativi all'applicazione la cui decisione è subordinata al consenso degli utenti.

1.8 GLI ORACOLI: IL PONTE TRA BLOCKCHAIN E MONDO REALE

La blockchain può avere accesso solo ai dati che si trovano sulla rete e dunque può avere accesso a funzioni limitate: ampliando i dati a cui quest'ultima può accedere accrescono anche le sue potenzialità. Ed è qui che entrano in gioco gli oracoli.

Gli smart contract sono stati introdotti, come già precedentemente detto, per estendere le funzionalità stesse della blockchain, ma in alcuni casi sono limitati. Per questo motivo, hanno bisogno di accedere a dati esterni e dunque di elaborare dati off-chain.

¹⁴ Bug: errore nel funzionamento di un software.

L'oracolo è un componente dell'architettura che permette agli smart contract di interfacciarsi con la blockchain per l'invio di dati off-chain. Ha la capacità di catturare dati da molteplici fonti per poi impacchettarli e fornirli alla blockchain. Il suo utilizzo si rende necessario per le limitazioni stesse dei contratti intelligenti, che non posso interagire, per loro natura, con dati e sistemi al di fuori.

Tali limitazioni derivano proprio dalla struttura della blockchain, progettata per essere sicura ed inattaccabile, e dunque creata per essere completamente isolata dal mondo esterno. Ciò costituisce un vantaggio ma anche un limite, e questo è il motivo per cui nasce la necessità di ampliare lo spettro delle applicazioni possibili per garantire l'interoperabilità.

Ad esempio, tutte le applicazioni DeFi richiedono l'accesso a dati esterni e dunque è necessario, per il loro corretto funzionamento, l'utilizzo degli oracoli, essenziali per l'accesso a dati off-chain.

L'oracolo, dunque, non rappresenta un dato, bensì l'interfaccia che consente lo scambio di informazioni: deve essere affidabile ed in grado di fornire agli smart contract dati attendibili per non compromettere il loro funzionamento o esecuzione.

Esistono varie tipologie di oracoli: oracoli hardware, la cui funzione è l'estrazione di dati dal mondo fisico reale, ed oracoli software, che contrariamente procedono all'estrazione e aggregazioni di dati online, come ad esempio dalla rete internet, e sono in grado di fornire tali info in tempo reale. Tale ultima funzione non può essere unicamente assolta dallo smart contract, ma è chiaro che per il corretto funzionamento delle DApp è necessaria l'integrazione degli oracoli.

Di fatto, la direzione verso cui tale progresso muove è precisa: l'integrazione degli smart contract e oracoli per lo sviluppo di DApp sempre più sofisticate.

La struttura dell'oracolo può essere centralizzata o decentralizzata: la prima consente lo scambio di informazioni che provengono da un'unica entità centrale e comporta un rischio evidente in quanto tutte le informazioni sono concentrate in un unico punto. Se l'oracolo dovesse venire hackerato o dovesse andare offline, il resto delle applicazioni che fanno affidamento su di esso non potrà più funzionare correttamente e dunque gli smart contract non potrebbero più accedere ai dati necessari per l'esecuzione delle loro funzioni.

L'oracolo decentralizzato invece, è distribuito su più nodi ed è in grado di aggregare più fonti di informazioni: l'oracolo può essere attaccato in più punti ma la decentralizzazione assicura maggiore integrità dei dati. Gli smart contract, in aggiunta, si servono di più punti di informazioni.

Il funzionamento dell'oracolo è articolato in più fasi: raccolta di dati off-chain, aggregazione ed invio dei dati alla blockchain, consegna dei dati finiti agli smart contract. Una volta memorizzati i dati, tutti gli smart contract possono accedere ai dati tramite le funzioni dell'oracolo. Infine, da direzione dei dati comunicati tramite gli oracoli può variare, a seconda se questi siano oracoli di input o output. Gli oracoli di input si occupano della ricerca di dati off-chain e della loro comunicazione agli smart contract. Gli oracoli di output invece, prelevano dei dati dagli smart ed eseguono azioni off-chain. Gli ambiti in cui ad oggi vengono maggiormente utilizzati gli oracoli sono essenzialmente DeFi, applicazioni di gaming e NFT; il loro necessario utilizzo è giustificato

dal fatto che, in particolar modo negli ambiti sopra elencati, è necessario un continuo aggiornamento di dati in tempo reale.

CAPITOLO SECONDO

TOKEN NON FUNGIBILI

La maggior parte delle persone, quando sente parlare di blockchain, associa questa particolare tecnologia alle criptovalute. In realtà, la blockchain può essere vista come mezzo attraverso cui è possibile l'utilizzo delle criptovalute ma, come già detto, queste ultime sono solo uno dei tanti possibili utilizzi.

Una delle più recenti applicazioni, infatti, riguarda i non-fungible token, meglio noti come NFT. Per poter al meglio comprendere cosa si intende per NFT, bisogna innanzitutto chiarire il concetto di token e di conseguenza quello dei token non fungibili.

2.1 TOKEN E TOKENIZZAZIONE

I token¹⁵ non sono altro che stringhe di carattere che riproducono un'unità di valore all'interno di un sistema informatico che permette agli utenti di interagire con esso direttamente, senza la presenza di intermediari. In generale, dunque, possono essere considerati come rappresentazioni digitali il cui scopo è il trasferimento di valore.

I token, come anche i coin¹⁶, vengono qualificati come criptovalute ma vi è una netta distinzione tra essi. Mentre i coin vengono direttamente creati sulla blockchain e sono la moneta nativa di quest'ultima, alternativi alla moneta fiat, i token si basano su blockchain preesistenti ed incorporano un'ampia gamma di attività e servizi.

Al termine token, è gioco forza associare quello della tokenizzazione. Per tokenizzazione si intende il processo attraverso cui un'informazione, un oggetto o una risorsa viene convertita in token e dunque, l'output ottenuto non è altro che la rappresentazione digitale dell'entità o informazione precedentemente sottoposta a tokenizzazione.

In particolare, nell'ambito della blockchain, il risultato finale derivante dal processo di tokenizzazione è un asset o una valuta all'interno dello stesso ledger.

Tale processo di trasformazione non solo permette all'utente di acquisire la proprietà del token, ma comporta che le informazioni dell'oggetto o della risorsa già convertita in token, vengano riportate all'interno di un blocco della blockchain. Ottenuto il token, quest'ultimo può essere scambiato e trasferito tra gli utenti presenti all'interno della piattaforma, proprio perché l'utente ne diventa legittimo proprietario.

¹⁵ Token: letteralmente gettone.

¹⁶ Coin: moneta.

2.2 LA DISTINZIONE TRA TOKEN DI UTILITÀ E TOKEN DI SICUREZZA

Con il termine ICO viene indicato un progetto di finanziamento definito come “Initial Coin Offering”.

Oggetto dell’offerta delle ICO possono essere due tipologie di token: utility token e security token.

I token di utilità sono un modo per finanziare progetti precedentemente non finanziati. Per costruire un tale ecosistema, alcuni token possono essere "pre-estratti" e venduti in un "crowdsale" durante il lancio del token. Lo scopo di questo token è di consentire l'accesso ai prodotti o ai servizi dell'azienda in futuro. Creando utility token, le startup possono vendere "coupon digitali" per i servizi che stanno sviluppando, proprio come alcuni rivenditori di elettronica accettano preordini per videogiochi che non verranno rilasciati per mesi. I token di utilità rappresentano servizi o unità di servizio che possono essere acquistati ancorché non ancora disponibili sul mercato. La caratteristica distintiva di questa tipologia di token è che non sono ideati come strumento d’investimento e ciò comporta l’impossibile applicazione a questi ultimi delle leggi relative ai titoli finanziari a tutela dei risparmiatori.

I token di sicurezza mentre raffigurano la proprietà di un asset nel mondo reale: sono dunque coloro che regolano gli NFT. Questi ultimi, infatti, utilizzano un sistema blockchain per tracciare e verificare i proprietari degli asset.

I security token inoltre, facilitano l’accesso a investimenti multipli. È di fatto possibile la creazione di un portafoglio digitale basato su blockchain che può contenere differenti token di sicurezza, esattamente come un conto d’investimento può incorporare diverse azioni e obbligazioni. Nessuno dei due tipi di token richiede la propria blockchain in quanto è possibile l’esternalizzazione dei relativi sistemi di contabilità e archiviazione, utilizzando registri blockchain preesistenti. Ad esempio, nel caso degli NFT, la maggior parte dei marketplace si affida alla blockchain di Ethereum: ecco perché gli utenti che inviano token tracciati e registrati sulla blockchain di Ethereum devono pagare alla piattaforma una piccola commissione di transazione, una gas tax¹⁷, ecc. rete di ragioni per convalidare le transazioni.

2.3 FUNGIBLE E NON-FUNGIBLE TOKEN

I token fungibili e non fungibili si differenziano per due particolari caratteristiche appartenenti esclusivamente ai token non fungibili: la rarità e l’unicità.

I token fungibili in particolare sono standardizzati ed intercambiabili tra loro. Ciò significa che possono essere divisi in sottounità e sono perfettamente uguali tra di loro. Un esempio pratico è rappresentato dal Bitcoin: non è possibile distinguere un bitcoin da un altro.

¹⁷ Gas tax: equivalente alla fee tax già precedentemente descritta.

Diversamente, per i NFT: non è possibile la loro suddivisione in sottounità in quanto ciascun NFT è unico ed irripetibile. Ciò perché, nello specifico, un NFT altro non è che la rappresentazione di un asset di valore che in quanto unico, non può essere scambiato allo stesso modo dei token fungibili: da qui, infatti, il termine “non-fungible”.

I token memorizzando informazioni aggiuntive, risultano per natura maggiormente complessi rispetto le semplici criptovalute. Per questo motivo un token non fungibile può essere definito come la proprietà digitale di un oggetto sottoposto a tokenizzazione. Un NFT può essere qualsiasi cosa sia unica, con un valore, anche potenziale, e che possa essere archiviata digitalmente. In sostanza, sono proprio come qualsiasi altro oggetto da collezione fisico, ma invece di avere una rappresentazione del mondo reale, sono file JPG. Tutto ciò, compreso il mantenimento della proprietà del NFT da parte dell'utente, è reso possibile grazie alla sua rappresentazione su blockchain mediante smart contract. Infatti, più nello specifico, possedere un NFT significa possederne il certificato di autenticità e proprietà: l'opera non diviene privata, è comunque accessibile online, ma i diritti di proprietà vengono ceduti dal creatore all'acquirente e, sarà proprio quest'ultimo, il solo ed unico a vantare diritti derivanti dalla proprietà dell'asset stesso.

2.4 ETHEREUM REQUEST FOR COMMENT

Gli Ethereum Request for Comment, meglio noti come ERC, sono standard tecnici utilizzati sulla piattaforma di Ethereum. Tali standard fungono da linee guida che gli sviluppatori di applicazioni o smart contract devono seguire affinché questi ultimi possano essere caricati all'interno della piattaforma Ethereum. Definire il preciso standard che lo sviluppatore deve necessariamente utilizzare, comporta la semplificazione del processo di sviluppo.

La piattaforma ha sviluppati differenti standard, a seconda dell'oggetto della creazione. Di seguito, vengono riportati gli ERC maggiormente utilizzati.

ERC-20

Lo standard Ethereum Request for Comment – 20 viene utilizzato per la creazione di token fungibili ovvero intercambiabili tra loro, all'interno della piattaforma Ethereum. Tale standard fu per la prima volta proposto nel 2015 da Fabian Vogelsteller e, ad oggi, è lo standard maggiormente utilizzato per i token fungibili.

L'insieme di regole definite riguardano la capacità di trasferire token fra indirizzi e l'approvazione dei relativi trasferimenti. Seguendo l'ERC-20 viene non solo facilitata l'interazione tra token, ma anche tra DApp dato che anche quest'ultime seguono tale tipologia di standard.

ERC-721

A differenza dello standard precedentemente descritto, l'ERC-721 definisce le regole per i token non fungibili, differenti da quelli fungibili. Le funzioni collegate ad ERC-721 comprendono la capacità di trasferimento di proprietà del NFT da un indirizzo ad un altro, nonché la capacità di reperire informazioni circa un determinato NFT. Le DApp, oltre che poter seguire ERC-20, possono anche essere implementate su ERC-721.

ERC-1155

Nato nel 2018 grazie a Enjin, questo standard permette la gestione e la creazione di entrambe le tipologie di token, fungibile e non-fungibile, nonché la loro interazione con gli smart contract.

I token ERC-1155 possono rappresentare una varietà di asset, come oggetti di gioco, valuta virtuale e altri asset digitali. Sono progettati per essere altamente efficienti ed economici, in quanto consentono l'archiviazione di molteplici token all'interno di un singolo contratto, riducendo le gas fee associate alla gestione di un gran numero di token. Tra le altre regole che lo standard stabilisce troviamo la creazione di token fungibili e non fungibili all'interno dello stesso contratto, il trasferimento di token tra indirizzi, l'ottenimento del saldo di un particolare indirizzo e l'approvazione o disapprovazione del trasferimento di token.

2.5 STORIA DEGLI NFT

La storia dei non-fungible token ha inizio nel 2017, con l'introduzione sul mercato del videogioco, CryptoKitties che ha consentito l'introduzione degli NFT ad un pubblico esteso. Il videogioco permette agli utenti di acquistare e allevare i gatti virtuali presenti al suo interno in edizione limitata. Il primo NFT venduto su Cryptokitties è stato battuto all'asta per 246 ETH (circa 113.000 dollari) nel Novembre del 2017.

Figura 1.2, Genesis Cat.



Genesis

#1 ⚡ Gen 0 ⌚ Fast Cooldown (1m)

Stimpson J. Cat
Owner



Immagine riportare da CryptoKitties, <https://www.cryptokitties.co/kitty/1>.

All'interno del game è possibile far accoppiare gatti virtuali al fine di creare nuovi gattini con differente rarità. Si evince dunque che l'elemento di rarità di questi NFT è rappresentato dai tratti genetici degli stessi. Nonostante tale gioco on-chain¹⁸ non sia considerato un reale videogame ha acquistato importanza per due differenti motivi: gli sviluppatori hanno ideato un algoritmo di allevamento nascosto dietro uno smart contract che stabilisce la sequenza genetica del gatto e dunque i suoi attributi e, inoltre, è stato inventato il contratto d'asta olandese¹⁹, uno dei più utilizzati per la scoperta del prezzo degli NFT.

Il sistema del gioco comporta l'acquisto del NFT da parte dell'utente il quale, una volta fatto accoppiare il proprio gatto con un altro sempre in suo possesso, rivende on-chain il gatto ottenuto dall'accoppiamento dei primi due.

Il successo del gioco fu immediato anche se non fu un bene. La giustificazione di tale affermazione risiede nel fatto che sulla piattaforma di Ethereum è possibile l'elaborazione di un numero limitato di transazioni alla volta e, essendoci stata un'affluenza sulla rete maggiore rispetto a quello che Ethereum avrebbe potuto effettivamente sostenere, un grande numero di transazioni rimasero in sospeso e per questo, il prezzo delle gas tax aumentò al crescere delle transazioni. La problematica descritta deriva essenzialmente da problemi di scalabilità.

I nuovi utenti pagavano dunque tasse elevate e aspettavano ore prima che le loro transazioni venissero approvate. Tutto ciò condusse alla "bolla CryptoKitty": in una fase iniziale, la nuova domanda comportò la crescita dei prezzi i quali, a loro volta, determinarono l'ulteriore aumento della domanda.

¹⁸ On-chain: transazione o processo che avviene sulla blockchain.

¹⁹ Contratto d'asta olandese: tipologia di asta che ha come punto di partenza un prezzo elevato che, pian piano, decresce. Il partecipante che ferma la discesa si aggiudica l'asset al prezzo annunciato.

Molte persone, dunque, hanno investito in CryptoKitty spingendo il prezzo degli NFT alle stelle, ma tale bolla speculativa ebbe una rapida deflazione con il crollo dei prezzi dei token.

Ma nonostante il crollo del mercato, gli investitori hanno visto negli NFT una vera e propria opportunità; di fatto, successivamente a CryptoKitty, sono stati sviluppati nel 2018-2019 altri videogame caratterizzati dalla presenza di NFT all'interno, come Axie Infinity.

Sempre nel 2018 inoltre, venne lanciato il progetto del metaverso di Decentraland, piattaforma all'interno della quale è possibile l'acquisto di territori virtuali resi NFT, che riesce a raggiungere i 26,000,000€ tramite ICO.

Inoltre, aumentata la notorietà, è stata ideata una piattaforma di monitoraggio di NFT, ovvero "NonFungible.com".

Nello stesso periodo, inoltre, si inizia ad avvicinare a tale tipologia di asset anche il mondo dell'arte: se una delle caratteristiche principali degli NFT è proprio quella di confermare l'autenticità dell'opera, è altresì vero che autenticità e verifica sicura della proprietà di un'opera sono attributi essenziali affinché l'opera stessa abbia un valore reale. È questo il motivo per cui sono emerse numerose piattaforme di arte digitali e sono stati creati marchi reali utilizzando proprio gli smart contract.

Nel 2021 di fatto, viene venduta la celebre opera "the First 5000 Days" al prezzo di 69,300,000€. Gli ambiti di applicazione, tuttavia, sono innumerevoli: il fondatore di Twitter²⁰, Jack Dorsey, tokenizzato il suo primo tweet, lo vende al prezzo di 2,900,000€.

2.6 CARATTERISTICHE NFT

UNICITA'

Ciò che caratterizza i NFT sono i metadati²¹: è ciò che rende l'asset differente da tutti gli altri. Attraverso i metadati è possibile l'archiviazione permanente, senza possibilità di alterazioni. I metadati contenuti, rendendo i NFT unici, possono essere paragonati al certificato di autenticità che rende un'opera d'arte nel mondo reale, per l'appunto, autentica. Sempre i metadati, oltre che identificare il NFT, delineano l'identità digitale di quest'ultimo.

RARITA'

²¹ Metadati: insieme di informazioni utilizzate per descrivere un altro insieme di dati, consentendo l'identificazione, la classificazione, l'archiviazione e il recupero in modo efficiente.

A scegliere la quantità del NFT da rendere disponibile sul mercato, è lo sviluppatore stesso. Dato che però nella maggior parte dei casi la scarsità è una variabile determinante nel prezzo poiché rende lo stesso NFT più appetibile agli occhi dell'acquirente, il creatore sceglie sempre lo sviluppo di un singolo NFT oppure di molteplici ma con caratteristiche minime che ne permettono la distinzione. In ogni caso però, ogni NFT ha un identificativo univoco con un solo proprietario, anche se ne esiste un altro visibilmente identico.

INTEROPERABILITA'

Gli standard creati per lo scambio dei NFT consentono che quest'ultimi si muovano facilmente sul mercato: ciò avviene perché una volta pubblicato l'NFT, è possibile accedere a quest'ultimo non solo dal marketplace all'interno del quale viene reso disponibile, ma anche da altri fornitori di portafogli e consentendo lo scambio del NFT su diversi mercati.

2.7 FORMATO

I formati ammessi per la creazione degli NFT sono vari e dipendono essenzialmente da quanto stabilito dalla piattaforma, così come anche la dimensione massima che può essere raggiunta dal singolo file.

Per quanto concerne la dimensione, che per l'appunto dipende dalla piattaforma, solitamente varia dai 20 MB fino ad arrivare ai 400 MB.

I tipi di file genericamente ammessi sono: jpg, gif, mp3, mp4, png, svg, wav, ogg, glb, glt, webm.

Ciò significa che gli NFT possono essere: video, audio, immagini e modelli 3D.

2.8 FUNZIONAMENTO

Affinché gli NFT possano essere trasferiti all'interno di un marketplace, diventano indispensabili gli smart contract. Questi ultimi, oltre che rendere possibile lo scambio di NFT su mercati differenti, sono indispensabili per confermare la proprietà del token.

Dunque, smart contract e NFT sono strettamente collegati tra loro: gli NFT rappresentano un asset digitale, presente sulla blockchain, gli smart contract invece sono programmi software eseguiti sempre sulla blockchain, che consentono lo scambio dei token e rendono disponibili informazioni circa, non solo l'attuale proprietario del NFT, ma anche di tutti quelli precedenti e dunque l'history²² del NFT.

I NFT vengono conservati all'interno del wallet, utilizzato anche per verificare le transazioni in entrate ed in uscita dell'indirizzo ad esso associato. I wallet, a loro volta, possono essere distinti in "hot wallet" e "cold

²² History: termine utilizzato per indicare l'elenco dei soggetti a cui è appartenuto il NFT a partire dalla sua creazione.

wallet”. Gli hot wallet sono completamente online e l’esito positivo di ogni transazione è subordinato all’autorizzazione, che può essere data solo tramite connessione al portafoglio possibile solo se si è in possesso della chiave privata, generata online a partire dall’indirizzo dell’utente. Questa tipologia di wallet viene molto più comunemente usata per transazioni che hanno ad oggetto criptovalute o NFT. I cold wallet sono di contro molto più sicuri e per questo motivo vengono utilizzati per la protezione di grandi patrimoni. La loro sicurezza deriva dal fatto che la chiave privata, generata a partire dall’indirizzo pubblico, viene creata offline per poi essere trasmessa alla blockchain tramite un dispositivo collegato ad internet. Questi ultimi, pertanto, hanno un livello di sicurezza di gran lunga superiore agli hot wallet in quanto, non essendo la chiave generata online, non può essere rubata e dunque è impedito l’accesso a quanto contenuto nel wallet.

Dunque, i NFT sono verificati e protetti dalla blockchain, ne è definita la proprietà e contengono al loro interno l’history.

Ogni NFT presenta: un’anteprima, per dare un aspetto visuale al token, una descrizione, volta a fornire la storia del NFT, i tratti, che nella maggior parte dei casi sono indicativi della rarità del NFT.

Di seguito, viene riportato un esempio di NFT, nello specifico una Bored Ape, di cui è possibile vedere l’anteprima e i tratti.

Figura 2.1, BoredApe YachtClub.

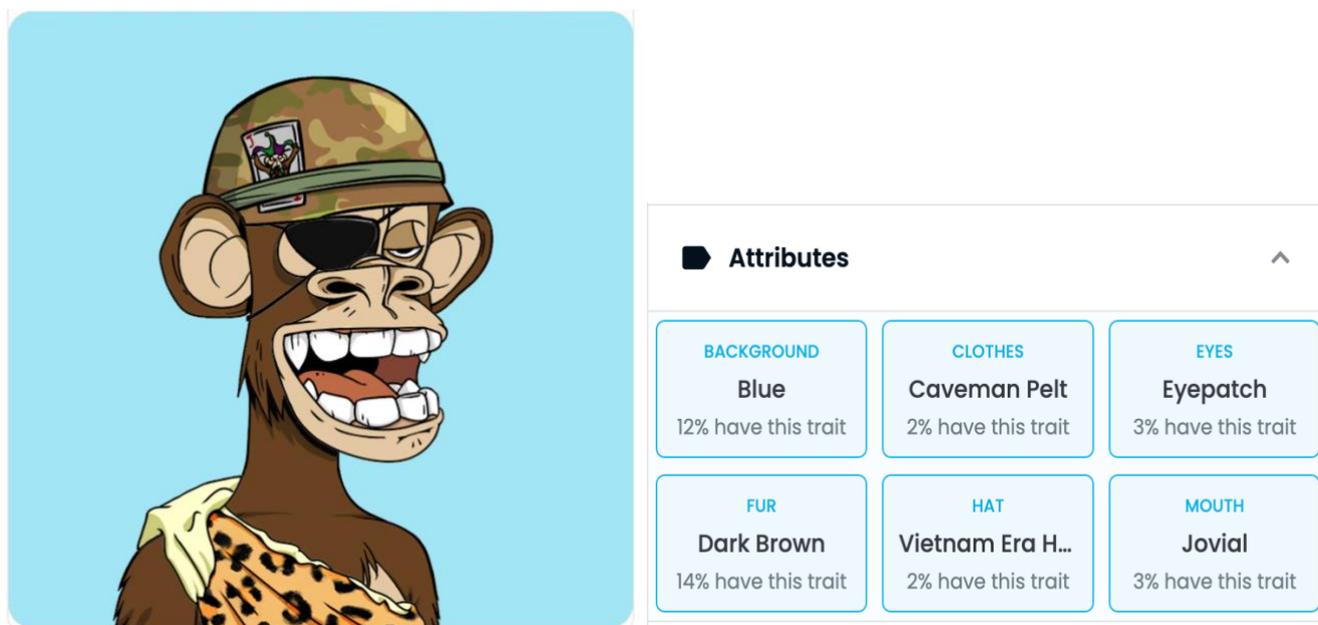


Immagine riportata da OpenSea.

Nella parte destra è resa disponibile la visuale dell’anteprima, nella parte sinistra mentre, sono indicati i tratti che caratterizzano l’NFT. Di seguito invece, viene riportata la sezione dettagli della Bored Ape.

Figura 2.2, dettagli BoredApe YachtClub.

Details	
Contract Address	0xbc4c...f13d
Token ID	2017
Token Standard	ERC-721
Chain	Ethereum
Metadata	Frozen
Creator Earnings ⓘ	2.5%

Immagine riportata da OpenSea.

In particolare, nella sezione dettagli, è possibile verificare le seguenti informazioni: l'indirizzo dell'attuale possessore dell'NFT dal quale è possibile accedere all'history, il token identificativo, che è univoco, lo standard con il quale è stato creato il NFT, la blockchain di riferimento, i metadati e la percentuale di guadagno che spetta al creatore per ogni rivendita del NFT successiva alla prima.

La percentuale spettante al creatore ogni volta che viene venduto il NFT viene definita royalty. Quest'ultima viene delineata direttamente all'interno dello smart contract e, una volta definito il contratto, non potrà mai più essere modificata. Può essere prevista o meno all'interno del contratto solo dal suo creatore. La royalty può essere parimeriti paragonata alle gas fee. Infatti, rappresentano entrambe costi di transazione in capo all'acquirente per l'acquisto del NFT. Solitamente, è una percentuale nella misura variabile dal 3% al 10%, stabilito sempre a discrezione del creatore.

Le piattaforme in cui avviene lo scambio di NFT vengono per l'appunto definite marketplace. Trattasi di luoghi virtuali dove possono esseri comprati o venduti token in base all'accettazione o meno da parte del market degli standard del token stesso. Come già detto precedentemente, è il creatore a stabilire se inserire o meno all'interno dello smart contract una royalty. In realtà l'ultima parola spetta proprio al marketplace che può scegliere se commerciare o meno NFT che prevedono la royalty, proprio per ridurre i costi di transazione che l'acquirente deve sopportare dato che quest'ultimo dovrà innanzitutto pagare la gas fee per l'acquisto alla piattaforma. Tuttavia, i marketplace che non prevedono l'inserimento della royalty all'interno dello smart contract, sono quelli meno trafficati in quanto tutelano minormente il creatore dell'opera, non consentendogli un guadagno perpetuo.

Le modalità d'acquisto degli NFT in realtà sono molteplici, ma variano in base alla categoria di NFT. Nello specifico, se prendessimo come esempio un videogame, le modalità d'acquisto degli asset messi a disposizione potrà avvenire, oltre che nel marketplace, anche all'interno del videogioco o potrà essere guadagnato dall'utente giocando al videogame stesso.

2.9 CATEGORIE

COLLECTIBLES

Definiti anche collectibles, gli oggetti in questione sono NFT creati per essere collezionati. Nella maggior parte dei casi vengono lanciati attraverso drop: viene annunciato il giorno di lancio dei token e gli acquirenti scommettono su quelli che comprano. Il loro valore è interamente basato sulla loro scarsità e unicità e sono creati a partire da algoritmi di intelligenza artificiale che combinano le loro componenti randomicamente per poter appunto ottenere, un NFT unico. Inoltre, possono contenere delle utility ovvero funzionalità anche esterne che conferiscono al possessore ulteriori diritti oltre quello di proprietà. È possibile trovare tra i collectibles tra i più vari asset digitali: opere d'arte, oggetti, carte, skin²³, armature e personaggi di videogiochi.

CRYPTO ARTE

L'applicazione di smart contract ed NFT al mondo dell'arte è di facile intuizione. Tramite NFT viene accertato il proprietario effettivo dell'opera e, sempre tramite quest'ultimo, ne viene provata l'autenticità. Rendere un'opera d'arte un NFT significa dunque reprimere fenomeni illegali propri del mondo dell'arte come, ad esempio, la contraffazione delle opere. Inoltre, all'interno degli smart contract, l'autore può prevedere una royalty, che, come già visto, consente, nella pratica, l'attribuzione di una percentuale fissa al creatore dell'opera per ogni rivendita successiva la prima. Le royalties consentono di superare i limiti entro cui possono essere applicati nel mondo reale i diritti di seguito. È vero che questi ultimi consentono all'autore, come le royalties, di percepire una percentuale per ogni rivendita, tuttavia, la loro applicazione non è sempre prevista. Questi ultimi, infatti, nella normativa italiana trovano applicazione esclusivamente per opere che superano il valore di 3.000,00€ e solo nel caso in cui la cessione dell'opera non avvenga tra privati.

SPORT

Il mondo dello sport può contare su un numero di appassionati non indifferente e gli NFT rappresentano ad oggi, una porzione del guadagno del mercato sportivo. Tramite NFT, possono essere destinati alla vendita autografi, carte di giocatori, trofei e foto. Soprattutto nel mondo, agli NFT sportivi vengono associate delle utility che vanno da diritti di partecipazione alla community alla vendita di biglietti per eventi sportivi.

REAL ESTATE

²³ Skin: caratteristica riguardante l'apparenza del personaggio di un videogame che va a mutare il suo aspetto.

Per quanto riguarda l'ambito del real estate, è necessario introdurre più ampiamente il concetto di metaverso. Con il termine metaverso si suole indicare un universo parallelo all'interno del quale è possibile ricreare esperienze reali in un mondo che non esiste realmente, ma che è frutto della combinazione di video, realtà virtuale e aumentata. Se l'intento del metaverso è proprio quello di consentire agli utenti al suo interno la possibilità di vivere virtualmente delle esperienze proprie e tipiche del mondo reale, viene certamente consentito l'acquisto di molteplici categorie di beni, dagli immobili sino ad oggetti preziosi o qualsiasi altro bene che possa essere oggetto di tokenizzazione.

GAMING

Il mondo dei videogiochi ha subito, e continua a subire, l'hype derivante dal mondo NFT e blockchain. In particolare, ad oggi, c'è la possibilità di guadagnare all'interno dei games qualsiasi asset che nel mondo reale è una risorsa preziosa. I token nei game rappresentano oggetti unici, come personaggi, oggetti o altri beni digitali, che possono essere utilizzati all'interno dei giochi. I token NFT stanno diventando sempre più popolari nel mondo dell'intrattenimento ludico, poiché offrono ai giocatori la possibilità di acquisire e scambiare proprietà digitali in modo sicuro e trasparente. Inoltre, i token NFT possono essere utilizzati per creare giochi basati sulla proprietà, in cui i giocatori possono acquisire e scambiare proprietà digitali all'interno del gioco. Quanto detto, è solo una porzione degli ambiti di applicazioni del mondo dei game, che verrà accuratamente analizzato nel capitolo successivo.

CAPITOLO TERZO

SERIE STORICHE E GAME

Un fenomeno che sta prendendo piede nell'ultimo decennio, da quando le funzioni di alcune blockchain non sono più solo circoscritte alle sole transazioni di criptovalute, è il fenomeno dei “play to earn”. Il termine “play to earn” viene utilizzato per tutti quei videogiochi, nonché DApp, implementati all'interno di una blockchain che preveda il loro utilizzo sulla base di uno smart contract.

Il maggior impatto della blockchain nel mondo dei videogames è rappresentato dall'utilizzo dei NFT. Come già detto, i NFT dei games sono oggetti unici, come personaggi, oggetti o altri asset digitali che possono essere utilizzati all'interno dei giochi. La popolarità dei NFT all'interno dei games deriva dalle loro potenzialità: in concreto, offrono ai gamers la possibilità di acquistare e scambiare proprietà digitali in modo sicuro e trasparente. Ulteriore modo in cui la blockchain sta rivoluzionando il mercato dei videogames è l'utilizzo delle DApp, nel caso specifico, si parla di videogiochi decentralizzati. Questi ultimi sono tipologie di games che non dipendono da server centrali e ciò implica una maggiore resistenza a problemi legati alla sicurezza e all'equità. In sintesi, la blockchain sta rapidamente diventando una parte importante del mondo dei videogiochi per le opportunità che offre non solo ai giocatori, ma anche agli sviluppatori dei videogames.

La novità di questi videogiochi, inoltre, è rappresentata dalla possibilità per gli utenti di ottenere un guadagno reale giocando al videogioco o scambiando oggetti al suo intero e dunque il gamer viene ripagato per il tempo e l'impegno che lui stesso spende all'interno del game. La costituzione dei “play to earn” all'interno della blockchain implica che il videogioco stesso sia decentralizzato. La decentralizzazione, a sua volta, permette a tutti i gamers di interagire con altri gamers all'interno del gioco e dunque viene meno la centralizzazione della casa madre, produttrice del videogioco.

3.1 UTILIZZO DELLA BLOCKCHAIN NEL GAMING

L'applicazione della blockchain sta influenzando e rivoluzionando il concetto di videogioco sotto molteplici aspetti, in particolare per quanto concerne le proprietà digitali, i giochi decentralizzati, le monete virtuali e le transazioni.

Per quanto riguarda le proprietà digitali, la tecnologia permette ai giocatori di acquistare e scambiare asset presenti all'interno del game. Questo significa che i giocatori possono possedere realmente le loro “in-game items”²⁴ e scambiarle con altri giocatori. Il possesso da parte del giocatore dell'asset deriva dalla sua registrazione all'interno della blockchain e, dato che l'asset altro non è che un NFT, a quest'ultimo corrisponde

²⁴ In-game items: oggetti presenti all'interno del videogioco volti a potenziare il personaggio.

un identificativo univoco che permette la sua identificazione nonché l'identificazione dell'utente che lo possiede. Ciò che conferisce valore al NFT non è solo l'unicità, ma anche la rarità. Molto spesso, infatti, i NFT rilasciati sono limitati nella quantità e ciò implica che il loro valore, data la scarsità, può crescere nel tempo. I NFT all'interno del game possono essere guadagnati in molteplici modi: completamento di missioni, vittorie di battaglie o acquisto presso altri giocatori. Altra caratteristica degli asset digitali dei games è rappresentata dalla possibilità di commercio. Infatti, è possibile la loro conservazione, scambio o vendita su marketplace specializzati, offrendo la possibilità ai giocatori di monetizzare le loro abilità di gioco e le loro proprietà virtuali, ottenendo come output finale un guadagno reale.

I giochi decentralizzati, invece, rientrando nella categoria delle DApps, sono basati su uno smart contract. Ciò che discende da tali presupposti è che il gioco stesso viene eseguito autonomamente e dunque senza la necessità di server centrali. La soppressione del server centrale implica una maggiore sicurezza in quanto i dati e le attività dei videogames sono integralmente registrati sulla blockchain e protetti da crittografia.

Altro tema sono le monete virtuali. Attraverso tale termine si suole indicare la valuta utilizzata all'interno del game che può essere guadagnata dal gamer nello stesso modo in cui vengono guadagnati gli asset digitali. Attraverso le monete virtuali, è possibile l'acquisto o la vendita di proprietà digitali non solo all'interno del game, ma molto spesso anche all'interno di marketplace specializzati nell'ambito dei quali sono previsti tali asset.

3.2 STRUMENTI PER LA COMPrensIONE DEL FENOMENO

La blockchain, dunque, ha apportato molteplici benefici nel mondo del game, dando inizio ad una rivoluzione irreversibile. Al fine di poter comprendere al meglio tale cambiamento, ed in particolare di come alcuni videogiochi abbiano avuto più o meno successo, è necessaria un'analisi in serie storiche del volume delle transazioni e del valore dei cripto-game implementati su tecnologia blockchain. Di seguito viene approfondita la metodologia di analisi e la tecnica di analisi utilizzata.

3.3 SERIE STORICHE, APPROCCIO STOCASTICO E VARIABILI CASUALI

Le serie storiche sono una sequenza di osservazioni di una variabile osservata nel tempo, in cui gli eventi sono registrati in ordine cronologico. Queste osservazioni possono essere raccolte in diversi intervalli di tempo: giorni, settimane, mesi, trimestri, anni, ecc. Le serie storiche possono essere utilizzate per analizzare e comprendere il comportamento di una variabile nel tempo, identificando le tendenze, le fluttuazioni stagionali e le variazioni irregolari e dunque la loro analisi può avere come fine ultimo la descrizione o spiegazione di un fenomeno d'interesse o, inoltre, possono essere utilizzate per effettuare delle previsioni.

L'analisi delle serie storiche assume rilevanza in quanto è in grado di fornire informazioni utili per prendere decisioni informate, fare previsioni e identificare le tendenze e i cambiamenti nel tempo.

L'analisi di cui si discorre è stata arricchita, negli ultimi anni, grazie all'utilizzo di tecniche e strumenti di analisi più sofisticati, come l'utilizzo di modelli stocastici e di "machine learning". Questi permettono di modellare la variabilità del fenomeno nel tempo in modo più accurato, considerando anche la presenza di eventuali trend e stagionalità. Inoltre, l'analisi delle serie storiche viene sempre più integrata con l'analisi dei dati, al fine di ottenere una maggiore comprensione del fenomeno e individuare eventuali legami temporali con altri fattori. Al fine di poter al meglio comprendere le modalità di utilizzo delle serie storiche, è necessario approfondire il concetto di approccio stocastico.

In statistica l'approccio stocastico si riferisce all'uso di modelli probabilistici per descrivere e analizzare fenomeni che presentano caratteri di incertezza e variabilità. In questo approccio, le variabili vengono considerate come variabili casuali, ovvero come quantità che possono assumere diversi valori in modo casuale, ma con una certa distribuzione di probabilità. A loro volta, le variabili casuali sono quelle che influenzano l'andamento di una serie storica e dunque, in altre parole, sono responsabili dell'andamento osservato all'interno della serie stesse.

L'analisi stocastica viene utilizzata in molti campi della statistica, tra cui l'analisi dei dati in serie storiche e la previsione. Nello specifico, l'approccio stocastico per le serie storiche consiste nell'utilizzare modelli probabilistici per descrivere e analizzare le serie temporali, ovvero le sequenze di dati raccolti in modo ordinato nel tempo. Questo approccio si basa sull'idea che i dati delle serie storiche sono il risultato di un processo casuale che può essere descritto da un modello matematico basato sulla teoria delle probabilità.

Uno dei modelli stocastici più utilizzati è il modello ARIMA (Autoregressive Integrated Moving Average), che combina l'analisi dell'autocorrelazione (AR) e la media mobile (MA) per catturare le tendenze e le fluttuazioni casuali della serie storica. Il modello ARIMA viene utilizzato per la previsione della serie storica, ovvero per stimare i valori futuri della serie sulla base dei dati storici.

3.4 CLASSIFICAZIONE DELLE SERIE STORICHE

Innanzitutto, è utile disporre di una classificazione delle serie storiche in base al tipo di serie temporale che si desidera analizzare. La prima differenza riguarda il tempo che intercorre tra due osservazioni consecutive. Si possono distinguere due tipi di serie storiche: regolarmente distanziate nel tempo e irregolarmente distanziate nel tempo. Nel primo caso l'intervallo tra due osservazioni consecutive è costante. Nel secondo caso, l'intervallo tra due osservazioni consecutive non è costante ma varia, ed è descritto statisticamente da una variabile casuale. In questo caso, è necessario specificare un modello probabilistico per il tempo tra le osservazioni.

La seconda differenza riguarda il numero di fenomeni di interesse. Puoi avere serie temporali univariate o multivariate. Infine, si può considerare la distinzione tra serie storiche riferite a fenomeni di stock e serie storiche riferite a fenomeni di flusso. Nel primo caso, la grandezza osservata viene rilevata in un determinato momento nel tempo. Nel secondo caso, l'intervallo temporale di riferimento rileva la grandezza. Tutte queste distinzioni sono importanti per determinare il metodo statistico più appropriato per analizzare le serie storiche. Ad esempio, l'analisi di serie temporali irregolarmente spaziate richiede metodi statistici più complessi, mentre l'analisi di serie temporali multivariate deve considerare la relazione tra diversi fenomeni. Inoltre, la distinzione tra le serie storiche sui fenomeni di stock e le serie storiche sui fenomeni di flusso è importante per l'attuazione di eventuali aggiustamenti dovuti a cambiamenti di calendario.

3.5 OPERATORE RITARDO E OPERATORE DIFFERENZA

L'operatore ritardo viene ampiamente utilizzato nell'analisi delle serie temporali in quanto indica la relazione esistente tra i valori della serie in momenti di tempo differenti. L'operatore ritardo può essere definito "backward" e dunque indicato con B oppure, nella terminologia anglosassone, viene definito "lag operator" e, per questo motivo, è indicato con la lettera L. Il lag operator viene definito nel seguente modo:

$$LY_t = Y_{t-1}$$

$$L^2Y_t = Y_{t-2}$$

$$L^kY_t = Y_{t-k}$$

Data una costante a , $La=a$.

L'operatore differenza di contro, come il termine stesso suggerisce, indica la differenza, nonché la variazione, tra due valori nel tempo. L'operatore differenza prima viene indicato nel seguente modo:

$$\Delta Y_t = Y_t - Y_{t-1} = Y_t(1 - L)$$

L'operatore differenza seconda mentre, è definito:

$$\Delta^2 Y_t = \Delta \Delta Y_t = \Delta(Y_t - Y_{t-1}) = Y_t - 2Y_{t-1} + Y_{t-2} = Y_t(1 - 2L + L^2) = Y_t(1 - L)^2$$

L'operatore differenza i-esima è dato da:

$$\Delta^i Y_t = Y_t(1 - L)^i.$$

La distinzione tra differenza prima, seconda, sino ad arrivare alla i-esima, consiste nel numero di osservazioni prese in considerazione. Più nello specifico, l'operatore differenza prima viene utilizzato per calcolare la differenza tra un'osservazione e la sua precedente, la differenza seconda per il calcolo della variazione tra l'osservazione e le sue due precedenti, l'operatore differenza i-sima per la differenza tra l'osservazione e le sue i-esime precedenti.

3.6 STAZIONARIETA' E INVERTIBILITA'

Stazionarietà ed invertibilità, nell'ambito dell'analisi delle serie storiche, sono due condizioni necessarie e richieste affinché possa essere realizzata l'autoregressione. Una serie storica viene definita stazionaria se:

1. Il valore atteso di ogni variabile Y_t , $E(Y_t)$ è costante e dunque non dipende da tempo;

$$E(Y_t) = \mu, \forall t;$$

2. La varianza di ogni variabile Y_t è finita e costante, anch'essa, non dipende dal tempo;

$$Var(Y_t) = \sigma < \infty, \forall t;$$

3. La covarianza tra Y_t e Y_{t-k} , indicata con γ_k , non dipende dal tempo t ma solo

dal ritardo k . Quindi, per il primo ritardo:

$$\gamma_1 = Cov(Y_1, Y_2) = Cov(Y_3, Y_2) = \dots = Cov(Y_t, Y_{t-1}),$$

per il secondo ritardo:

$$\gamma_2 = Cov(Y_2, Y_3) = Cov(Y_4, Y_3) = \dots = Cov(Y_t, Y_{t-2}),$$

per il generico ritardo k :

$$\gamma_k = Cov(Y_{k+1}, Y_1) = Cov(Y_{k+2}, Y_2) = \dots = Cov(Y_t, Y_{t-k}).$$

Il concetto di stazionarietà, dunque, presuppone che la distribuzione di probabilità della serie storica rimanga invariata con il trascorrere del tempo; diversamente, la serie viene definita non stazionaria. Sotto l'ipotesi assunta della stazionarietà, i modelli stimati possono essere utilizzati per effettuare previsioni.

Una serie storica viene definita invertibile quando la variabile dipendente Y_t può essere anche definita:

$$Y_t = h(Y_{t-1}, Y_{t-2}, Y_{t-3}, \dots) + a_t,$$

dove a_t rappresenta l'errore.

Se la serie storica è invertibile, è possibile la ricostruzione della sequenza originale dei valori della serie a partire dalle loro combinazioni passate.

3.7 FUNZIONE DI AUTOCORRELAZIONE GLOBALE E PARZIALE:

AUTOCOVARIANZA STANDARD

Correlazione e covarianza sono due concetti strettamente legati fra loro. Nell'ambito delle serie storiche, tuttavia, queste ultime vengono definite come autocorrelazione e autocovarianza. Nello specifico, l'autocovarianza esprime la relazione che intercorre tra due variabili casuali, entrambe espressione dello stesso fenomeno d'interesse ma differenti tra loro poiché lo esprimono in tempi differenti.

La generica autocovarianza può essere espressa come:

$$\gamma_k = Cov(Y_t, Y_{t-k}).$$

Risulta evidente la relazione esistente tra autocovarianza e autocorrelazione espressa nel seguente modo:

$$\begin{aligned} \gamma_k = \text{Corr}(Y_t, Y_{t-k}) &= Cov(Y_t, Y_{t-k}) / (\sqrt{Var(Y_t)}) \sqrt{Var(Y_{t-k})} \\ &= \frac{\gamma_k}{\sqrt{\sigma_y^2} \sqrt{\sigma_y^2}} \\ &= \frac{\gamma_k}{\sigma_y^2}. \end{aligned}$$

dove $\sigma_y^2 = Var(Y_t) = Cov(Y_t, Y_t) = \gamma_0$, si può scrivere più sinteticamente

$$\rho_k = \frac{\gamma_k}{\gamma_0}$$

Tale coefficiente viene definito globale in quanto tiene in considerazione delle variabili che intercorrono tra Y_t e Y_{t-k} . Ciò significa che risulterà diverso da zero anche qualora tra le due variabili Y_t e Y_{t-k} non esista alcuna relazione ma esista tra Y_t ed almeno una delle altre variabili intermedie.

Di seguito vengono riportate alcune delle proprietà dell'autocorrelazione globale:

1. $\rho_0 = 1$;
2. $\rho_k = \rho_{-k}$;
3. $-1 \leq \rho_k \leq 1$;
4. Data la trasformazione lineare di X_t di Y_t , definito come $X_t = a + bY_t$, le autocorrelazioni, sia di X_t , sia di Y_t , al generico ritardo k , sono identiche tra loro, ovvero:

$$\rho_k(X_t) = \rho_k(Y_t)$$

La funzione di autocorrelazione parziale al contrario è espressamente volta a valutare la relazione che intercorre tra due generiche variabili e può essere espressa nei seguenti termini:

$$\pi_k = \text{Corr}(Y_t, Y_{t-k} | Y_{t-1}, \dots, Y_{t-k+1}).$$

Tale formulazione presuppone che se tra le due variabili generiche esiste solo un legame indiretto, la funzione di autocorrelazione parziale risulterà nulla a differenza di quella globale.

3.8 MODELLI STATISTICI

3.8.1 WHITE NOSE: $\epsilon_t \sim WN(0, \sigma_\epsilon^2)$.

Con il termine "White Nose" viene indicata una serie storica ϵ_t con le seguenti caratteristiche:

1. Il valore atteso delle variabili ϵ_t è nullo;

$$E(\epsilon_t) = 0, \forall t;$$

2. La varianza delle variabili ϵ_t è finita e costante e dunque anch'essa non dipende da tempo;

$$\text{Var}(\epsilon_t) = \sigma_\epsilon^2 < \infty, \forall t;$$

3. La covarianza delle variabili ϵ_t e ϵ_{t-k} è nulla per ogni t e per ogni ritardo k ;

$$\text{Cov}(\epsilon_t, \epsilon_{t-k}) = E(\epsilon_t \epsilon_{t-k}) = 0, \forall t, \forall k \neq 0$$

In altre parole, il White Nose è volto alla rappresentazione di una serie storica le cui variabili non sono legate tra loro. Ciò significa non solo che quanto accaduto al tempo t non ha alcuna relazione con il passato, ma anche che quest'ultimo non avrà alcuna relazione con i tempi futuri.

L'indipendenza della variabile Y_t dalle sue osservazioni passate presuppone che non solo la funzione di autocorrelazione globale sia nulla, ma anche che risulta tale quella di autocorrelazione parziale. Inoltre, data la definizione di White Nose e quella di stazionarietà, una serie storica del tipo appena descritto, in quanto tale, sarà sempre stazionaria.

3.8.2 MODELLI AUTOREGRESSIVI AR(p)

Le serie storiche Y_t possono essere rappresentate tramite l'utilizzo del modello autoregressivo di ordine p , AR(p) dove con il termine p viene indicato il numero dei ritardi:

$$Y_t = \varphi_0 + \varphi_1 Y_{t-1} + \varphi_2 Y_{t-2} + \dots + \varphi_p Y_{t-p} + \epsilon_t$$

dove $\epsilon_t \sim \text{WN}(0, \sigma_\epsilon^2)$.

La variabile ϵ_t indica la componente errore che, nell'ambito delle serie temporali, può essere rappresentato da uno shock o da un'innovazione. Dalla formulazione sopra esposta si evince chiaramente che anche l'errore è importante e significativo per la determinazione di Y_t .

Ponendo $\varphi(L) = 1 - \varphi_1 L - \varphi_2 L^2 - \dots - \varphi_p L^p$, in cui L è l'operatore ritardo, il modello può essere anche espresso come:

$$\varphi(L)Y_t = \varphi_0 + \epsilon_t$$

Il modello è stazionario se la sua equazione caratteristica, ha la radice in valore assoluto superiore all'unità;

$$\varphi(L) = 0$$

e dunque:

$$1 - \varphi_1 L - \varphi_2 L^2 - \dots - \varphi_p L^p = 0$$

Il modello AR(p) stazionario può sempre essere iscritto come modello MA(∞), il quale verrà approfonditamente trattato in seguito.

Per quanto concerne la condizione di invertibilità, quest'ultima è sempre assicurata in quanto il modello AR(p) non è altro che l'espressione dei suoi ritardi p .

Il valore atteso di tale modello viene espresso come

$$E(Y_t) = \varphi_0 + \varphi_1 E(Y_{t-1}) + \varphi_2 E(Y_{t-2}) + E(\epsilon_t)$$

meglio descritto

$$\mu = \varphi_0 + \varphi_1 \mu + \varphi_p \mu$$

il quale diviene

$$\mu = \frac{\varphi_0}{1 - \varphi_1 - \dots - \varphi_p}$$

Se la media è nulla, anche il coefficiente φ_0 sarà tale. Ricavando $\varphi_0 = (1 - \varphi_1 - \varphi_2)\mu$, il modello AR(p) può scriversi come

$$Y_t - \mu = \varphi_1(Y_{t-1} - \mu) + \dots + \varphi_p(Y_{t-p} - \mu) + \epsilon_t$$

anche espresso

$$Y_t = \mu + \varphi_1(Y_{t-1} - \mu) + \dots + \varphi_p(Y_{t-p} - \mu) + \epsilon_t$$

La varianza per una serie storica stazionaria è data da:

$$Var(Y_t) = \varphi_1^2 Var(Y_{t-1}) + \dots + \varphi_p^2 Var(Y_{t-p}) + \sigma_\epsilon^2 + 2 \sum_{i=1}^{p-1} \sum_{j=i+1}^p \varphi_i \varphi_j Cov(Y_{t-i}, Y_{t-j})$$

la quale diventa:

$$\sigma_y^2 = \varphi_1^2 \sigma_y^2 + \dots + \varphi_p^2 \sigma_y^2 + \sigma_\epsilon^2 + 2 \sum_{i=1}^{p-1} \sum_{j=i+1}^p \varphi_i \varphi_j Cov(Y_{t-i}, Y_{t-j})$$

La funzione di autocorrelazione globale mentre, è la seguente:

$$\rho_k = \varphi_1 \rho_{k-1} + \varphi_2 \rho_{k-2} + \dots + \varphi_p \rho_{k-p}$$

Man mano che i ritardi aumentano, l'autocorrelazione tende a zero.

Di contro, la funzione di autocorrelazione parziale è data da:

$$\begin{aligned} \pi_k &\neq 0 & k &= 1, 2, \dots, p \\ \pi_k &= 0 & k &> p \end{aligned}$$

Il valore atteso e la varianza al tempo $t-1$ sono dati da:

$$\begin{aligned} E(Y_t | I_{t-1}) &= E(\varphi_0 + \varphi_1 Y_{t-1} + \dots + \varphi_p Y_{t-p} + \epsilon_t | I_{t-1}) \\ &= \varphi_0 + \varphi_1 Y_{t-1} + \dots + \varphi_p Y_{t-p} \end{aligned}$$

$$\begin{aligned} Var(Y_t | I_{t-1}) &= Var(\varphi_0 + \varphi_1 Y_{t-1} + \dots + \varphi_p Y_{t-p} + \epsilon_t | I_{t-1}) \\ &= \sigma_\epsilon^2 \end{aligned}$$

3.8.3 MODELLI MOVING AVERAGE MA(q)

Le serie storiche Y_t vengono definite del tipo MA(q) se

$$Y_t = \mu + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q}$$

Anche in questo caso, come nel modello precedentemente analizzato, l'errore è $\epsilon_t \sim \text{WN}(0, \sigma_\epsilon^2)$.

Ponendo $\theta(L) = 1 + \vartheta_1 L + \dots + \vartheta_q L^q$, dove L è rappresentativo dell'operatore ritardo, il modello può essere ulteriormente scritto come

$$Y_t = \mu + \vartheta(L)\epsilon_t$$

Se per la condizione di stazionarietà possiamo affermare che quest'ultima sia sempre verificata in quanto il modello MA è costruito per essere un modello di media di un processo stazionario, per l'invertibilità è necessario considerare la seguente equazione caratteristica:

$$1 + \vartheta_1 L + \dots + \vartheta_q L^q = 0,$$

e verificare che le q radici dell'equazione siano tutte maggiori di 1 in valore assoluto.

La caratteristica del modello MA(q) è che quest'ultimo può essere anche espresso come modello AR(∞).

Infatti, il suo valore atteso è dato da

$$E(Y_t) = E(\mu + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q}) = \mu$$

La sua varianza è data da

$$\begin{aligned} \text{Var}(Y_t) &= \text{Var}(\mu + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q}) = \sigma_y^2 \\ &= \sigma_\epsilon^2 (1 + \vartheta_1^2 + \dots + \vartheta_q^2) \end{aligned}$$

Per quanto concerne le funzioni di autocorrelazione globale e parziale, se per la prima è unicamente necessario sottolineare la diversità da zero per $k \leq q$ mentre si annulla per $k > q$, la funzione di autocorrelazione parziale tende a zero all'aumentare dei ritardi considerati ma non si annulla mai.

Il valore atteso e la variazione considerati al tempo $t-1$ sono rispettivamente:

$$E(Y_t | I_{t-1}) = E(\mu + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q} | I_{t-1}) = \mu + \vartheta_1 \hat{\epsilon}_{t-1} + \dots + \vartheta_q \hat{\epsilon}_{t-q}$$

$$\text{Var}(Y_t | I_{t-1}) = \text{Var}(\mu + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q} | I_{t-1}) = \sigma_\epsilon^2$$

3.8.4 MODELLO AUTOREGRESSIVE MOVING AVERAGE ARMA (p, q)

La serie storica Y_t segue il modello ARMA(p, q) se

$$Y_t = \varphi_0 + \varphi_1 Y_{t-1} + \dots + \varphi_p Y_{t-p} + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q}$$

dove $\epsilon_t \sim \text{WN}(0, \sigma_\epsilon^2)$.

Tale serie storica può essere anche scritta nel seguente modo:

$$\varphi(L)Y_t = \varphi_0 + \varphi(L)\epsilon_t$$

dove $\varphi(L) = 1 - \varphi_1 L - \dots - \varphi_p L^p$ e $\theta(L) = 1 + \vartheta_1 L + \dots + \vartheta_q L^q$.

Per quanto riguarda la condizione di stazionarietà, valgono le condizioni precedentemente viste per il modello AR(p), per quelle dell'invertibilità invece, quelle già viste per il modello MA(q).

Se si estendono i concetti precedente espressi per i modelli già analizzati, il modello ARMA(p, q) è descritto in:

$$Y_t = \mu + \varphi_1(Y_{t-1} - \mu) + \dots + \varphi_p(Y_{t-p} - \mu) + \epsilon_t + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q}$$

Il valore atteso e la varianza condizionati sono dati da:

$$E(Y_t | I_{t-1}) = \varphi_0 + \varphi_1 y_{t-1} + \dots + \varphi_p y_{t-p} + \vartheta_1 \epsilon_{t-1} + \dots + \vartheta_q \epsilon_{t-q}$$

$$\text{Var}(Y_t | I_{t-1}) = \sigma_\epsilon^2$$

3.9 PROCEDURA BOX-JENKINS

La procedura di Box-Jenkins è un approccio statistico utilizzato per identificare, stimare e prevedere i modelli delle serie storiche. Tale procedura si compone di tre principali fasi: identificazione, stima e validazione del modello.

3.9.1 IDENTIFICAZIONE

Durante la fase di identificazione si cerca di identificare il modello appropriato per la serie storica attraverso l'analisi della funzione di autocorrelazione globale e parziale.

Per poter stimare la funzione di autocorrelazione globale, è necessario considerare una serie storica $y_t, t = 1, 2, \dots, T$ e la stima di tale coefficiente è data da

$$\hat{\rho}_k = \frac{\hat{Y}_k}{\hat{Y}_0}$$

nello specifico

$$\hat{\rho}_k = \frac{\sum_{t=k+1}^T (y_t - \bar{y})(y_{t-k} - \bar{y})}{\sum_{t=1}^T (y_t - \bar{y})^2}$$

Se le variabili prese in considerazione Y_t, Y_{t-k} con $k \neq 0$ fossero incorrelate, sarebbe possibile dimostrare

$$R_k \rightarrow N\left(0; \frac{1}{T}\right)$$

Di contro, per poter stimare il coefficiente di autocorrelazione parziale si fa ricorso al modello regressione in quanto il coefficiente π_k indica la relazione che intercorre tra due generiche variabili intermedie e dunque

$$Y_t = \varphi_{0k} + \varphi_{1k}Y_{t-1} + \varphi_{2k}Y_{t-2} + \dots + \varphi_{kk}Y_{t-k} + a_t$$

Il coefficiente φ_{kk} altro non è che il coefficiente di autocorrelazione parziale indicante la relazione che intercorre tra Y_t e Y_{t-k} .

Ciò significa che il coefficiente al ritardo k può essere anche stimato attraverso una regressione di Y_t su k ritardi e considerando il coefficiente stimato della variabile Y_{t-k} .

Posto ciò, otterremo

$$\hat{\pi}_k = \hat{\varphi}_{kk}$$

Se tra le variabili Y_t e Y_{t-k} non esistesse alcun legame, e dunque fossero incorrelate, con $k \neq 0$, lo stimatore $\hat{\pi}_k$ del tipo $P_k \rightarrow N(0; \frac{1}{T})$.

Stimate le funzioni di autocorrelazione della serie storica, al fine dell'identificazione del modello da preferire per quest'ultima, è necessario un confronto con i coefficienti di autocorrelazione stimati con coefficienti teorici.

In particolare, è necessario effettuare un test d'ipotesi in cui le due ipotesi prese in considerazione sono le seguenti:

$$H_0 : \rho_k = 0$$

$$H_1 : \rho_k \neq 0$$

Si accetta l'ipotesi nulla e dunque H_0 con un livello di significatività α se

$$-z_{\alpha/2} < \hat{\rho}_k - \frac{0}{\sqrt{\frac{1}{T}}} < z_{\alpha/2}$$

dove $z_{\alpha/2}$ è il percentile della variabile normale standard Z che

$$P\left(Z > \frac{z_{\alpha}}{2}\right) = \frac{\alpha}{2} \quad \text{ovvero} \quad \frac{-z_{\alpha}}{2} < \hat{\rho}_k < \frac{-z_{\alpha}}{2}$$

Essendo la distribuzione rappresentativa di ogni ritardo, il risultato è valido per ogni k e dunque ritardo. Ciò significa che i valori critici che dividono la ragione di accettazione da quella di rifiuta, fissata tramite il livello di significatività α , rimangono immutati per ogni k .

Il correlogramma globale è un utile strumento per l'analisi delle storie storiche. Di fatto, il correlogramma permette di rappresentare le autocorrelazioni $\hat{\rho}_k$ stimate, permette di tracciare due linee orizzontali in corrispondenza di $-z_{\alpha/2}$ e $z_{\alpha/2}$, volte a formare una banda di confidenza. La regione della banda di confidenza varia a seconda del livello di significatività utilizzato e dunque di α .

Per quanto concerne i coefficienti di autocorrelazione parziale, valgono le stesse ipotesi delineate per l'autocorrelazione globale e dunque si andranno a considerare le due ipotesi di seguito descritte

$$H_0 : \pi_k = 0$$

$$H_1 : \pi_k \neq 0$$

e si giunge al risultato di accettazione dell'ipotesi nulla se

$$\frac{-z_{\alpha}}{2} < \hat{\pi}_k < \frac{-z_{\alpha}}{2}$$

3.9.2 STIMA

Se attraverso la fase di identificazione è possibile effettuare una buona rappresentazione dei dati, secondariamente sarà necessario effettuare una stima dei parametri. Questi ultimi sono $p+q+2$ se il modello d'analisi è del tipo ARMA (p,q) , dove 2 altro non è che la costante. È necessario dunque stimare i p parametri della componente autoregressiva, i q parametri della parte "moving average" e la varianza dell'errore ovvero σ_{ϵ}^2 .

Il metodo di stima maggiormente utilizzato viene definito come metodo della massima verosimiglianza. La funzione di verosimiglianza viene utilizzata per descrivere quanto un dataset si adatti al modello.

In altre parole, tale metodo consente di trovare i valori dei parametri del modello che massimizzano la verosimiglianza dei dati osservati. La funzione di verosimiglianza, indicata con $L(\mu; y_1, y_2, y_3, y_4)$ è data da

$$L(\mu; y_1, y_2, y_3, y_4) = f(y_1)f(y_2)f(y_3)f(y_4)$$

Tale funzione sta ad indicare che, mentre i parametri y_1, y_2, y_3, y_4 dell'equazione sono noti, μ ovvero la media rappresenta l'incognita.

Genericamente, in un'analisi temporale, le varie osservazioni non sono mai indipendenti per cui la funzione di verosimiglianza è anche data dalla sua funzione di densità congiunta che, presupposto che le variabili siano tra loro non indipendenti, non è uguale al prodotto delle funzioni di densità.

$$L(\beta; y) = f(y_1, y_2, \dots, y_t)$$

Dalla scomposizione di $f(y_1, y_2, \dots, y_t)$, si ottiene $f(y_1, y_2, \dots, y_T) = f(y_1)f(y_2|y_1)f(y_3|y_2, y_1) \dots f(y_T|y_{T-1}, \dots, y_1)$, da cui

$$L(\beta; y) = f(y_1) \prod_{t=2}^T f(y_t|y_{t-1}).$$

Dove $f(y_1)$ rappresenta la funzione di densità non condizionata mentre $f(y_t|y_{t-1})$ è la funzione di densità condizionata. È possibile la riscrittura di tale equazione attraverso il logaritmo naturale, definita funzione di log-verosimiglianza, maggiormente utilizzato per fini computazionali:

$$l(\beta; y) = \log f(y_1) + \sum_{t=2}^T \log f(y_t|y_{t-1}).$$

Maggiore sarà il numero delle T osservazioni, maggiore sarà la probabilità che la funzione di verosimiglianza esatta e quella di log-verosimiglianza coincidano.

Ottenuto il coefficiente β grazie l'utilizzo di tale funzione, è necessario effettuare un test d'ipotesi dove le ipotesi considerate sono

$$H_0 : \beta = 0$$

$$H_1 : \beta \neq 0$$

L'ipotesi nulla verrà rifiutata se

$$\left| \frac{\widehat{\beta}}{\sqrt{\widehat{Var}(B)}} > t_{T-r, \frac{\alpha}{2}} \right|$$

Dove r è il numero dei parametri del modello, β un qualsiasi parametro, $\widehat{\beta}$ la sua stima di massima verosimiglianza e B è il suo stimatore.

La maggior parte dei software, oltre che consentire una verifica attraverso il test dell'ipotesi, consentono anche di effettuare un test bilaterale, nonché il *p-value*, che è dato da

$$2P\left(t_{T-r} > \left| \frac{\beta}{\sqrt{\widehat{Var}(B)}} \right| \right)$$

Anche in questo caso, viene fissato un α livello di significatività e, successivamente, l'ipotesi nulla H_0 viene rifiutata nel caso in cui

$$p - value < \alpha$$

3.9.3 LA VERIFICA

La fase conclusiva della procedura Box-Jenkins prevede una verifica finale volta a determinare se il modello già stimato è effettivamente appropriato per la rappresentazione dei dati.

Se il modello si adatta bene al dataset a disposizione, allora risulterà un'evidenza a favore di $\epsilon_t \sim \text{WN}$. Per verificare questa ipotesi vengono utilizzate le stime dei residui ovvero ϵ_t .

È possibile effettuare una prima verifica a partire dal correlogramma: l'esistenza di legami fra le variabili viene verificata in base alla posizione all'interno del correlogramma dei coefficienti di autocorrelazione globali o parziali ovvero se questi ultimi ricadono o no all'interno della regione di accettazione. Di seguito, viene ritenuta accettabile l'ipotesi che $\epsilon_t \sim \text{WN}$ e il modello stimato viene confermato.

Inoltre, è anche possibile la verifica tramite il test Ljung-Box in cui le due ipotesi sono

$$H_0 = \rho_1 = \rho_2 = \dots = 0$$

L'ipotesi alternativa mentre, richiede che almeno uno dei coefficienti, e dunque non tutti, sia diverso da zero.

3.10 METODI ALTERNATIVI

Talvolta può capitare che la procedura di Box-Jenkins non sia sufficiente nella determinazione della scelta del modello. In tal caso, è possibile ricorrere alla determinazione dell'AIC e del BIC.

L'AIC, anche noto come Akaike Information Criterion, è un criterio di selezione del modello che si basa sull'idea di trovare quello che massimizza la probabilità dei dati ma, al tempo stesso, ha una formulazione tale da far preferire il modello con il minor numero di parametri. Il modello con un valore minore di AIC è considerato il migliore. L'AIC è dato da:

$$AIC = -2l + 2r$$

In cui l è il valore rappresentativo della log-verosimiglianza e r è il numero dei parametri presenti nel modello.

Il BIC, ovvero il Bayesian Information Criterion, permette la scelta del modello migliore in base al coefficiente che ne risulta dal calcolo. Anche in questo caso, come già visto per l'AIC, verrà scelto il modello con coefficiente minore. Tale indice tuttavia, permette la scelta di un modello con un maggior numero di parametri solo se quest'ultimi migliorano notevolmente la verisimiglianza. La sua formulazione è data da:

$$BIC = -2l + r \log T$$

3.11 LE PREVISIONI

Le serie storiche, oltre che poter essere utilizzate per la descrizione o spiegazione di un fenomeno d'interesse, possono essere ulteriormente impiegate per effettuare delle previsioni. Le previsioni in serie temporali, dunque, sono una tecnica a cui si ricorre per prevedere il futuro della serie, sulla base dei dati storici di quest'ultima. In altre parole, avendo a disposizione una serie storica per i tempi $t = 1, 2, \dots, T$ si intende dare una previsione del fenomeno d'interesse nei tempi successivi $T + 1, T + 2, \dots$.

È possibile da distinzione tra due tipologie di previsione: quella puntuale e quella per intervallo.

La previsione puntuale, che intende prevedere il fenomeno al tempo successivo $T + 1$, viene effettuata utilizzando il valore atteso di $T + 1$ condizionato a T , ovvero I_t . In altre parole, la previsione è unicamente basata sulla conoscenza della serie storica al tempo T .

$$Y_t(1) = E(Y_{t+1} | I_t)$$

Tale tipologia di previsione permette di minimizzare l'errore quadratico medio, EQMP, che misura l'accuratezza del modello in base ai dati osservati. In pratica, l'errore quadratico medio calcola la media delle differenze quadrate tra i valori previsti dal modello e i valori osservati per ogni punto della serie temporale.

L'EQMP è dunque dato da

$$EQMP = E(Y_{t+1} - Y_t(1))^2$$

L'EQMP, inoltre, è una funzione di perdita simmetrica. Ciò significa che oltre a fornire un'informazione circa l'errore associato ad una previsione errata, assume lo stesso valore, a parità di valore assoluto, indipendentemente dal segno. Si differenzia dunque da una funzione di perdita asimmetrica che, contrariamente, assume un determinato valore in base al segno dell'errore a parità di valore assoluto.

Nel paragrafo è stata esposta una previsione di Y_{t+1} e dunque una previsione del fenomeno d'interesse, immediatamente nell'istante successivo. Qualora si volesse effettuare una previsione di Y_{t+h} , e dunque non la previsione del solo istante successivo, la sua formulazione sarà la seguente:

$$y_t(h) = E(Y_{t+h} | I_t)$$

3.11.1 PREVISIONI PER MODELLI AR

Per tale tipologia di modelli, le previsioni di 1, 2 e h periodi avanti solo date da:

$$\begin{aligned}y_t(1) &= E(Y_{t+1}|I_t) = E(\varphi_0 + \varphi_1 Y_t + \dots + \varphi_p Y_{t+1-p} + \epsilon_{t+1}|I_t) \\ &= \varphi_0 + \varphi_1 Y_t + \dots + \varphi_p Y_{t+1-p}\end{aligned}$$

$$\begin{aligned}y_t(2) &= E(Y_{t+2}|I_t) = E(\varphi_0 + \varphi_1 Y_t + \dots + \varphi_p Y_{t+2-p} + \epsilon_{t+2}|I_t) \\ &= \varphi_0 + \varphi_1 Y_t(1) + \dots + \varphi_p Y_{t+2-p}\end{aligned}$$

La previsione di Y_t di h periodi avanti, con $h \leq p$ è data da

$$\begin{aligned}y_t(h) &= E(Y_{t+h}|I_t) = E(\varphi_0 + \varphi_1 Y_{t+h-1} + \dots + \varphi_p Y_{t+h-p} + \epsilon_{t+h}|I_t) \\ &= \varphi_0 + \varphi_1 Y_t(h-1) + \dots + \varphi_p Y_{t+h-p}\end{aligned}$$

La previsione di Y_t di h periodi avanti, con $h > p$ è data da:

$$\begin{aligned}y_t(h) &= E(Y_{t+h}|I_t) = E(\varphi_0 + \varphi_1 Y_{t+h-1} + \dots + \varphi_p Y_{t+h-p} + \epsilon_{t+h}|I_t) \\ &= \varphi_0 + \varphi_1 Y_t(h-1) + \dots + \varphi_p Y_t(h-p)\end{aligned}$$

3.11.2 PREVISIONI PER MODELLI MA

Per il modello MA(q), le previsioni 1, 2 e h periodi avanti sono date da:

$$\begin{aligned}y_t(1) &= E(Y_{t+1}|I_t) = E(\mu + \epsilon_{t+1} + \vartheta_1 \epsilon_t + \dots + \vartheta_q \epsilon_{t+1-q}|I_t) \\ &= \mu + \vartheta_1 (y_t - y_{t-1}(1)) + \dots + \vartheta_q (y_{t+1-q} - y_{t-q}(1))\end{aligned}$$

$$\begin{aligned}y_t(2) &= E(Y_{t+2}|I_t) = E(\mu + \epsilon_{t+2} + \vartheta_1 \epsilon_{t+1} + \dots + \vartheta_q \epsilon_{t+2-q}|I_t) \\ &= \mu + \vartheta_2 (y_t - y_{t-1}(1)) + \dots + \vartheta_q (y_{t+2-q} - y_{t+1-q}(1))\end{aligned}$$

Le previsioni del modello h periodi avanti, con $h \leq p$

$$\begin{aligned}
y_t(h) &= E(Y_{t+h}|I_t) = E(\mu + \epsilon_{t+h} + \vartheta_1\epsilon_{t+h} + \dots + \vartheta_q\epsilon_{t+h-q}|I_t) \\
&= \mu + \vartheta_h(y_t - y_{t-1}(1)) + \dots + \vartheta_q(y_{t+h-q} - y_{t+h-q-1}(1))
\end{aligned}$$

Di contro, le previsioni con $h > p$

$$\begin{aligned}
y_t(h) &= E(Y_{t+h}|I_t) = E(\mu + \epsilon_{t+h} + \vartheta_1\epsilon_{t+h} + \dots + \vartheta_q\epsilon_{t+h-q}|I_t) \\
&= \mu
\end{aligned}$$

3.11.3 PREVISIONI PER MODELLI ARMA

Vista la previsione prima per il modello AR(p), poi per il modello MA(q), risulta facile desumere che al fine di effettuare una previsione per modelli ARMA, debbano essere applicate le regole di previsione di entrambi i modelli.

3.11.4 ERRORE DI PREVISIONE

L'errore di previsione anche noto come "MFE" ovvero "Mean Forecast Error", è una metrica utilizzata per valutare l'accuratezza della previsione effettuata. Di fatto il suo calcolo altro non è che la differenza tra il valore futuro Y_{t+h} e il previsore $Y_t(h)$

$$e_t(h) = Y_{t+h} - Y_t(h)$$

In generale dunque

$$\begin{aligned}
e_t(h) &= \mu + \epsilon_{t+h} + \psi_1\epsilon_{t+h-1} + \psi_2\epsilon_{t+h-2} + \dots - (\mu + \psi_h\epsilon_t + \psi_{h-1}\epsilon_{t-1} + \dots) \\
&= \epsilon_{t+h} + \psi_1\epsilon_{t+h-1} + \dots + \psi_{h-1}\epsilon_{t-1}
\end{aligned}$$

Il valore atteso dell'errore di previsione, dunque, ha sempre valore atteso nullo e la sua varianza diminuisce all'aumentare di h e dunque in base a quanto aumenti il periodo temporale preso in considerazione.

3.12 MODELLO ARIMA

Nella realtà, molte serie storiche non possiedono il requisito già precedentemente esaminato della stazionarietà. Come già detto, quest'ultimo presuppone che media, varianza e altri momenti statistici rimangano costanti nel tempo. Nella realtà ciò non avviene.

Essendo la stazionarietà un requisito fondamentale delle serie storiche, al fine della loro analisi, è dunque necessario trasformare la serie storica affinché quest'ultima sia stazionaria. Le forme maggiormente diffuse di non stazionarietà riguardano la media, e dunque la disuguaglianza dei valori medi delle variabili casuali, oppure la varianza ovvero la disuguaglianza delle varianze delle variabili casuali.

Al fine di poter trasformare una serie storica non stazionaria in stazionaria, è necessario effettuare l'operazione di differenziazione, ovvero

$$Y_t = Y_{t-1} + \epsilon_t$$

Ne segue che

$$\epsilon_t = Y_t - Y_{t-1}$$

e dunque la serie diviene stazionaria se ϵ_t è un White Noise.

Dopo aver effettuato l'operazione di differenziazione è necessario verificare se la serie così ottenuta è effettivamente divenuta una serie temporale stazionaria. Contrariamente, sarà necessario effettuare altre operazioni di differenziazione al fine di poter rendere la serie stessa stazionaria. In base al numero di operazioni effettuate, la serie storica verrà definita integrata di ordine 1 e dunque I(1) se è stata effettuata un'unica operazione, integrata di ordine d se sono state effettuate d operazioni. I modelli ARIMA, dunque, sono analoghi e godono delle stesse proprietà dei modelli ARMA con la sola differenza che negli ARIMA vengono effettuate delle operazioni per rendere le serie temporali stazionarie.

3.13 VERIFICA DELLA STAZIONARIETA'

Alternativamente l'analisi dei correlogrammi per poter stabilire se una serie storica è stazionaria o meno, possono essere effettuati due ulteriori test. Il primo, definito come test di Dickey-Fuller prevede un test per poter verificare l'ipotesi nulla di non stazionarietà contro l'ipotesi alternativa di stazionarietà.

I valori critici al fine di poter effettuare tale verifica, tuttavia, non provengono da una distribuzione nota, ma sono stati appositamente ideati per tale verifica. Come si vedrà dalle due ipotesi prese in considerazione, il test può anche essere definito "della radice unitaria" in quanto viene verificata la presenza di radici unitarie all'interno della serie. Se sono presenti radici unitarie, il modello verrà definito non stazionario. Le due ipotesi considerate sono:

$$H_0: \varphi_1 = 1$$

$$H_1: \varphi_1 < 1$$

Il passo successivo è la stima del parametro φ_1

$$\hat{\varphi}_1 = \sum_{t=2}^T \frac{y_t y_{t-1}}{\sum_{t=2}^T y_{t-1}^2}$$

E la statistica test è

$$\tau(1) = \frac{\hat{\varphi}_1 - 1}{se(\hat{\varphi}_1)}$$

Sulla base del valore ottenuto e dei valori critici, si andrà a rifiutare o meno l'ipotesi nulla.

Oltre il test di Dickey-Fuller, è possibile verificare la proprietà statistica della stazionarietà anche con il Dickey-Fuller aumentato, meglio definito come Augmented Dickey-Fuller.

La principale differenza tra i due è che nella versione aumentata vengono presi in considerazione maggiori più fattori che possono influenzare la stazionarietà della serie storica e dunque la sua espressione è

$$\Delta Y_t = \varphi_0 + \beta_t + (\varphi_1 - 1)Y_{t-1} + \sum_{j=1}^p a_j \Delta Y_{t-j} + \epsilon_t$$

Anche in questo caso, le due ipotesi prese in considerazione per la verifica di stazionarietà sono

$$H_0: \varphi_1 = 1$$

$$H_1: \varphi_1 < 1$$

3.14 OUTLIERS E LEVEL CHANGES

Sia “outliers”, sia “level changes” rappresentano due tipologie di deviazioni significative nella serie storica che possono influenzare la sua analisi e la previsione.

Gli outliers sono valori estremi o anomali che si discostano significativamente dal resto dei dati della serie storica. Questi valori possono essere causati da errori di rilevazione o da eventi eccezionali che hanno influenzato il processo in modo significativo. Gli outliers possono influenzare la media e la varianza della serie storica, e possono rendere più difficile l'identificazione di tendenze e pattern nei dati. Pertanto, gli outliers devono essere individuati e gestiti in modo adeguato a evitare che influenzino negativamente l'analisi e la previsione. I level changes, o cambi di livello, sono variazioni significative nella media o nella varianza della serie storica che si verificano in un determinato punto nel tempo. Queste variazioni possono essere causate da fattori esterni o interni al processo, come cambiamenti nelle condizioni economiche o tecnologiche, oppure da

cambiamenti nella strategia o nel management dell'azienda. I cambi di livello possono influenzare la stazionarietà della serie storica e la validità dei modelli utilizzati per l'analisi e la previsione. Pertanto, è importante identificare e gestire i cambi di livello in modo adeguato per evitare che influenzino negativamente l'analisi e la previsione. In presenza di outliers oppure level changes, la serie storica osservata è disturbata e, dunque, essa risulterà inosservabile. Per rappresentare una serie storica contaminata a causa della presenza di una delle due tipologie di deviazioni si usa la scrittura X_t .

La relazione esistente tra la serie che presenta anomalie e la serie reale è

$$X_t = f(t) + Y_t$$

Dove $f(t)$ è una funzione parametrica²⁵ e deterministica²⁶.

²⁵ Parametrica: la funzione dipende da uno o più parametri.

²⁶ Deterministica: la funzione descrive la relazione esistente tra le variabili delle serie in modo preciso, senza prendere in considerazione fattori casuali.

CAPITOLO QUARTO

ANALISI IN SERIE STORICHE DEI PLAY TO EARN

Il fenomeno dei play to earn lascia sempre meglio spazio ai videogames tradizionali in quanto, come già visto, è possibile ricavarne un guadagno reale. Per poter comprendere appieno la diffusione degli NFT games, sono stati analizzati sei videogames nonché i tre di maggior successo e i tre che hanno avuto un impatto inferiore sul mercato. Nello specifico, per ciascun game analizzato, le variabili d'interesse sono le seguenti: UAW²⁷, numero delle transazioni e il valore di quest'ultimo espresso in dollari. Il periodo preso in considerazione va dal 19 gennaio 2023 sino al 19 aprile 2023.

4.1 AXIE INFINITY

Nato nel 2017 dall'idea della società vietnamita Sky Mavis, ad oggi è uno dei giochi più celebri del panorama dei play to earn. Axie Infinity, lanciato nel 2018, prevede la creazione e la raccolta di creature digitali denominate "Axie", utilizzate per il combattimento con altri giocatori presenti all'interno della piattaforma. Gli Axies sono collezionabili e possiedono caratteristiche uniche come abilità di combattimento, colori e forme. I giocatori possono acquisire Axies con l'acquisto oppure coltivando uova, incubate all'interno del game. All'interno del gioco, inoltre, sono previste due tipologie di token: Axie Infinity Shards (AXS) e Small Love Potion (SLP). Il primo, AXS, è un token di governance che consente ai giocatori non solo di votare circa le decisioni del gioco, i quali, grazie la loro partecipazione, potranno anche ricevere delle ricompense per la partecipazione attiva all'interno del game. Questo token, inoltre, è anche utilizzato per l'acquisto di Axies ed altri oggetti all'interno del gioco. Il secondo token invece, ovvero SLP, viene utilizzato come forma di ricompensa per i giocatori che partecipano ai combattimenti tra Axies. Questi ultimi inoltre, vengono anche utilizzati dai gamers per potenziare i loro Axies, i quali, divenuti più forti, potranno essere venduti ad un prezzo maggiore sul mercato.

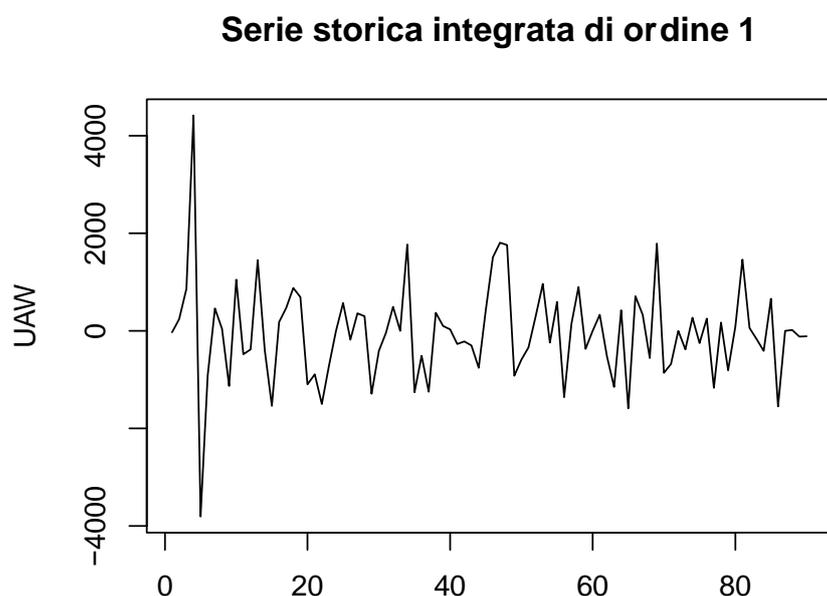
4.1.1 ANALISI IN SERIE STORICHE UAW

Nel seguente grafico viene rappresentata la serie storica integrata di ordine 1. Tale serie storica non è stazionaria dunque, al fine di rendere quest'ultima stazionaria per poter procedere con la sua analisi, è

²⁷ UAW: numero di portafogli attivi univoci (UAW) che interagiscono o eseguono una transazione con i contratti intelligenti di un DApp.

necessario effettuare un'operazione d'integrazione. Sull'asse x è riportato il numero delle osservazioni, sulla
asse y i valori corrispondenti a questi ultimi.

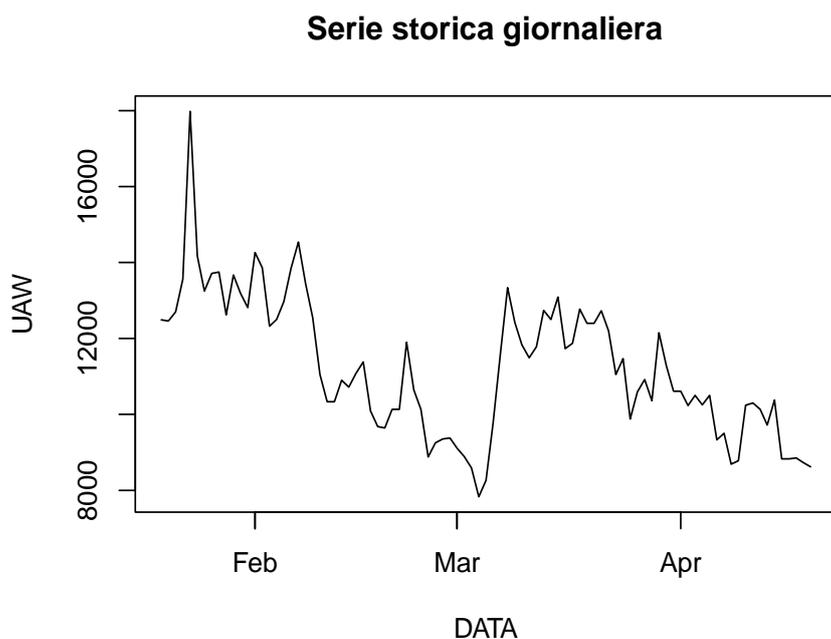
Figura 4.1.1, serie storica integrata di ordine 1.



Fonte: elaborazione personale.

Nel seguente grafico, viene indicata la serie storica la cui variabile d'interesse è rappresentata dal UAW.
Sull'asse delle ascisse è riportato il periodo temporale, sull'asse delle ordinate il numero dei portafogli attivi.

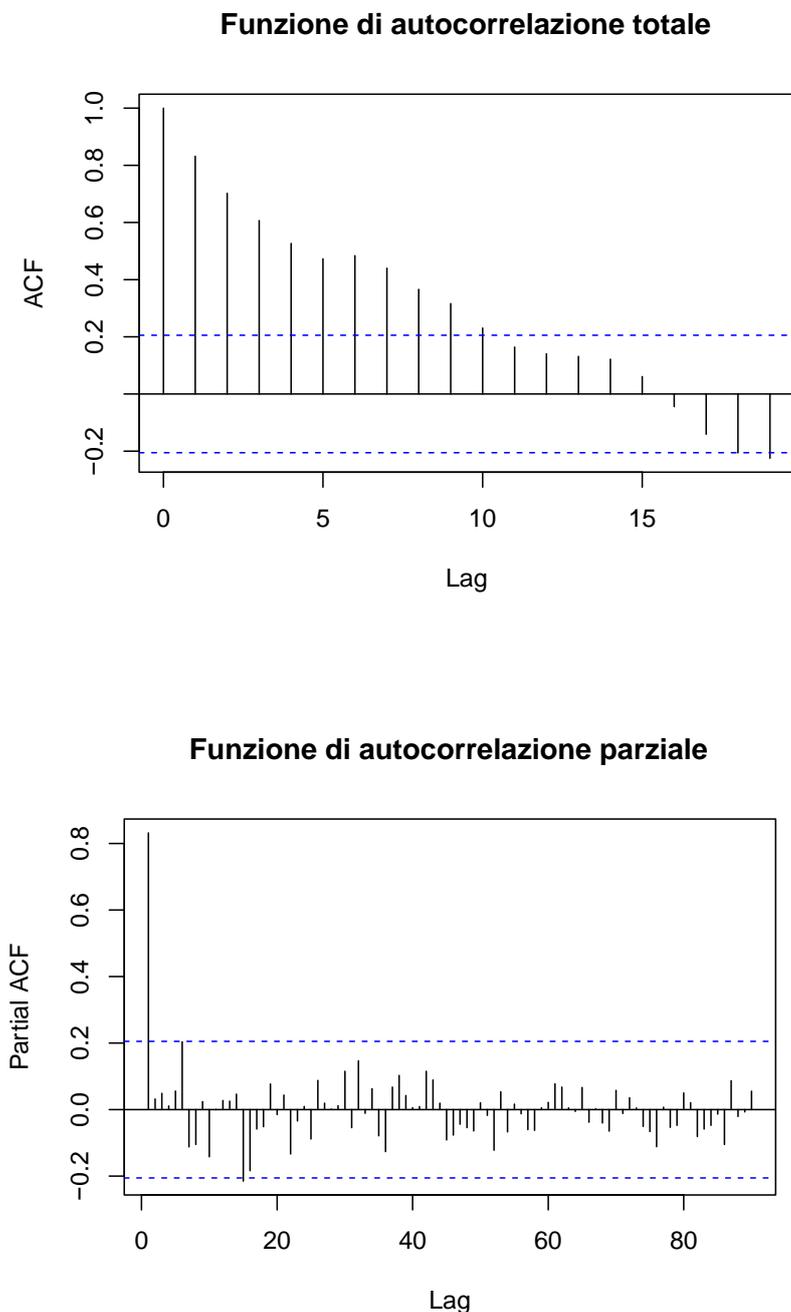
Figura 4.1.2, serie storica giornaliera UAW.



Fonte: elaborazione personale.

Entrambe le funzioni di autocorrelazioni sono presentate di seguito:

Figura 4.1.3, correlogramma di autocorrelazione totale e parziale.



Fonte: elaborazione personale.

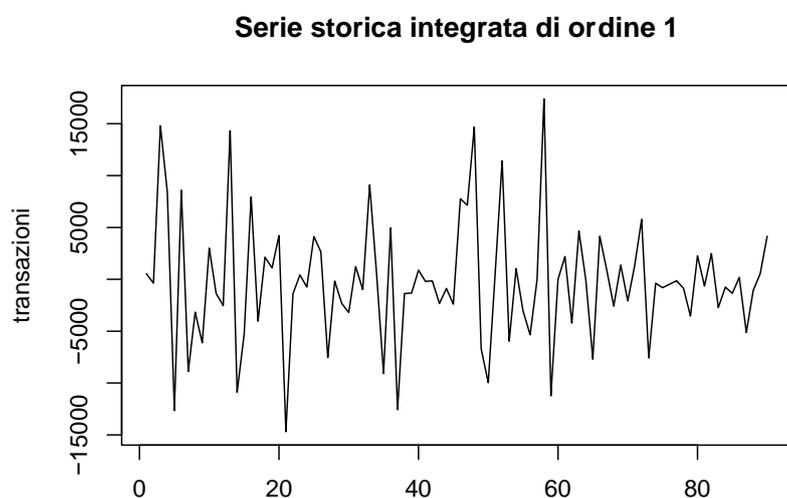
Tramite l'utilizzo di una specifica funzione su R-studio, è stato possibile individuare il modello ARIMA che più si adatta ai dati. Il modello definito è ARIMA (0,1,0). Ciò indica che per la costruzione del modello, che tuttavia non presenta né ritardi e né media mobile, è stata effettuata una sola operazione di differenziazione per rendere la serie stazionaria. Dato che il modello stimato non include alcun termine di regressione, coefficiente ed errore standard risultano essere pari a 0. Il modello sottostante può essere definito "random walk", ed è il più tipo tra i modelli non stazionari. Dall'analisi, il BIC risulta essere pari a 1504.72, l'AIC

1502,22 ed il p-value $9.775226e-74$. Essendo un random walk, nonostante sia possibile effettuare una previsione, quest'ultima sarà basata unicamente sull'ultimo valore della serie storica e dunque risulta essere pari a 8620.

4.1.2 ANALISI IN SERIE STORICHE NUMERO DELLE TRANSAZIONI

Nel seguente grafico è riportata la serie storica integrata di ordine 1 per la quale è stata eseguita un'operazione di differenziazione al fine di renderla stazionaria. Sull'asse delle ordinate è riportato il numero delle osservazioni, sull'asse delle ordinate il numero delle transazioni.

Figura 4.1.4, serie storica integrata di ordine 1.

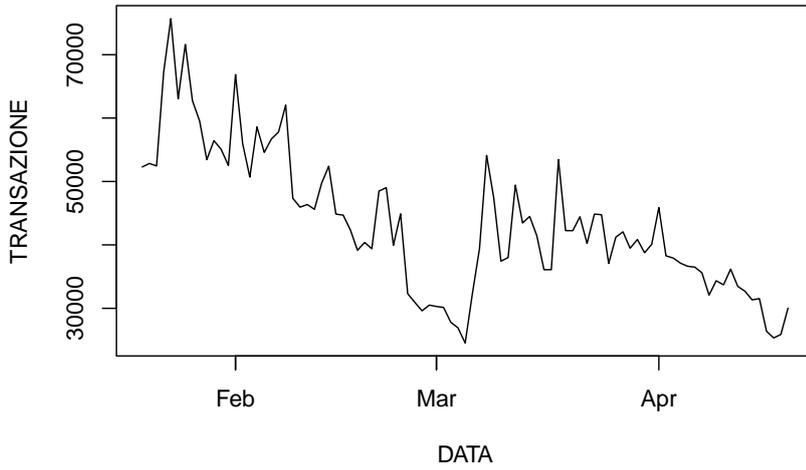


Fonte: elaborazione personale.

Il grafico che segue riporta la serie storica del numero delle transazioni. Sull'asse x viene indicato il periodo temporale considerato, sull'asse y il numero delle transazioni.

Figura 4.1.5, serie storica giornaliera numero transazioni.

Serie storica giornaliera

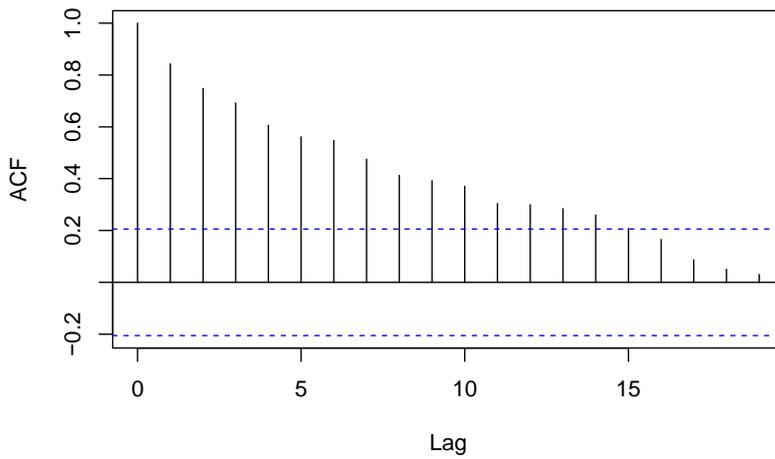


Fonte: elaborazione personale.

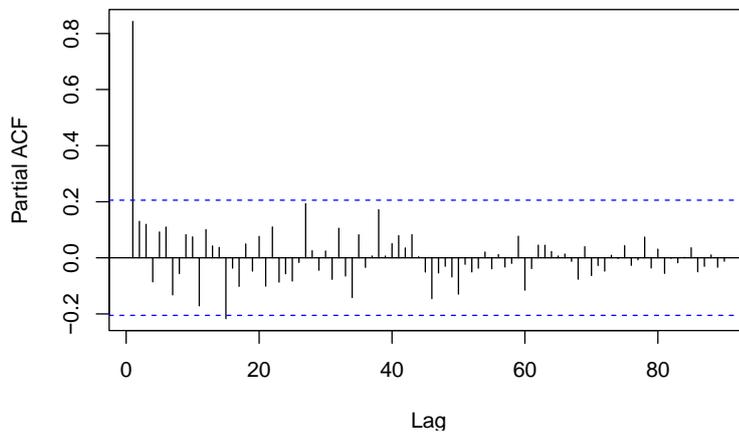
I correlogrammi delle funzioni stimate sono:

Figura 4.1.6, Funzione di autocorrelazione totale e parziale

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

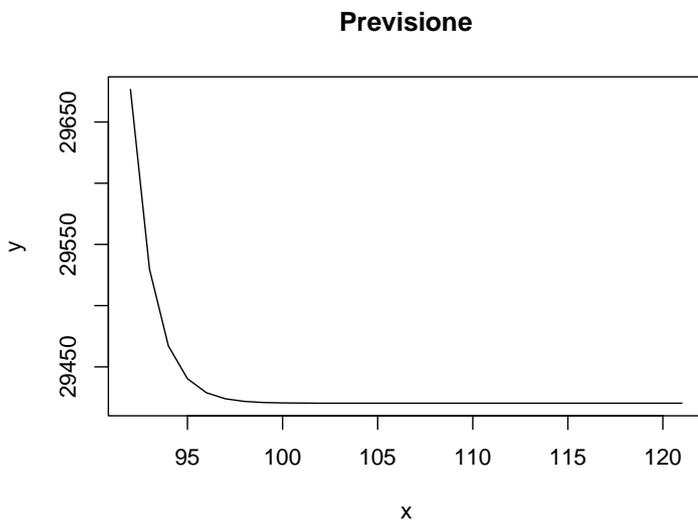
Coefficienti	Stime	Standard error	p-value
φ_1	0.4275	0.1836	0.6690
θ_1	-0.7552	0.1310	0.4501

Per quanto concerne il modello ARIMA stimato, è stato individuato l'ARIMA (1,1,1) e dunque è stata effettuata un'operazione di differenziazione al fine di rendere la serie stazionaria, il valore attuale della serie è dipendente dai suoi valori passati e dagli errori di questi ultimi.

Il coefficiente AR risulta essere pari ad 0.4275, con un errore standard pari a 0.1836, mentre il coefficiente MA ha valore negativo pari a -0.7552 con errore standard di 0.1310. I due indici AIC e BIC sono rispettivamente 1815.83 e 1823.33. Infine, per quanto riguarda il p-value, quest'ultimo risulta essere $1.346687e-56$.

La previsione di tale modello dei 30 giorni successivi l'ultimo valore considerato sarà:

Figura 4.1.7, previsione a 30 giorni del numero delle transazioni.

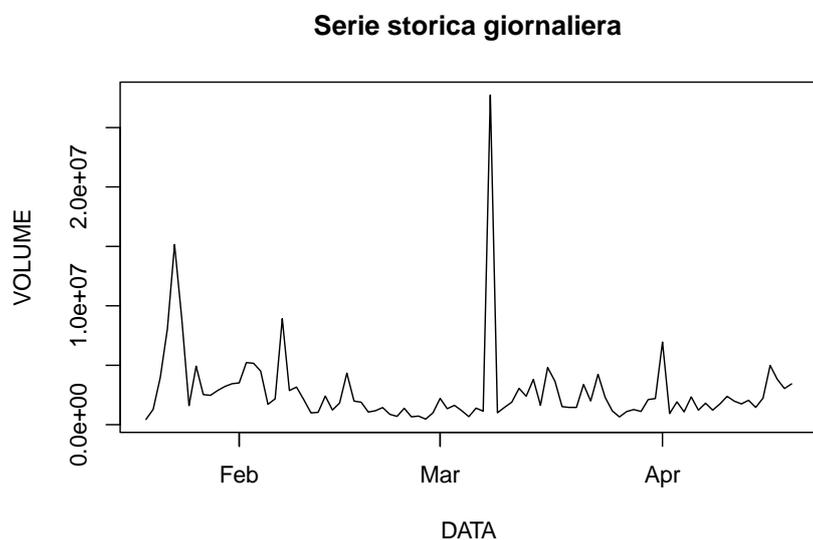


Fonte: elaborazione personale.

4.1.3 ANALISI IN SERIE STORICHE DEL VOLUME

Nel seguente grafico è riportato il volume delle transazioni espresso in dollari. Sull'asse y sono riportati i valori mentre sull'asse x il periodo considerato.

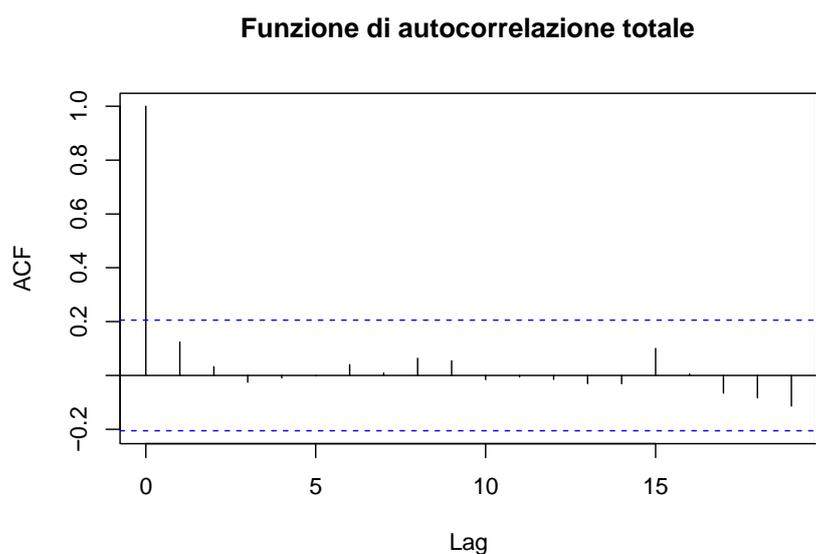
Figura 4.1.8, serie storica giornaliera volume.



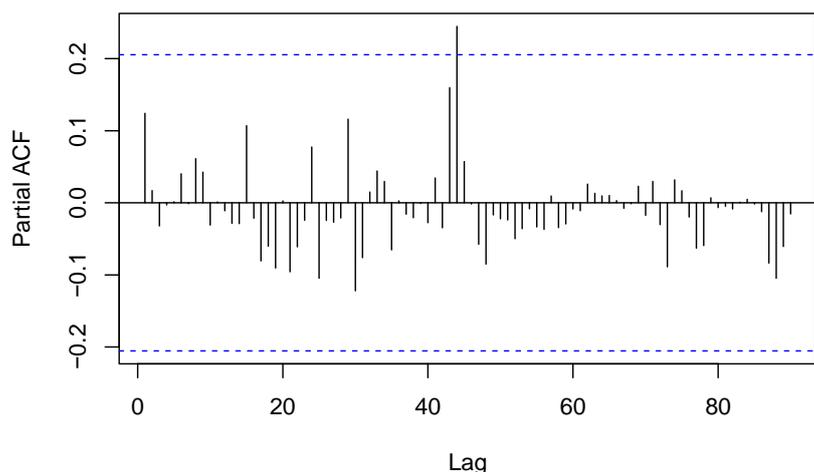
Fonte: elaborazione personale.

Le due funzioni di autocorrelazione stimate:

Figura 4.1.9, Funzione di autoregressione totale e parziale e coefficienti di autocorrelazione parziale.



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

Per quanto riguarda il modello ARIMA che maggiormente si adatta, è del tipo ARIMA (0,0,0) e dunque non è prevista la componente di differenziazione, quella autoregressiva e quella di media mobile. In questo caso, tuttavia, risulta significata la media, pari a 2823020.1 con errore standard di 356628.1. l'AIC e il BIC sono rispettivamente 2999.58 e 3004.6, mentre il p-value risulta essere $7.587736e-12$.

Per quanto concerne le previsioni, queste ultime risultano essere pari alla media della serie storica, ovvero 2823020, e ciò è giustificato dal modello ARIMA (0,0,0) stimato.

4.2 GODS UNCHAINED

Gods Unchained è un gioco di carte collezionabili (CCG) online, sviluppato dallo studio australiano Immutable. Il gioco è stato lanciato su Ethereum blockchain nel 2019, il che significa che le carte del gioco sono acquistabili, scambiabili e vendibili utilizzando la criptovaluta Ether (ETH).

In Gods Unchained, i giocatori assumono il ruolo di potenti dei che lottano per il controllo dell'Olimpo e del mondo sottostante. Ogni giocatore costruisce un mazzo di carte che rappresentano creature, incantesimi e armi, con i quali affrontare gli avversari in partite uno contro uno.

Il gioco prevede diverse modalità di gioco, tra cui la partita classica, la partita classificata, la partita con il mazzo preconfezionato e la partita del draft. In ognuna di queste modalità, i giocatori hanno l'opportunità di guadagnare nuove carte e premi in base al loro successo.

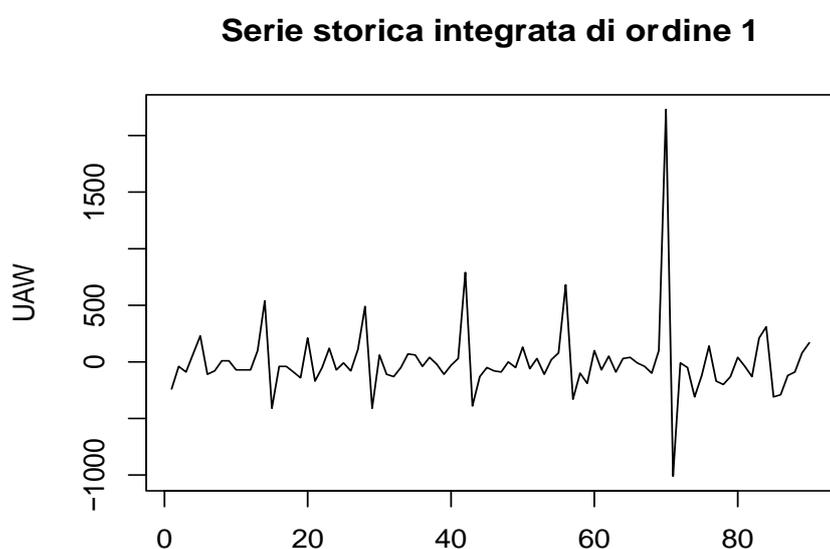
Le carte di Gods Unchained sono divise in quattro categorie: Comuni, Rare, Epiche e Leggendarie. Ogni carta ha un costo in ETH associato, che varia in base alla rarità e alla forza della carta. I giocatori possono acquistare pacchetti di carte casuali o specifiche per cercare di ottenere le carte più forti per il loro mazzo.

Inoltre, le carte di Gods Unchained sono tutte immutabilmente registrate sulla blockchain Ethereum, il che significa che vengono salvate in modo permanente e sicuro, e non possono essere modificate o copiate.

4.2.1 ANALISI IN SERIE STORICHE UAW

Nel seguente grafico è rappresentata la serie storica integrata di primo ordine dei UAW che risulta non essere stazionaria e dunque, al fine della costruzione del modello ARIMA, è stata effettuata un'operazione d'integrazione. Sull'asse delle ascisse è stato riportato il numero delle osservazioni, sull'asse delle ordinate i UAW.

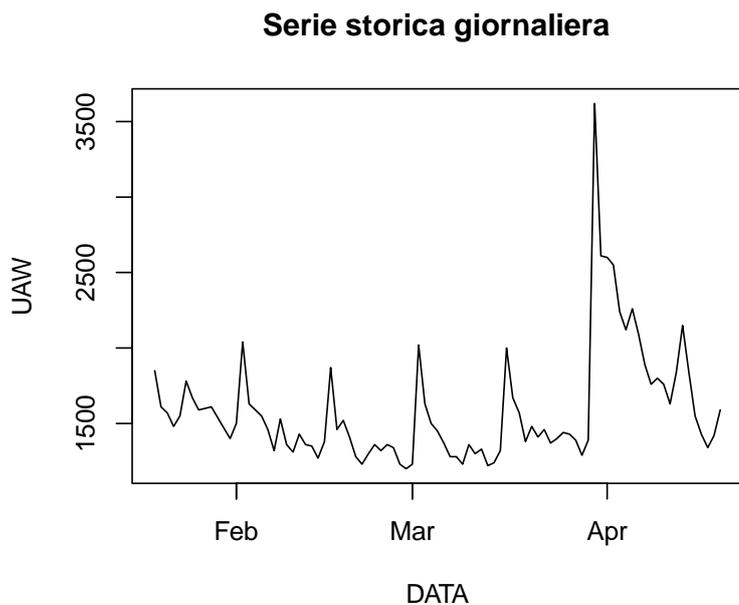
Figura 4.2.1, serie storica integrata di primo ordine.



Fonte: elaborazione personale.

Nel seguente grafico, viene indicata la serie storica la cui variabile d'interesse è rappresentata dal UAW. Sull'asse delle ascisse è riportato il periodo temporale, sull'asse delle ordinate il numero dei portafogli attivi.

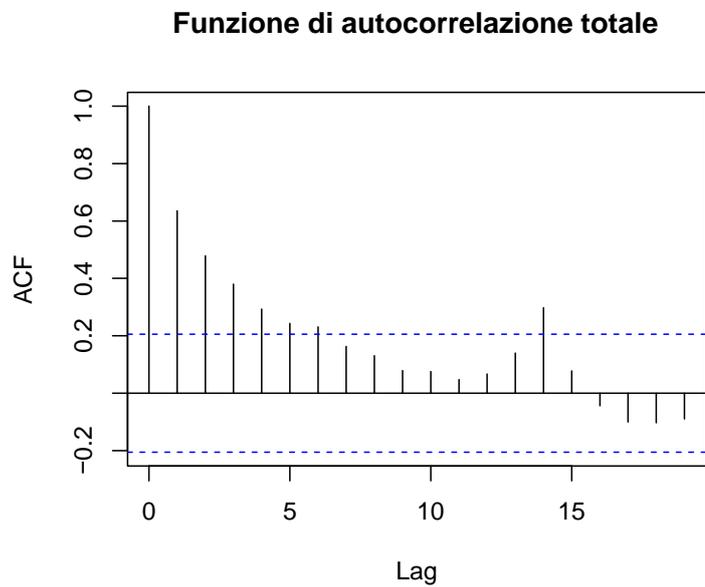
Figura 4.2.2, serie storica giornaliera UAW.



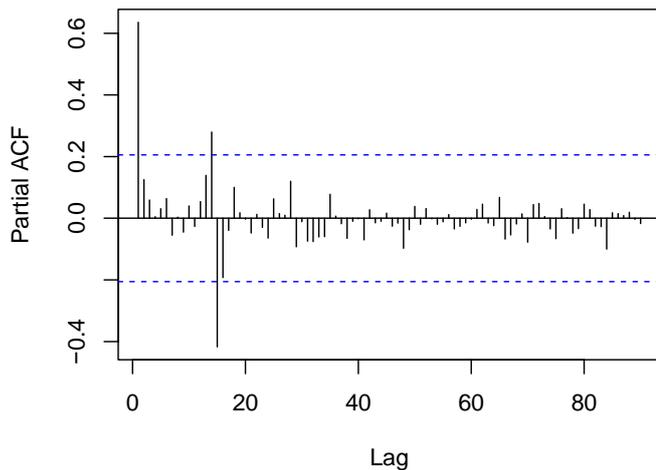
Fonte: elaborazione personale.

Le funzioni di correlazione globale e parziale risultano essere:

Figura 4.2.3, funzione di autocorrelazione globale e parziale.



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

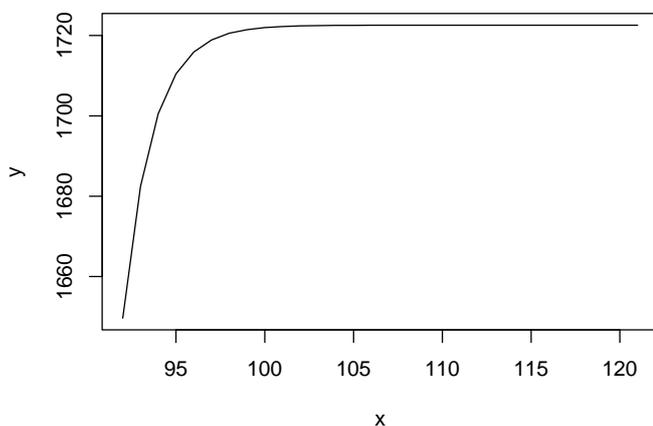
Coefficienti	Stime	Standard error	p-value
φ_1	0.5500	0.1605	0.5823
ϑ_1	-0.9185	0.1030	0.3583

Il modello ARIMA stimato (1,1,1) presenta una componente autoregressiva, una di media mediabile ed, inoltre, è stata effettuata un'operazione d'integrazione al fine di rendere la serie stazionaria. I coefficienti AR e MA risultano essere rispettivamente 0.5500 e -0.9185. il primo coefficiente ha errore standard pari a 0.1605, mentre il secondo 0.1030. L'AIC e il BIC calcolati sono 1285.76 il primo, 1293.26 il secondo. Il p-value è invece $5.757172e-59$.

Effettuata la previsione, i valori stimati sono:

Figura 4.2.4, previsioni a 30 gg.

Previsione

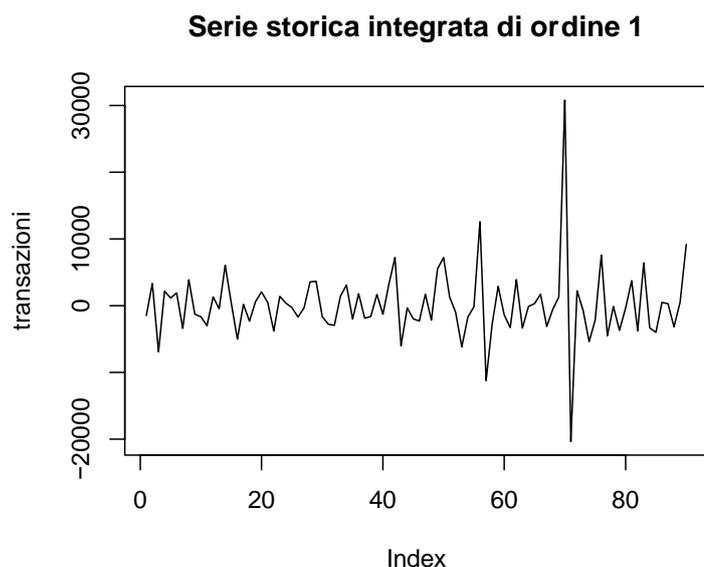


Fonte: elaborazione personale.

4.2.2 ANALISI IN SERIE STORICHE TRANSAZIONI

Il seguente grafico riporta sull'asse y il numero delle transazioni, sull'asse x il numero delle osservazioni. In questo viene riportata la serie storica integrata di primo ordine per cui è stata effettuata un'operazione di integrazione al fine di renderla stazionaria.

Figura 4.2.5, serie storica integrata di ordine 1.

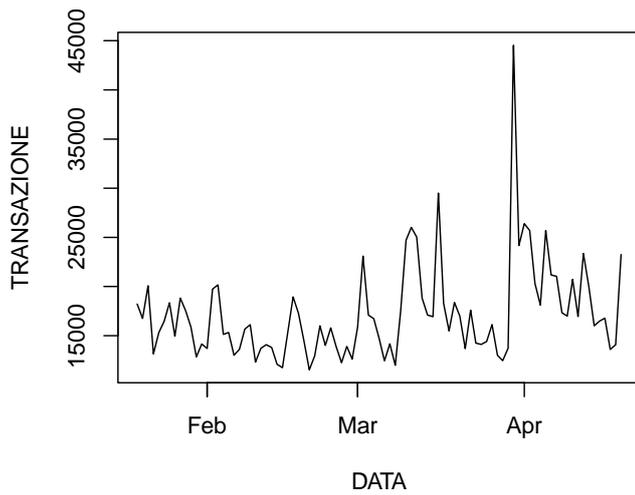


Fonte: elaborazione personale.

Il grafico che segue riporta la serie storica del numero delle transazioni. Sull'asse x viene indicato il periodo temporale considerato, sull'asse y il numero delle transazioni.

Figura 4.2.6, serie storica giornaliera numero transazioni.

Serie storica giornaliera

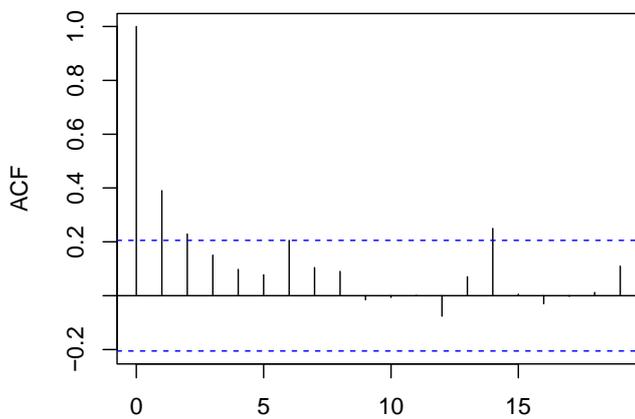


Fonte: elaborazione personale.

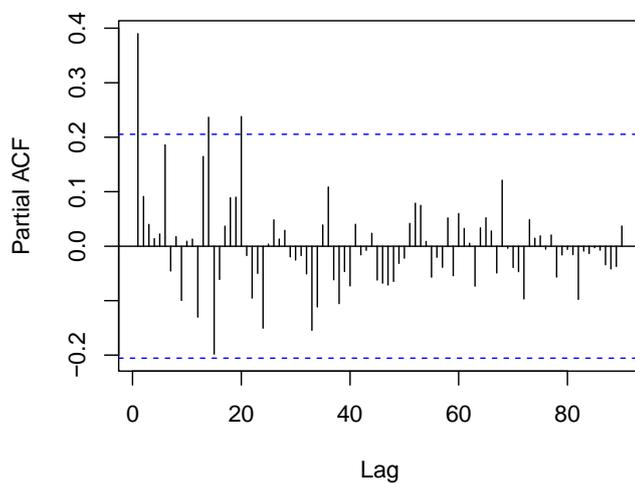
Le funzioni di autocorrelazione globale e parziale sono le seguenti:

Figura 4.2.7, funzione di autocorrelazione globale e parziale.

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



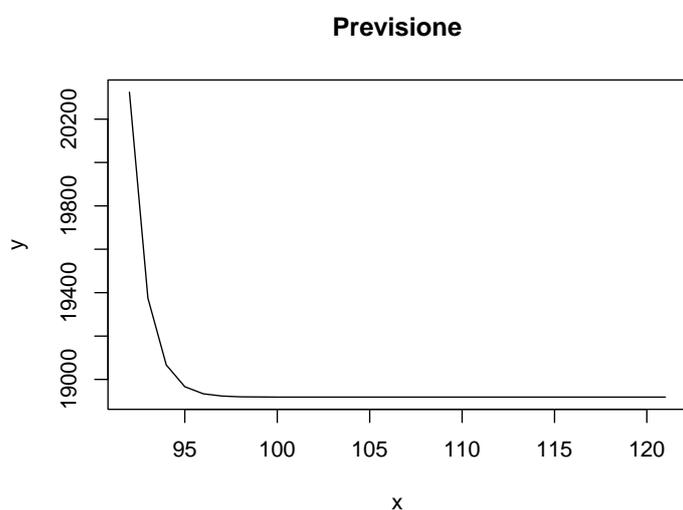
Fonte: elaborazione personale.

Coefficienti	Stime	Standard error	p-value
φ_1	0.3246	0.1131	0.7454
ϑ_1	-0.9374	0.0457	0.3485

Il modello ARIMA (1,1,1) presenta coefficiente AR pari a 0.3246 e MA pari a -0.9374. Per quanto riguarda gli errori standard, questi ultimi sono rispettivamente 0.1131 e 0.0457. Il p-value risulta essere $7.737137e-53$ mentre AIC e BIC sono il primo 1775.87, ed il secondo 1783.37.

Le previsioni effettuate mostrano i seguenti dati:

Figura 4.2.8, previsioni a 30 giorni.



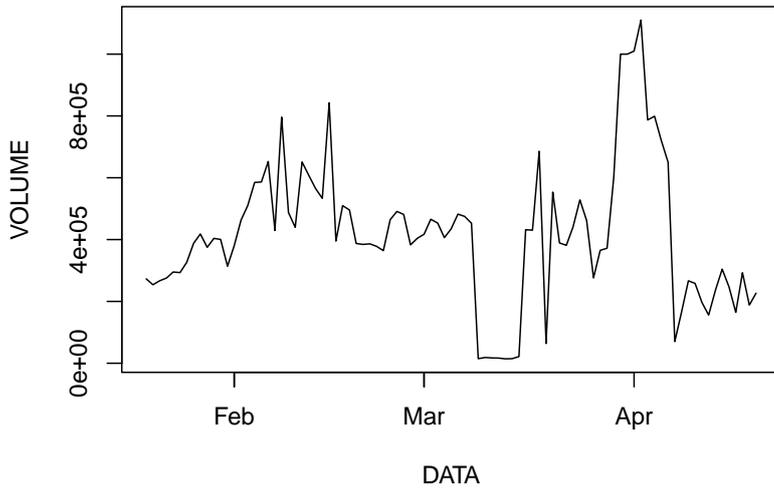
Fonte: elaborazione personale.

4.2.3 ANALISI IN SERIE STORICHE VOLUME

Nel seguente grafico è riportato il volume delle transazioni espresso in dollari. Sull'asse y sono riportati i valori mentre sulla asse x il periodo considerato.

Figura 4.2.9, serie storica giornaliera volume.

Serie storica giornaliera

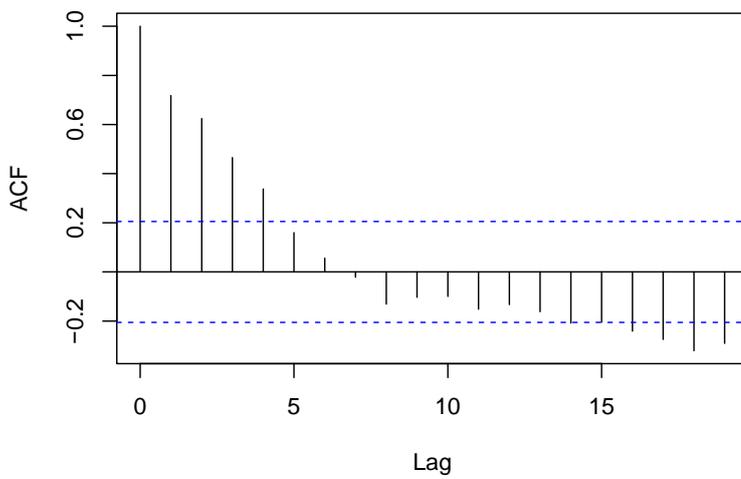


Fonte: elaborazione personale.

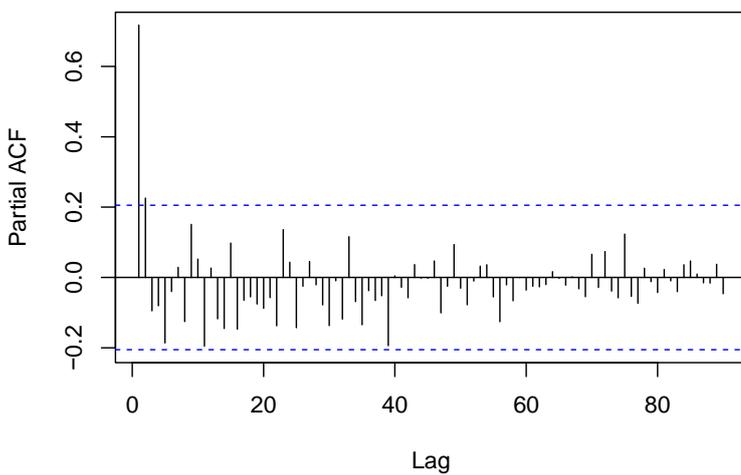
Le funzioni di autocorrelazione globale e parziale presentano i seguenti andamenti:

Figura 4.2.10, funzione di autocorrelazione globale e parziale.

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



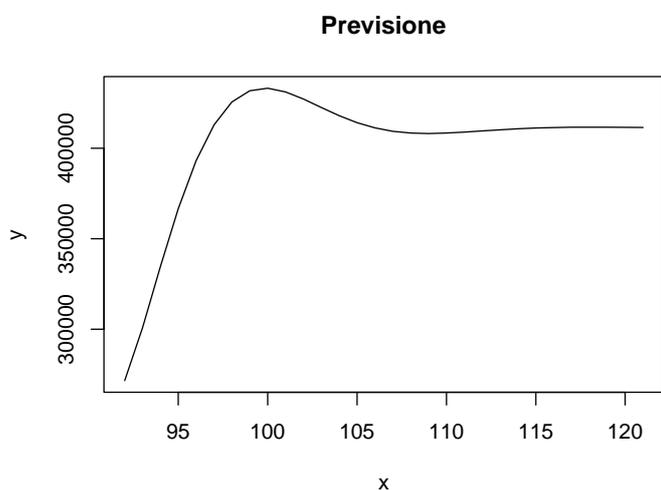
Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
φ_1	1.5173	0.2084	0.1291
φ_2	-0.6496	0.1807	0.5159
ϑ_1	-0.9920	0.2117	0.3211
ϑ_2	0.4305	0.1338	0.6668

Il modello ARIMA (2,0,2) non presenta alcuna componente I ad indicare il fatto non è stata effettuata nessun'operazione di differenziazione al fine di rendere la serie stazionaria in quanto quest'ultima presenta già tale caratteristica. Di contro, è possibile osservare due coefficienti AR, 1.5173 e -0.6496, con errore standard 0.2084 e 0.1807, e due coefficienti MA ovvero -0.9920 e 0.4305, con errore standard pari a 0.2117 e 0.1338. il p-value risulta essere 1.832904e-30, l'AIC e il BIC 2440.14 e 2455.21.

Le previsioni illustrano i seguenti dati:

Figura 4.2.11, previsioni a 30 giorni.



Fonte: elaborazione personale.

4.3 SANDBOX

Il gioco di Sandbox è un videogioco in cui il giocatore ha la possibilità di creare e manipolare un'ambientazione di gioco virtuale. Il gioco non ha uno scopo preciso, ma piuttosto offre al giocatore la libertà di esplorare e sperimentare. Di solito, il gioco di Sandbox utilizza un'interfaccia grafica semplice e intuitiva che consente al giocatore di interagire con gli oggetti e gli elementi dell'ambientazione di gioco che possono essere creati, distrutti, spostati o modificati in vari modi.

Uno dei principali aspetti del game è la sua libertà creativa. Il giocatore, infatti, ha la possibilità di creare qualsiasi cosa desideri, senza limiti di tempo o risorse. Ad esempio, il giocatore può costruire una casa, un ponte, una città o addirittura un intero mondo. Inoltre, il gioco di Sandbox spesso include anche una serie di strumenti e opzioni per manipolare l'ambiente di gioco. Questi strumenti possono includere la possibilità di cambiare la gravità, il clima, la luce e altri aspetti dell'ambiente.

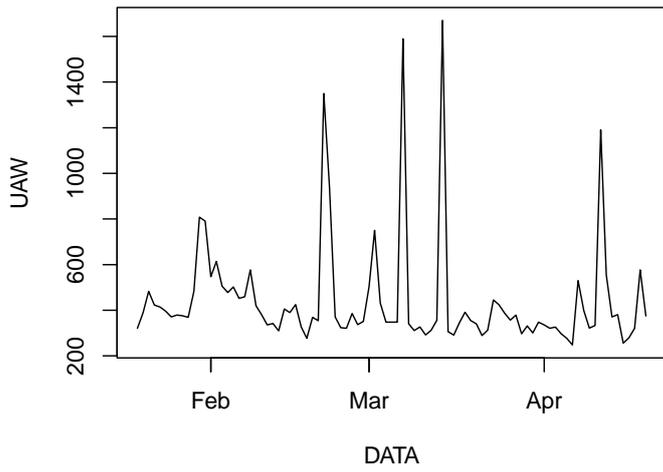
Il game, dunque, offre ai giocatori la possibilità di esplorare e sperimentare in un ambiente di gioco virtuale senza regole o limiti specifici. Per quanto concerne la blockchain Sandbox, questa si basa sulla tecnologia Ethereum, che consente la creazione di contratti intelligenti e di token non fungibili (NFT). In Sandbox, gli utenti possono acquistare token SAND, che possono essere utilizzati per acquistare terreni virtuali e altri oggetti all'interno del gioco. Ogni terreno virtuale è rappresentato da un contratto intelligente sulla blockchain Ethereum, che garantisce la proprietà e la gestione del terreno all'utente. Inoltre, gli utenti possono creare oggetti virtuali personalizzati utilizzando la tecnologia NFT, che consente di creare token unici e irripetibili sulla blockchain. Gli oggetti NFT possono essere utilizzati all'interno del gioco o venduti ad altri utenti. Ad esempio, un utente potrebbe creare un oggetto virtuale, come una spada magica, e rilasciarlo come NFT sulla blockchain Sandbox. Altri utenti possono quindi acquistare l'oggetto NFT e utilizzarlo all'interno del gioco.

4.3.1 ANALISI IN SERIE STORICHE UAW

Nel seguente grafico, viene indicata la serie storica la cui variabile d'interesse è rappresentata dal UAW. Sull'asse delle ascisse è riportato il periodo temporale, sull'asse delle ordinate il numero dei portafogli attivi.

Figura 4.3.1, serie storica giornaliera UAW.

Serie storica giornaliera

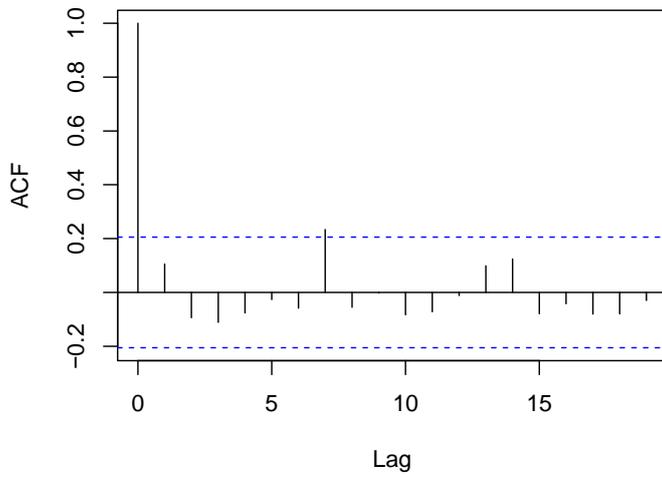


Fonte: elaborazione personale.

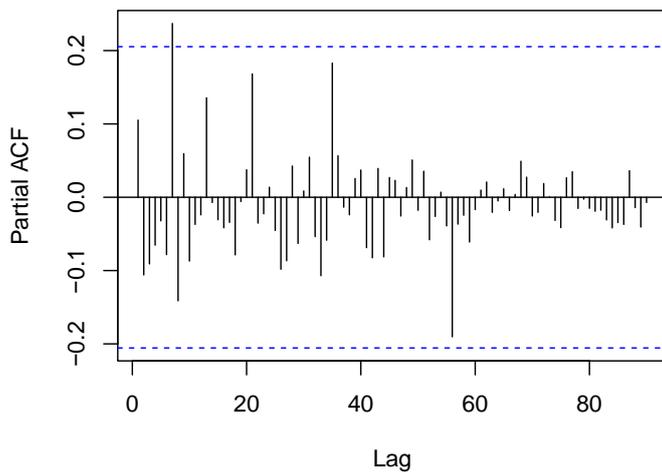
Le funzioni di autocorrelazione, globale e parziale, risultano essere:

figura 4.3.2, funzione di autocorrelazione globale e parziale.

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



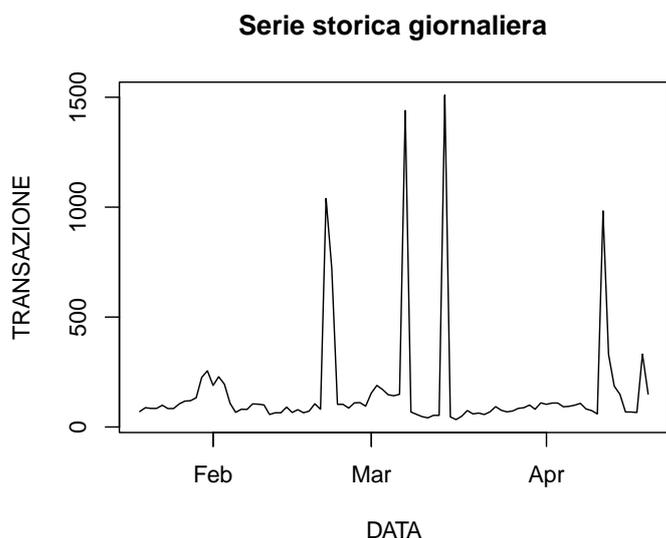
Fonte: elaborazione personale.

Il modello ARIMA (0,0,0) stimato non presenta la componente d'integrazione e non presenta coefficienti AR e MA. La media risulta 443.6813, con errore standard 26.1498, mentre l'AIC e il BIC risultano rispettivamente 1266.75 e 1271.78. Il test p-value per valutare la significatività del modello è $1.27734e-29$. Per quanto riguarda la previsione, essendo il modello ARIMA (0,0,0), quest'ultima è pari al valore della media e dunque 443.6813.

4.3.2 ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI

Il grafico che segue riporta la serie storica del numero delle transazioni. Sull'asse x viene indicato il periodo temporale considerato, sull'asse y il numero delle transazioni.

Figura 4.3.3, serie storica giornaliera numero delle transazioni.

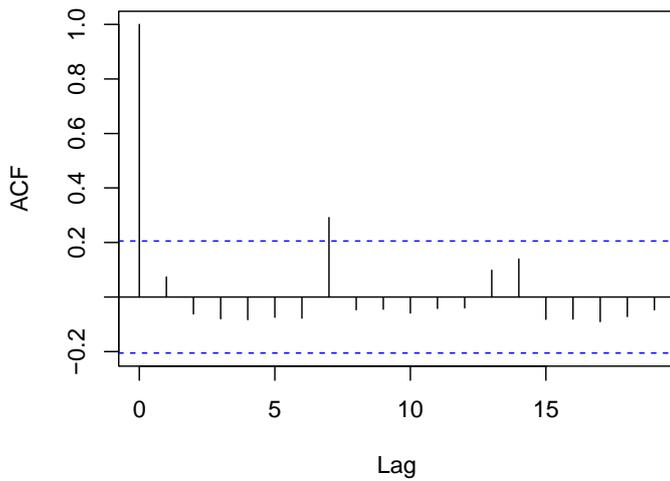


Fonte: elaborazione personale.

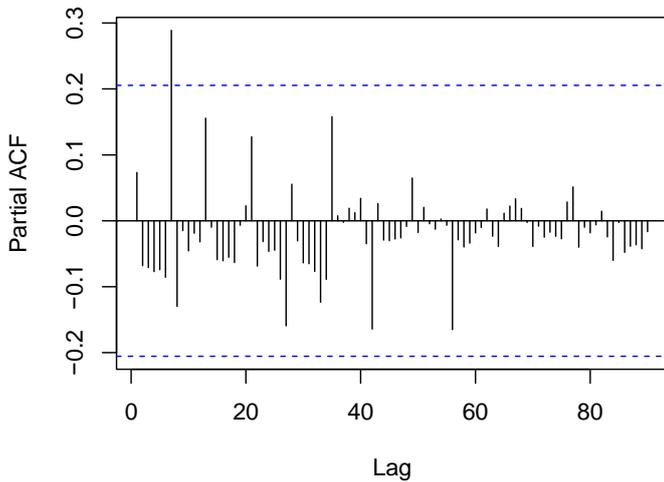
Le funzioni di autocorrelazione stimate:

Figura 4.3.4, funzione di autocorrelazione globale e parziale.

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



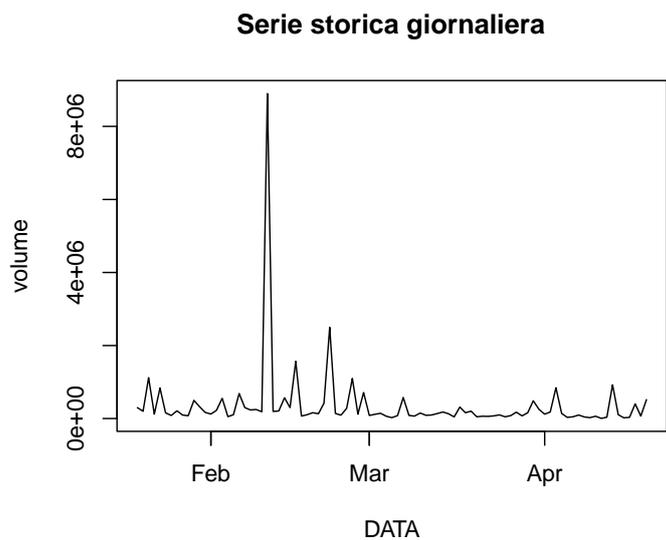
Fonte: elaborazione personale.

Anche in questo caso il modello ARIMA (0,0,0) risulta non avere la componente integrativa, i coefficienti AR e quelli MA. La media stimata è 160.9341 con errore standard 26.3843. L'AIC e il BIC del modello risultano essere 1268.38 e 1273.4, mentre il p-value è $3.037041e-08$. Come nel caso precedente, la previsione del modello è pari alla media e dunque 160.9341.

4.3.3 ANALISI IN SERIE STORICHE VOLUME

Nel seguente grafico è riportato il volume delle transazioni espresso in dollari. Sull'asse y sono riportati i valori mentre sulla asse x il periodo considerato.

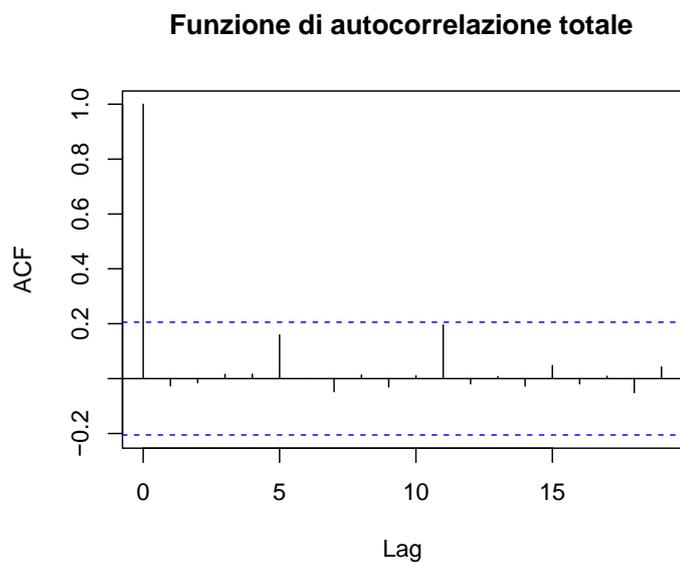
Figura 4.3.4, serie storica giornaliera volume.



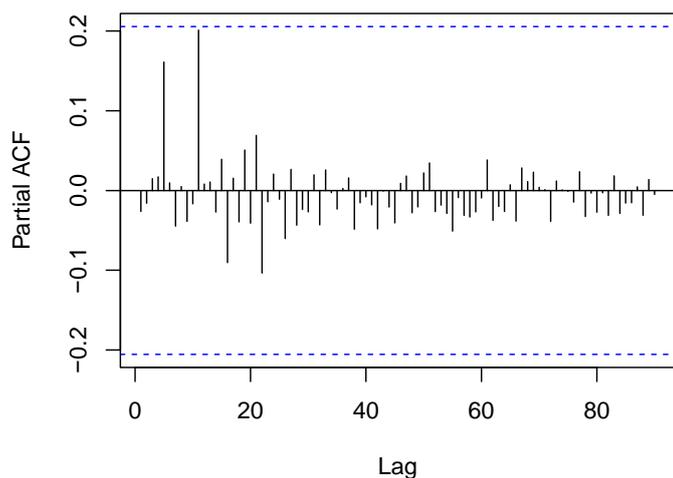
Fonte: elaborazione personale.

I seguenti correlogrammi rappresentano la funzione di autocorrelazione globale e parziale:

Figura 4.3.5, funzione di autocorrelazione globale e parziale.



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

Il modello ARIMA (0,0,0) non presenta coefficienti AR e MA e, in aggiunta, non è stata effettuata alcun'operazione di differenziazione al fine di rendere la serie stazionaria. La media stimata risulta essere 357922.2, con errore standard pari a 101724.6. L'AIC ed il BIC sono rispettivamente 2771.2 e 2776.22, mentre il test p-value dà come risultato 0.0007276918. Anche in questo caso la previsione effettuata coincide con la media e dunque è pari a 357922.2.

4.4 ALIENS WORLD

Aliens World è un gioco di ruolo multigiocatore online che si svolge in un mondo immaginario di fantascienza pieno di alieni, tecnologia avanzata e missioni intriganti. Il gioco è basato sulla tecnologia blockchain e utilizza token non fungibili (NFT) per rappresentare gli oggetti di gioco e gli asset digitali. Gli NFT di Aliens World sono creati sulla blockchain di Bella Protocol e sono disponibili per il commercio sui mercati NFT.

Gli NFT in Aliens World rappresentano oggetti di gioco unici come armi, veicoli, equipaggiamento e altro ancora. Questi, possono essere guadagnati partecipando alle missioni, raggiungendo gli obiettivi previsti dal gioco, attraverso lo scambio o la partecipazione ad eventi speciali in-game. I giocatori, dunque, possono possedere e commerciare liberamente i loro oggetti di gioco, creando un'economia di gioco decentralizzata all'interno di Aliens World. Inoltre, grazie alla tecnologia blockchain, gli NFT di Aliens World sono protetti dalla contraffazione e sono garantiti come unici e autentici.

4.4.1 ANALISI IN SERIE STORICHE UAW

Il grafico riporta la serie storica integrata di ordine 1 nella quale è possibile osservare la non stazionarietà della serie. Al fine di poter procedere con la sua analisi, è stata effettuata un'operazione d'integrazione. Sull'asse x è riportato il numero delle osservazioni, sull'asse y il valore dei UAW.

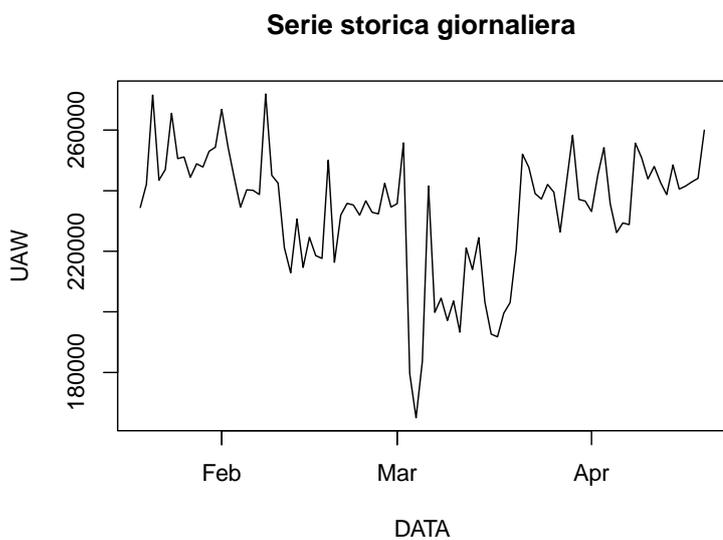
Figura 4.4.1, serie storica integrata di primo ordine.



Fonte: elaborazione personale.

Nel seguente grafico, viene indicata la serie storica la cui variabile d'interesse è rappresentata dal UAW. Sull'asse delle ascisse è riportato il periodo temporale, sull'asse delle ordinate il numero dei portafogli attivi.

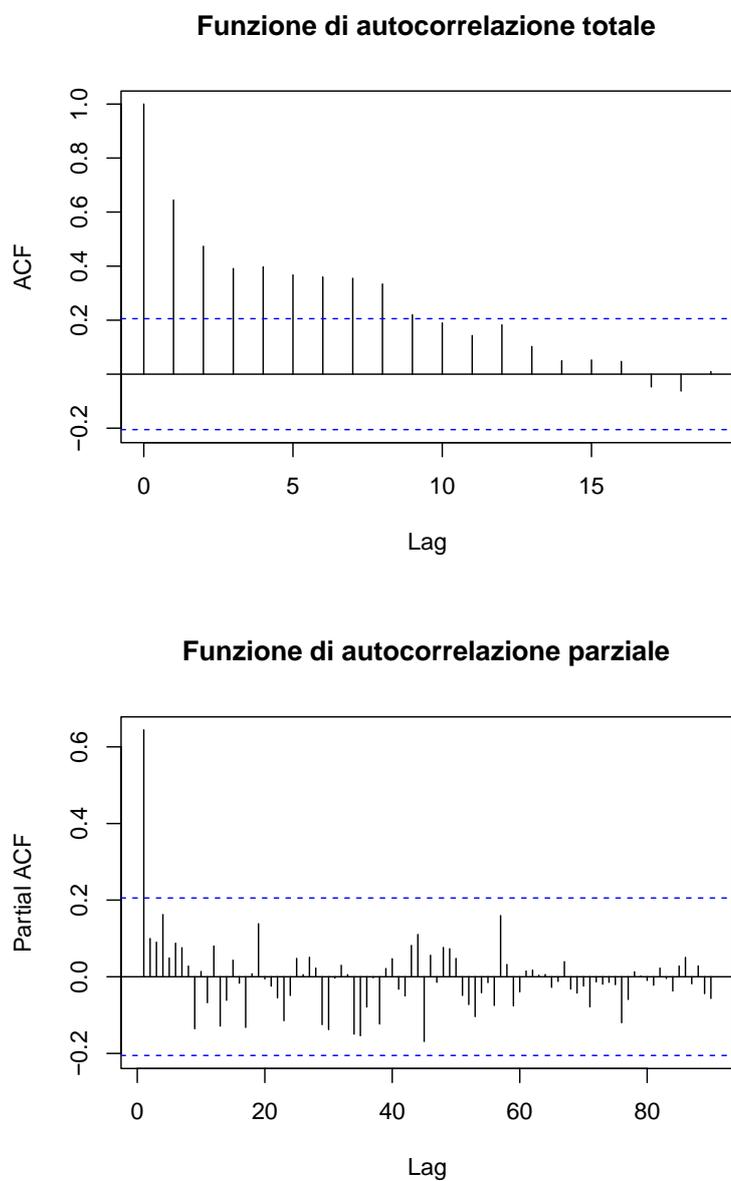
Figura 4.4.2, serie storica giornaliera UAW.



Fonte: elaborazione personale.

Le funzioni di autocorrelazione, totale e parziale, sono di seguito elencate:

Figura 4.4.3, funzione di autocorrelazione totale e parziale.



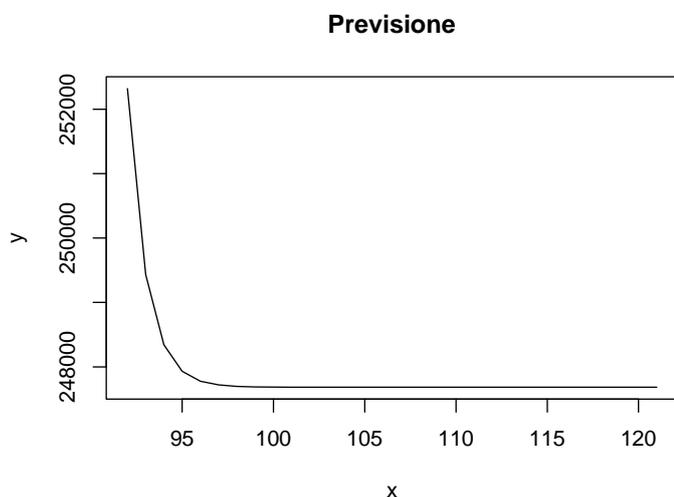
Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
φ_1	0.377	0.147	0.7061
ϑ_1	-0.8218	0.0892	0.4111

Il modello ARIMA (1,1,1) stimato, suggerisce una componente autoregressiva pari a 0.377, con errore standard 0.147, una componente di media mobile pari a -0.8218, con errore standard pari a 0.0892, ed una

componente integrativa ad indicare che è stata effettuata un'operazione di differenziazione per rendere la serie stazionaria. L'AIC ed il BIC stimati sono rispettivamente 1999.45 e 2006.94, mentre il p-value indica come risultato $8.076746e-97$. Infine, le previsioni effettuate indicano i seguenti risultati:

Figura 4.4.4, previsione a 30 giorni.



Fonte: elaborazione personale.

4.4.2 ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI

Nel seguente grafico è stata riportata la serie storica integrata di primo ordine. Sull'asse x è rappresentato il numero delle osservazioni, sull'asse y il numero delle transazioni.

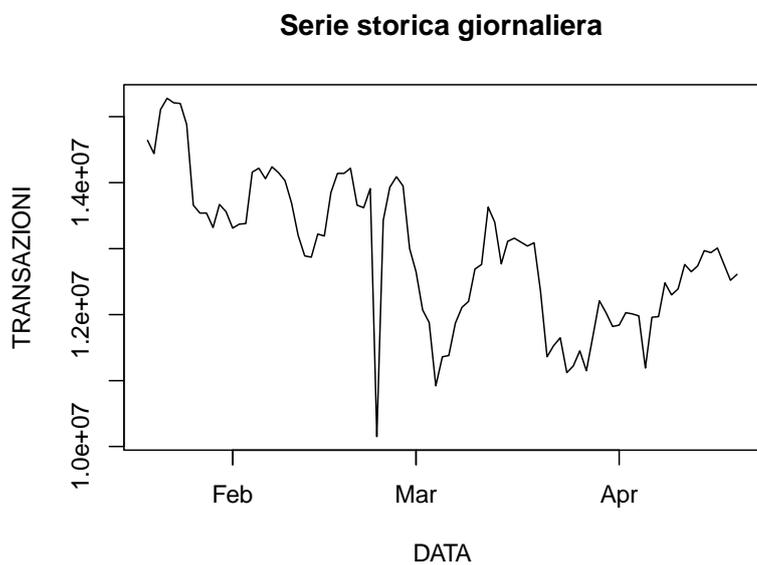
Figura 4.4.5, serie storica integrata di primo ordine.



Fonte: elaborazione personale.

Il grafico che segue riporta la serie storica del numero delle transazioni. Sull'asse x viene indicato il periodo temporale considerato, sull'asse y il numero delle transazioni.

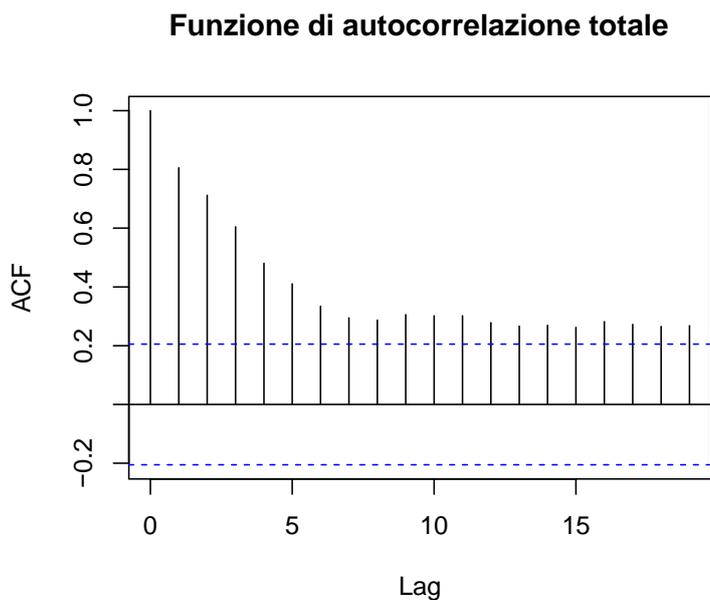
Figura 4.4.6, serie storica giornaliera numero transazioni.



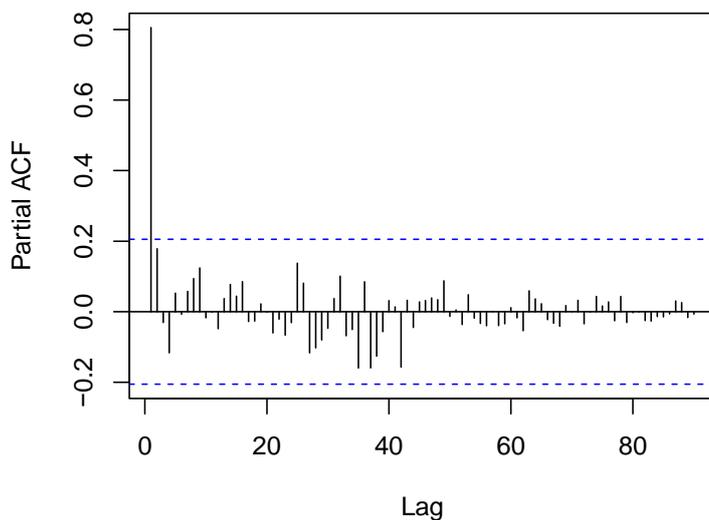
Fonte: elaborazione personale.

Le due funzioni di autocorrelazione stimate:

Figura 4.4.7, funzione di autocorrelazione totale e parziale.



Funzione di autocorrelazione parziale



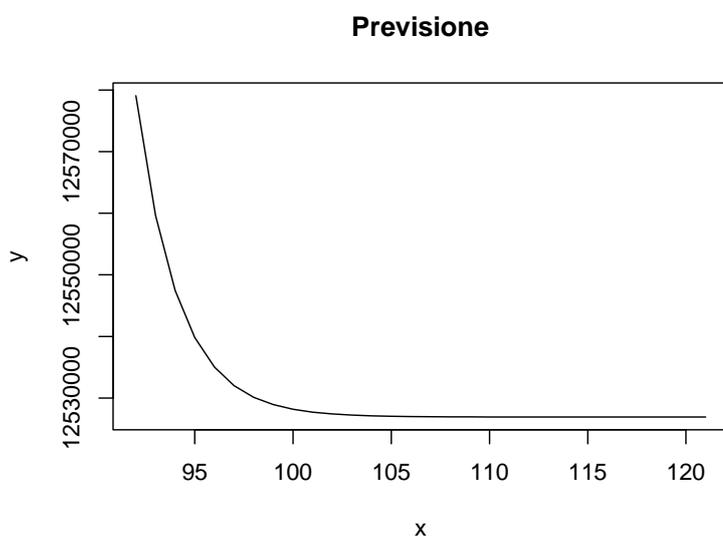
Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
φ_1	0.6278	0.1254	0.5301
ϑ_1	-0.8910	0.0719	0.3729

Il modello ARIMA (1,1,1) stimato indicata una componente AR, con coefficienti pari a 0.6278, il cui errore standard è 0.1254, ed una componente MA con coefficienti pari a -0.8910, ed errore standard pari a 0.0719. Il test p-value suggerisce come valore $7.827551e-99$, mentre l'AIC ed il BIC del modello corrispondono rispettivamente a 2662.65 e 2670.15.

Le previsioni stimate sono di seguito elencate:

Figura 4.4.8, previsioni a 30 giorni.

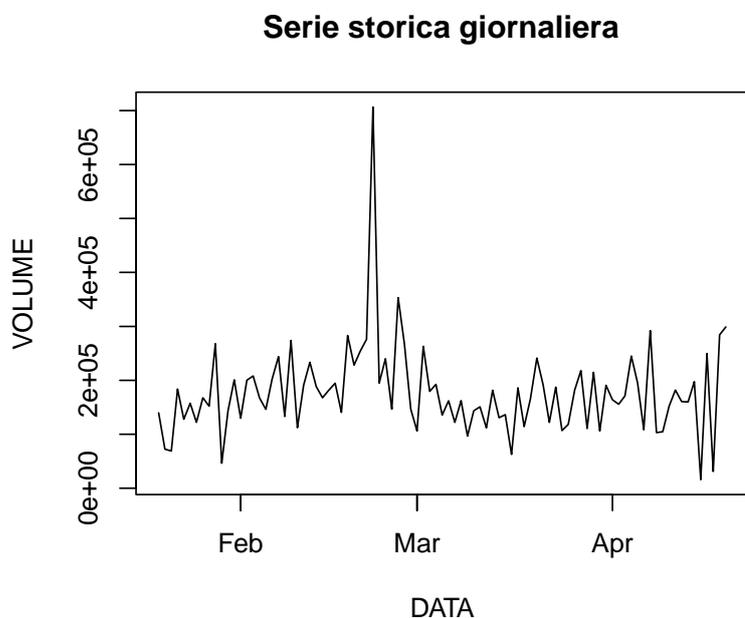


Fonte: elaborazione personale.

4.4.3 ANALISI IN SERIE STORICHE VOLUME

Nel seguente grafico è riportato il volume delle transazioni espresso in dollari. Sull'asse y sono riportati i valori mentre sulla asse x il periodo considerato.

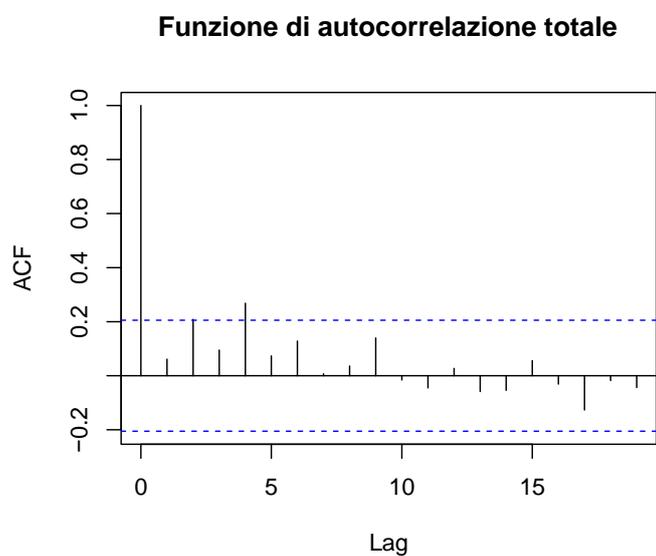
Figura 4.4.9, serie storica giornaliera volume.



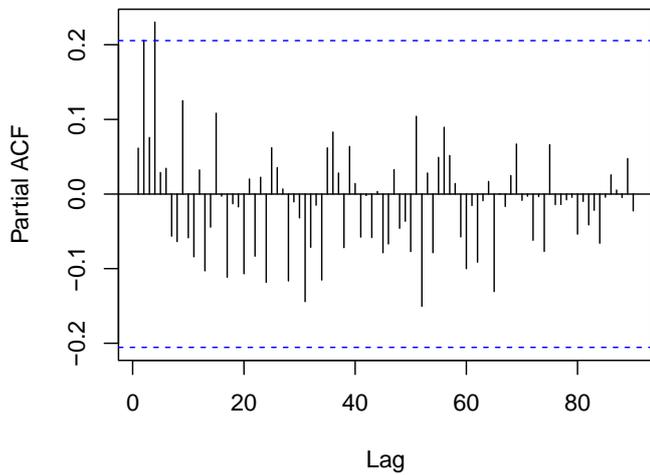
Fonte: elaborazione personale.

Le due funzioni di autocorrelazione stimate:

Figura 4.4.10, funzione di autocorrelazione totale e parziale.



Funzione di autocorrelazione parziale



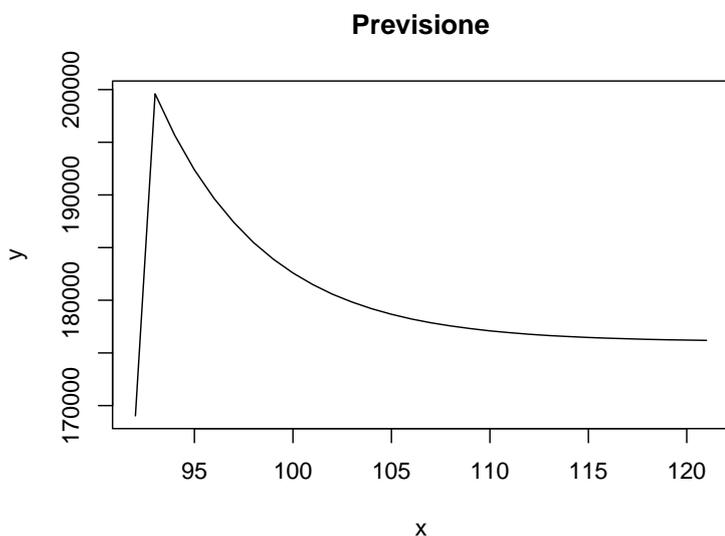
Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
φ_1	0.8329	0.1189	0.4049
ϑ_1	-0.8533	0.1567	0.3934
ϑ_2	0.1906	0.1157	0.8488

Il modello ARIMA (1,0,2) stimato presenta come coefficiente AR 0.8329, con errore standard 0.1189. per quanto riguarda la componente MA, vengono indicati due coefficienti, ovvero -0.8533 e 0.1906, i cui errori standard sono rispettivamente 0.1567 e 0.1157. L'AIC ed il BIC stimati sono pari 2323.66 il primo, 2336.22 il secondo. Il p-value è $5.737001e-35$.

Le previsioni presentano il seguente andamento:

Figura 4.4.11, previsioni a 30 giorni.



Fonte: elaborazione personale.

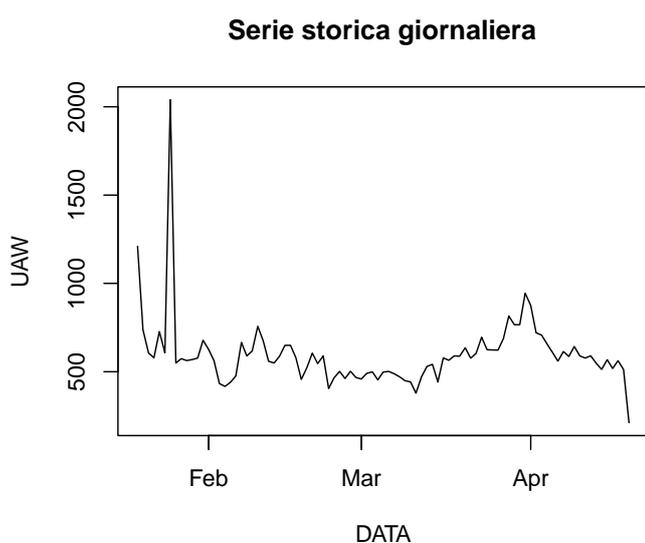
4.5 DECENTRALAND

Decentraland è un mondo virtuale completamente decentralizzato in cui i giocatori possono acquistare, possedere e sviluppare la propria terra virtuale utilizzando la tecnologia blockchain. Il mondo virtuale è formato da una mappa in cui ogni terreno virtuale è rappresentato da un token non fungibile (NFT) sulla blockchain Ethereum. I giocatori possono creare e personalizzare il proprio avatar, esplorare il mondo virtuale, socializzare con altri giocatori e partecipare a eventi e attività all'interno del gioco. Inoltre, questi ultimi possono acquistare e vendere terreni virtuali utilizzando la criptovaluta nativa del gioco, chiamata MANA. I terreni sono venduti in base alla loro posizione sulla mappa e alla loro dimensione. Possedendo un terreno, gli utenti possono costruire edifici, creare giochi e interagire con altri giocatori. Essendo un game su blockchain, Decentraland è completamente gestito dai suoi utenti che possono prendere decisioni attraverso la loro partecipazione alle votazioni nel game.

4.5.1 ANALISI IN SERIE STORICHE UAW

Nel seguente grafico, viene indicata la serie storica la cui variabile d'interesse è rappresentata dal UAW. Sull'asse delle ascisse è riportato il periodo temporale, sull'asse delle ordinate il numero dei portafogli attivi.

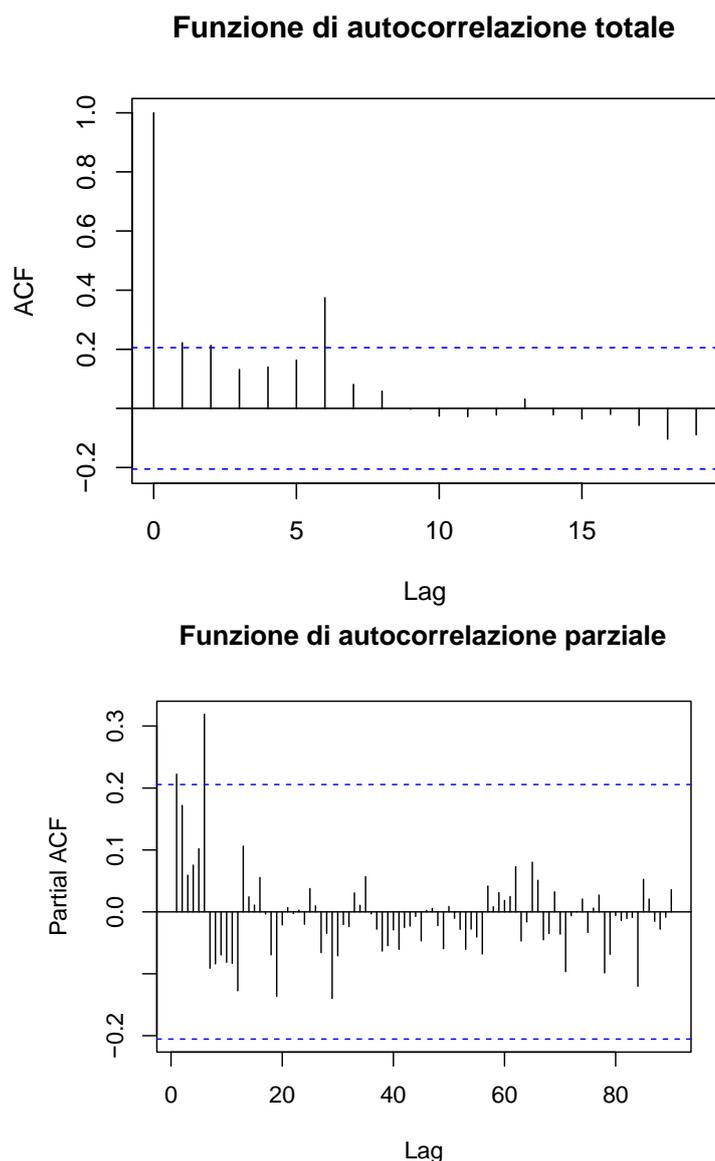
Figura 4.5.1, serie storica giornaliera UAW.



Fonte: elaborazione personale.

Le funzioni di autocorrelazione totale e parziale:

Figura 4.5.2, funzione di autocorrelazione totale e parziale.



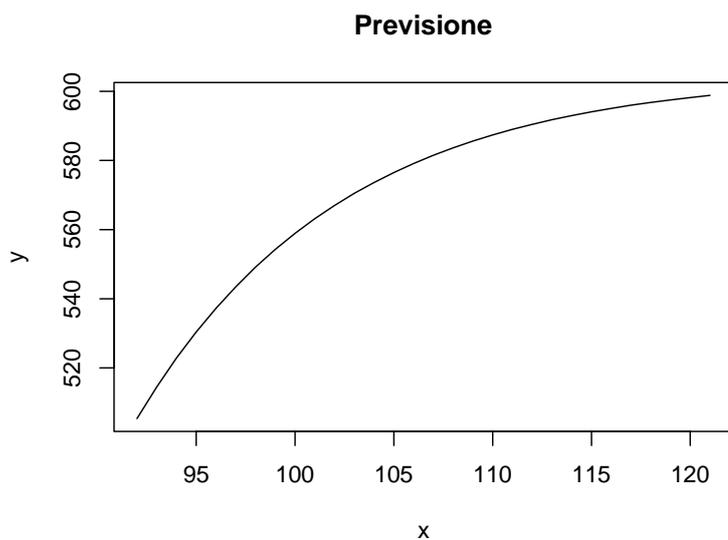
Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
φ_1	0.9079	0.0811	0.3639
ϑ_1	-0.7290	0.1142	0.466

Il modello ARIMA (1,0,1) suggerisce una componente autoregressiva con coefficiente pari 0.9079 ed errore standard 0.0811 ed una di media mobile pari a -0.7290, con errore standard 0.1142. L'AIC ed il BIC del modello sono 1217.67 e 1227.71, mentre il p-value $6.49164e-47$.

Le previsioni stimate del modello sono di seguito elencate:

Figura 4.5.3, previsioni a 30 giorni.

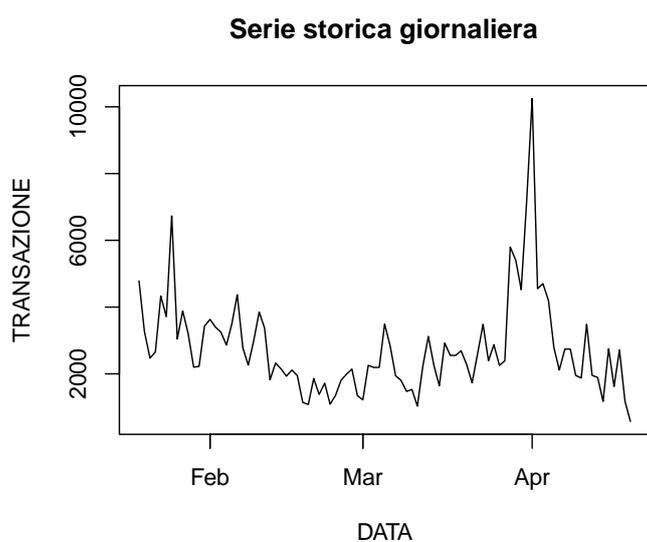


Fonte: elaborazione personale.

4.5.2 ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI

Il grafico che segue riporta la serie storica del numero delle transazioni. Sull'asse x viene indicato il periodo temporale considerato, sull'asse y il numero delle transazioni.

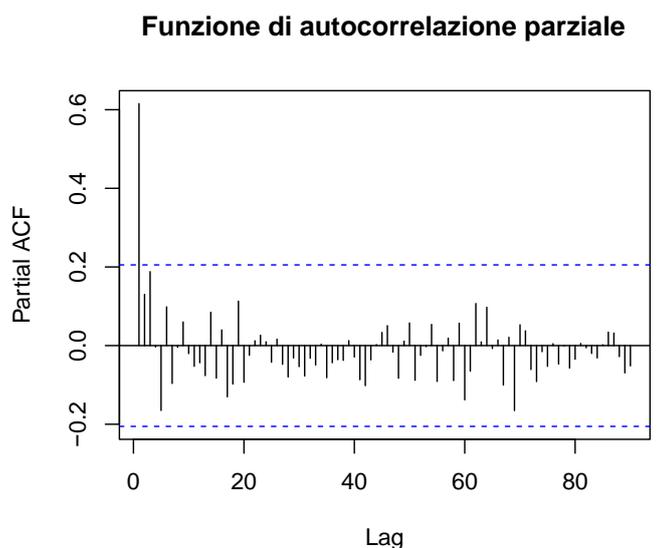
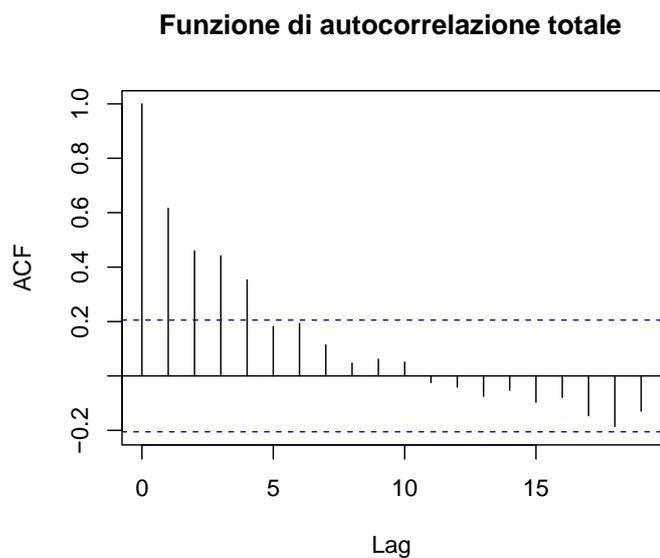
Figura 4.5.4, serie storica giornaliera numero transazioni.



Fonte: elaborazione personale.

Le funzioni di autocorrelazione stimate:

Figura 4.5.5, funzioni di autocorrelazione totale e parziale.



Fonte: elaborazione personale.

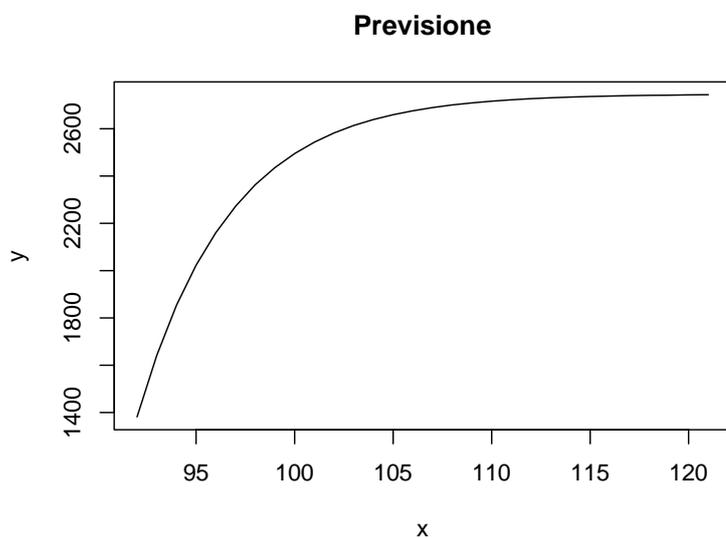
Coefficienti	Stime	Errore standard	p-value
φ_1	0.8094	0.0955	0.4182
ϑ_1	-0.3027	0.1588	0.7621

Il modello ARIMA (1,0,1) indica come coefficiente AR il valore 0.8094, con errore standard 0.0955. Per il coefficiente MA è stato stimato il valore -0.3027, con errore standard 0.1588. anche in questo caso, inoltre,

non è stata effettuata alcun'operazione d'integrazione per rendere la serie stazionaria. L'AIC ed il BIC indicati del modello sono 1541.39 e 1551.43. Il p-value risulta essere $6.276246e-32$.

Le previsioni del modello sono di seguito elencate:

Figura 4.5.6, previsioni a 30 giorni.



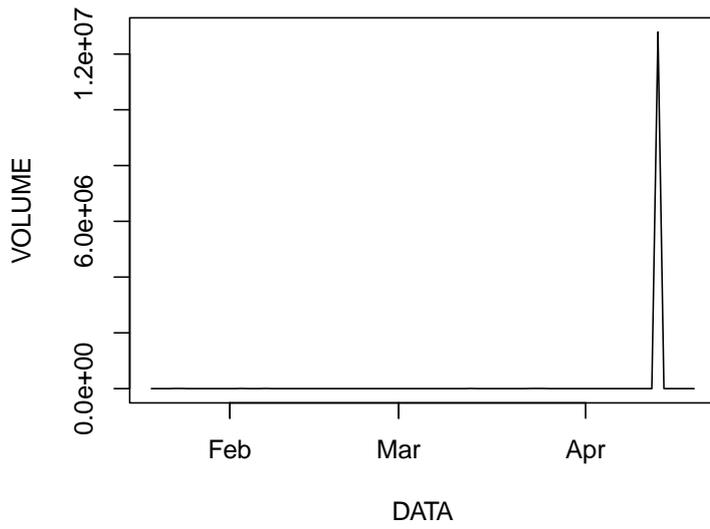
Fonte: elaborazione personale.

4.5.3 ANALISI IN SERIE STORICHE VOLUME

Nel seguente grafico è riportato il volume delle transazioni espresso in dollari. Sull'asse y sono riportati i valori mentre sulla asse x il periodo considerato.

Figura 4.5.7, serie storica giornaliera volume.

Serie storica giornaliera

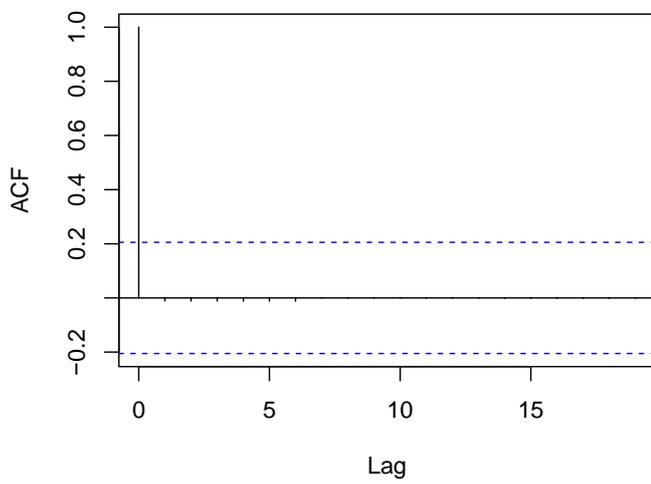


Fonte: elaborazione personale.

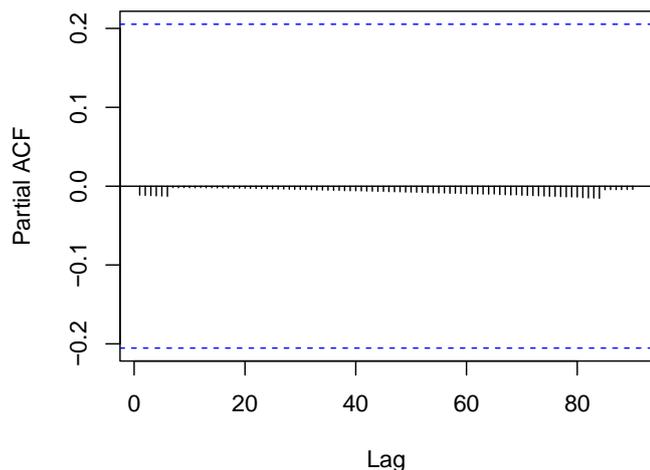
Le funzioni di autocorrelazione stimate:

Figura 4.5.8, funzione di autocorrelazione globale e parziale.

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

Il modello ARIMA (0,0,0) non presenta la componente integrativa, quella AR e quella MA. L'AIC ed il BIC stimati del modello sono rispettivamente 2828.04 e 2830.55. il p-value risulta essere 0.311948.

Per quanto concerne le previsioni, queste risulteranno uguali alla media ovvero 142892,10 in quanto il modello stimato è ARIMA (0,0,0).

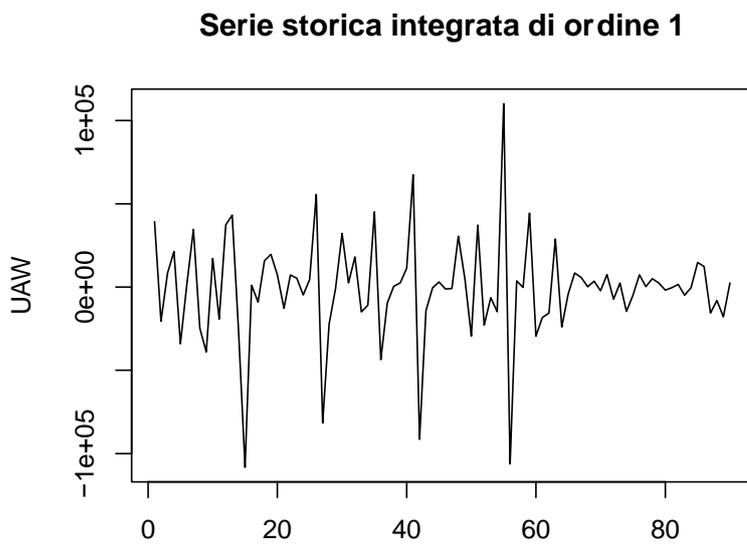
4.6 SPLINTERLANDS

Splinterlands è un gioco in cui i giocatori collezionano e usano carte per combattere contro altri giocatori in battaglie uno contro uno. Le carte sono rappresentate come token non fungibili (NFT) sulla blockchain di Hive e ogni carta rappresenta un personaggio unico con abilità speciali. I giocatori iniziano con una selezione di carte di base e possono guadagnare carte migliori completando missioni e partecipando a battaglie. Le carte possono essere migliorate utilizzando risorse in-game e possono essere vendute o scambiate con altri giocatori su mercati NFT. Le battaglie in Splinterlands si svolgono in tempo reale e sono gestite da un algoritmo di intelligenza artificiale che simula gli scontri tra le carte. I giocatori scelgono le loro carte e le posizionano in modo strategico sulla mappa di gioco, cercando di sconfiggere le carte dell'avversario e proteggere le proprie. All'interno del game, ci sono diverse modalità attraverso cui guadagnare il token nativo del game, denominato DEC. Partecipazione alle battaglie, completamento delle missioni, vendita delle carte e guadagni dei tornei sono le modalità principali. Inoltre, è possibile utilizzare il DEC per acquistare pacchetti di carte, che contengono carte casuali con differenti rarità ed abilità, e risorse in-game sulla piattaforma.

4.6.1 ANALISI IN SERIE STORICHE UAW

Nel seguente grafico è rappresentata la serie storica integrata di primo ordine per cui è stata effettuata un'operazione d'integrazione al fine di renderla stazionaria. Sull'asse y sono rappresentati i UAW, sull'asse x il numero delle osservazioni.

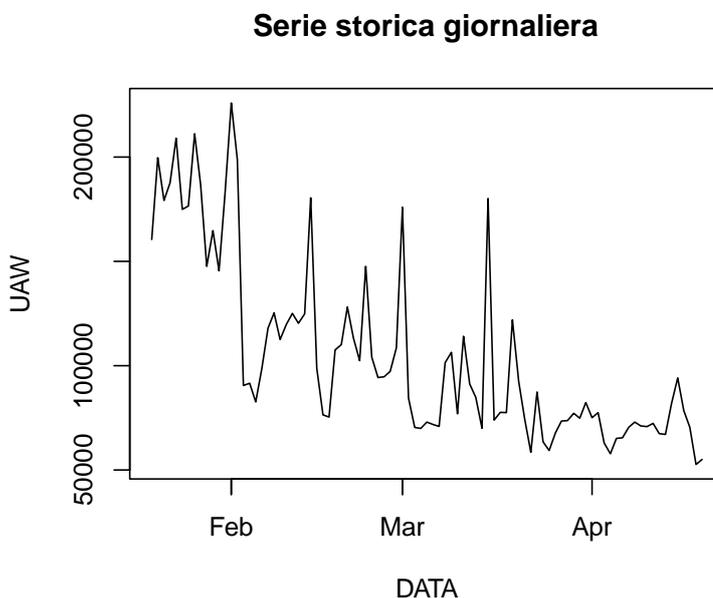
Figura 4.6.1, serie storica integrata di primo ordine.



Fonte: elaborazione personale.

Nel seguente grafico, viene indicata la serie storica la cui variabile d'interesse è rappresentata dal UAW. Sull'asse delle ascisse è riportato il periodo temporale, sull'asse delle ordinate il numero dei portafogli attivi.

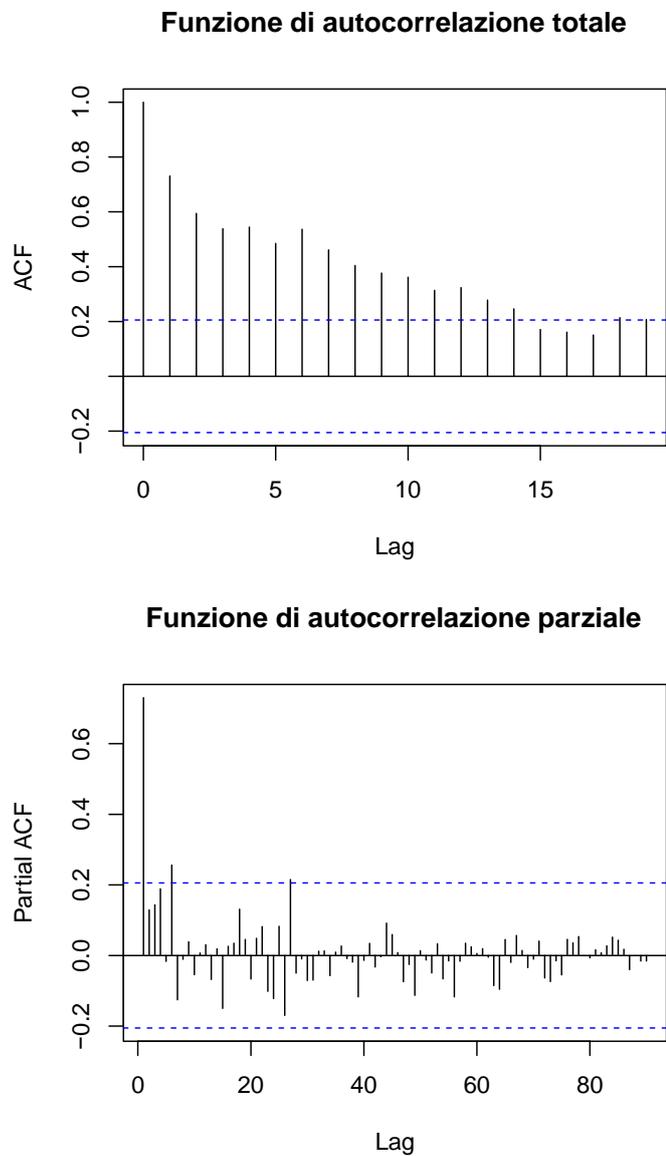
Figura 4.6.2, serie storica giornaliera UAW.



Fonte: elaborazione personale.

Le funzioni di autocorrelazione totale e parziale:

Figura 4.6.3, funzione di autocorrelazione totale e parziale.

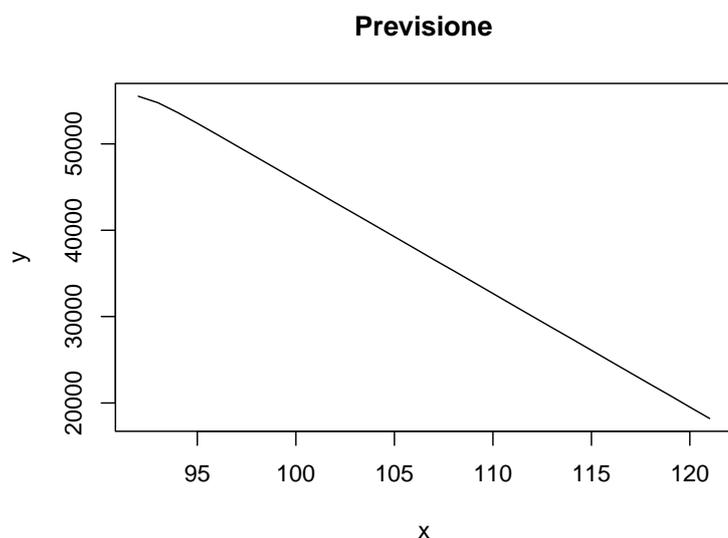


Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
φ_1	0.3243	0.1288	0.7457
ϑ_1	-0.9150	0.0668	0.36

Il modello ARIMA (1,1,1) presenta un'operazione d'integrazione, coefficiente AR pari a 0.3243 con errore standard 0.1288, e coefficiente MA pari a -0.9150 con errore standard 0.0668. Oltre coefficiente AR e MA, il modello stimato presenta un drift negativo il cui coefficiente ed errore standard sono rispettivamente -1315.4097 e 401.1446. L'AIC ed il BIC del modello sono 2097 e 2107 mentre il p-value è 2.101411e-39. Le previsioni stimate del modello sono le seguenti:

4.6.4, previsioni a 30 giorni.



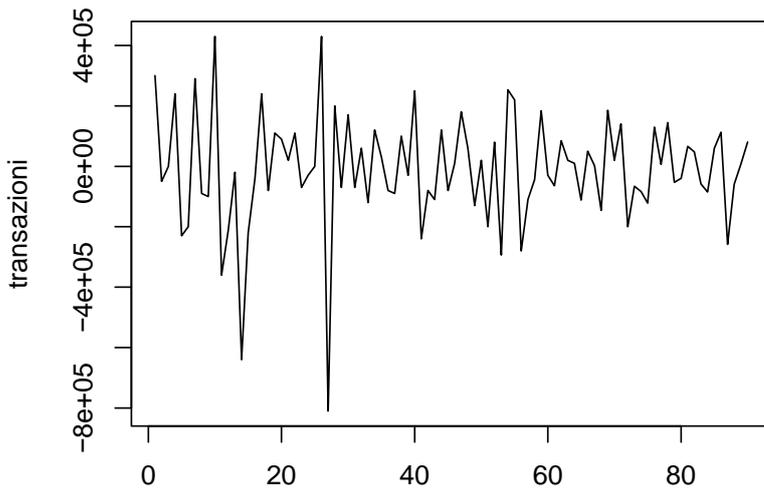
Fonte: elaborazione personale.

4.6.2 ANALISI IN SERIE STORICHE NUMERO TRANSAZIONI

Nel seguente grafico è stata riportata la serie storica integrata di primo ordine. Sull'asse x è rappresentato il numero delle osservazioni, sull'asse y il numero delle transazioni.

Figura 4.6.5, serie storica integrata di primo ordine.

Serie storica integrata di ordine 1

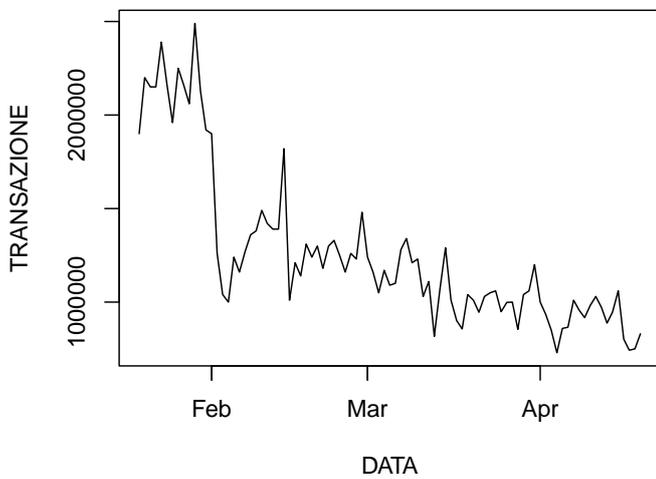


Fonte: elaborazione personale.

Il grafico che segue riporta la serie storica del numero delle transazioni. Sull'asse x viene indicato il periodo temporale considerato, sull'asse y il numero delle transazioni.

Figura 4.6.6, serie storica giornaliera numero transazioni.

Serie storica giornaliera

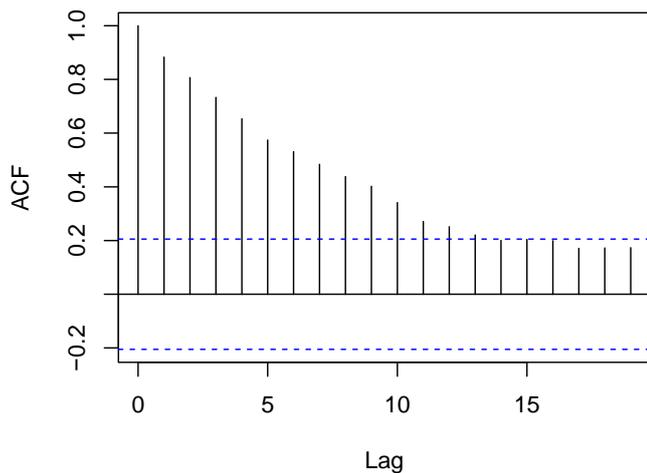


Fonte: elaborazione personale.

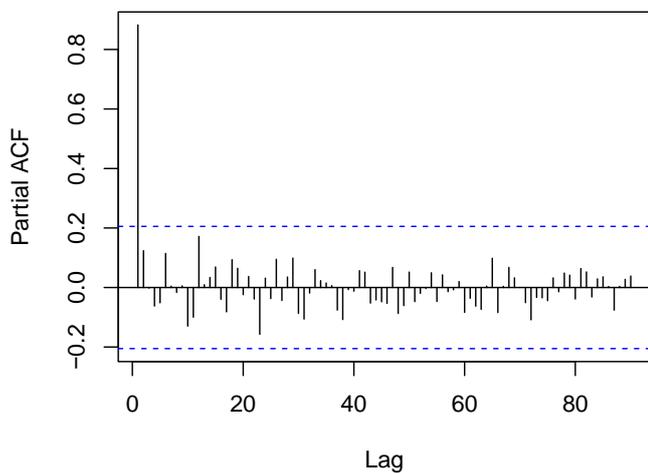
Le funzione di autocorrelazioni stimate:

Figura 4.6.7, funzione di autocorrelazione totale e parziale.

Funzione di autocorrelazione totale



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

Coefficienti	Stime	Errore standard	p-value
θ_1	-0.3114	0.1032	0.7554

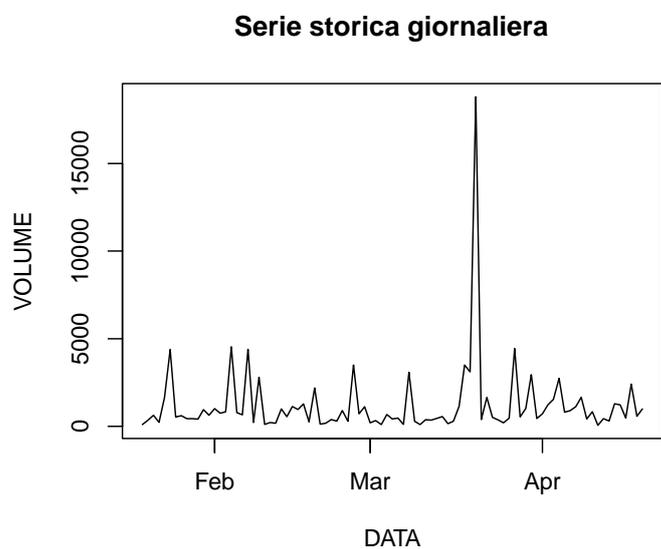
Il modello ARIMA(0,1,1) risulta non avere alcuna componente AR, una componente d'integrazione ed una MA con coefficiente pari a -0.3114 ed errore standard del coefficiente pari a 0.1032. L'AIC ed il BIC del modello sono in ordine 2436.32 e 2441.32. Il p-value risulta essere 6.978209e-47.

Le previsioni risultano essere uguali tra loro ed il valore stimato è 808121.8.

4.6.3 ANALISI IN SERIE STORICHE VOLUME

Nel seguente grafico è riportato il volume delle transazioni espresso in dollari. Sull'asse y sono riportati i valori mentre sulla asse x il periodo considerato.

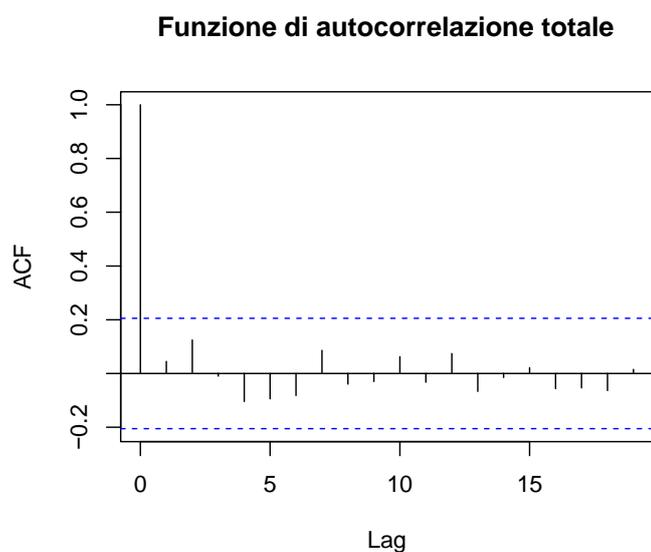
Figura 4.6.8, serie storica giornaliera volume.



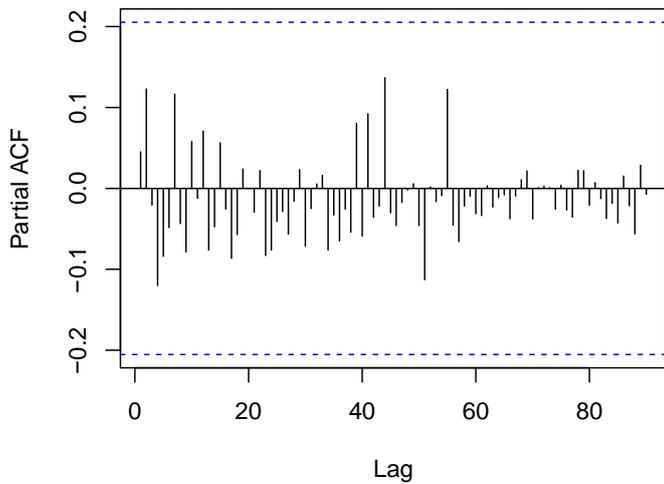
Fonte: elaborazione personale.

Le funzioni di autocorrelazione stimate:

Figura 4.6.9, funzione di autocorrelazione globale e parziale.



Funzione di autocorrelazione parziale



Fonte: elaborazione personale.

Il modello ARIMA (0,0,0) non presenta componente I, AR o MA. Tuttavia, risulta avere media non nulla pari a 1208.3077 con errore standard pari a 225.0868. L'AIC ed il BIC indicati del modello sono rispettivamente 1658.54 e 1663.56, il p-value è pari a $6.978209e-47$.

Come per i modelli ARIMA (0,0,0) analizzati in precedenza, le previsioni sono basate unicamente sul valore della media e dunque risultano essere 1208.3077.

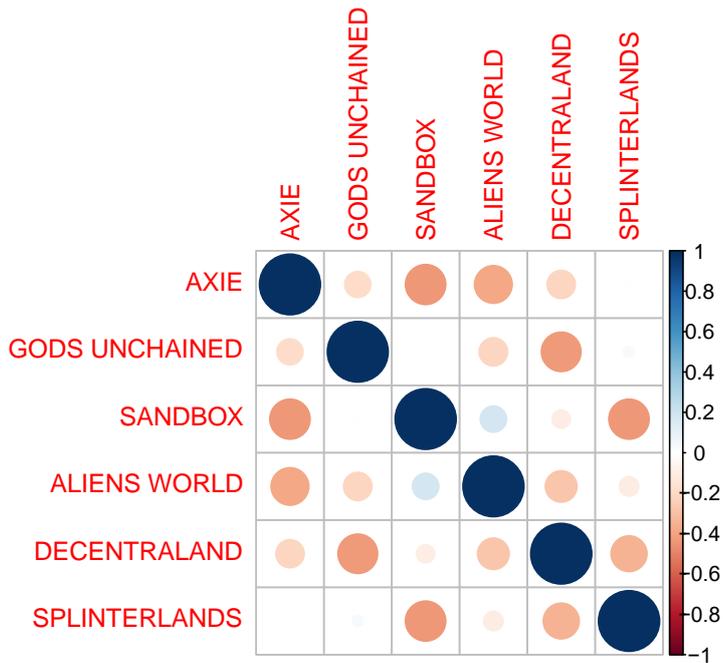
4.7 QUANTO SONO CORRELATI I VIDEOGAMES?

Un'ulteriore analisi statistica che può essere svolta è relativa la correlazione. Andando ad analizzare la correlazione esistente tra i videogiochi, è possibile determinare l'incidenza di ciascun videogioco sull'altro e dunque la relazione esistente tra i singoli videogame. Tale analisi consiste nel calcolo del grado di associazione tra le variabili, dove un valore vicino ad 1 indica una forte correlazione positiva, un valore vicino -1 una forte correlazione negativa e infine, un valore vicino 0 indica la mancanza di correlazione tra le variabili analizzate.

4.7.1 CORRELAZIONE VIDEOGAME: UAW

Di seguito è possibile andare ad osservare la correlazione esistente tra i vari UAW dei videogame. Dalla figura è possibile osservare che, per la maggior parte dei videogiochi, la relazione esistente è negativa.

Figura 4.7.1, correlazione videogames.

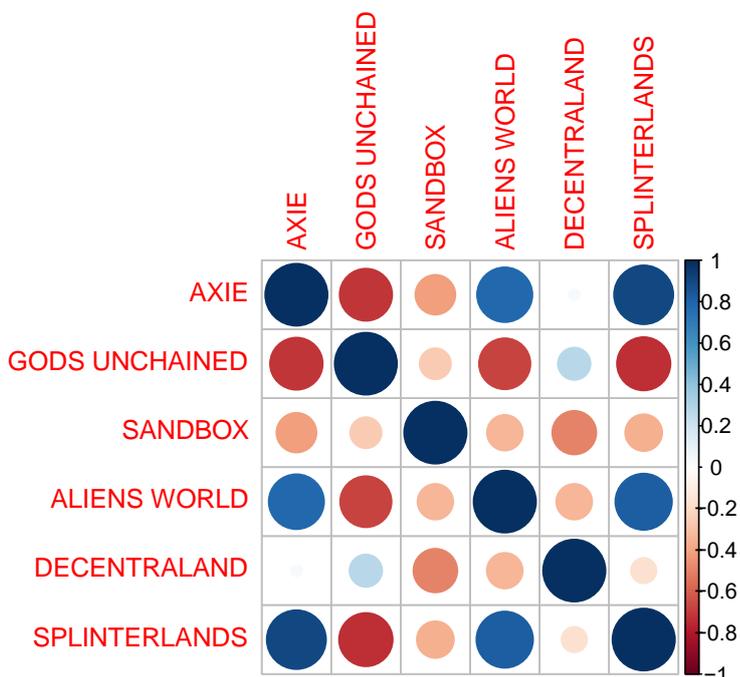


Fonte: elaborazione personale.

4.7.2 CORRELAZIONE VIDEOGAME: TRANSAZIONI

Di seguito è possibile andare ad osservare la correlazione esistente del numero di transazioni dei videogame. Dall'analisi emerge una maggiore variabilità di fatto, è possibile osservare che se da un lato la correlazione tra alcuni videogiochi è fortemente positiva, per altri risulta essere negativa.

Figura 4.7.2, correlazione videogames.

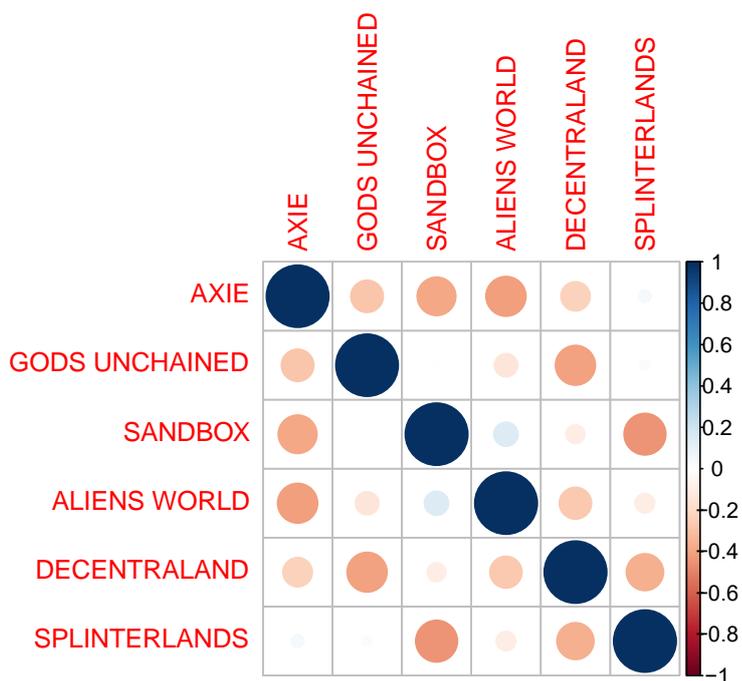


Fonte: elaborazione personale.

4.7.3 CORRELAZIONE VIDEOGAME: VOLUME

Di seguito viene riportata la correlazione esistente tra i videogames analizzati la cui variabile per la quale è stato eseguito il calcolo è il volume. Dalla figura emerge che, tra la maggior parte dei videogame, la correlazione è negativa.

Figura 4.7.3, correlazione videogames.



Fonte: elaborazione personale

CONCLUSIONI

L'analisi ha delineato le nuove tecnologie emergenti, come la blockchain e i NFT, focalizzandosi sul loro impatto nel mondo dei videogiochi, sulle caratteristiche principali della blockchain, e andando ad evidenziare la sua capacità di garantire la sicurezza delle transazioni e la trasparenza dei dati. Con particolare riguardo agli NFT, una parte dell'analisi si è incentrata sul funzionamento di questi, dei vantaggi che offrono agli sviluppatori dei videogiochi e delle opportunità che creano per i giocatori.

È stata, poi, approfondita la teoria delle serie storiche e i modelli AutoRegressive Integrated Moving Average (ARIMA), che consentono di analizzare i dati in serie storica relativi alle variabili, ossia: il numero di portafogli attivi unici (UAW), il numero di transazioni, e il volume di alcuni videogiochi play to earn. Grazie all'analisi effettuata su R, è stato possibile il calcolo dell'autocorrelazione di queste variabili, evidenziando come esse influenzino l'andamento dei videogiochi.

Attraverso lo studio congiunto dei fenomeni soprannominati, è stato raggiunto l'obiettivo della tesi.

In particolare, è stato osservato che l'impatto della blockchain nell'industria dei videogames è stato significativo ed è in continua evoluzione: non solo ogni giorno vengono implementati i play to earn esistenti, ma sempre più giocatori mostrano interesse per quest'ultimi incrementando così la domanda dei videogiochi stessi, grazie l'opportunità di guadagno che solo questi offrono.

La costruzione dei modelli ARIMA, oltre che esser stata utile per poter effettuare previsioni per ciascuna variabile analizzata, è stata rilevante anche per l'analisi dei dati: i coefficienti AR e MA stimati hanno fornito utili informazioni circa il comportamento delle variabili d'interesse.

Se, infatti, il coefficiente AR riflette l'effetto che le osservazioni passate hanno sull'osservazione attuale, i coefficienti MA stimati rappresentano i pesi assegnati agli errori di previsione passati per prevedere il valore corrente. I coefficienti stimati vengono selezionati in modo tale da minimizzare l'errore ma, è sempre bene stimare anche i criteri di informazione AIC e BIC al fine di poter essere certi che il modello stimato si adatti bene ai dati osservati.

Stimati i coefficienti, sono stati esaminati i p-value al fine di poter accertare la significatività dei coefficienti stessi.

Per concludere, dopo l'analisi disgiunta di ciascuna variabile, è stata analizzata la correlazione contemporanea esistente tra i vari videogiochi che ha evidenziato sia un legame positivo che un legame negativo e, in taluni casi, una correlazione inesistente.

Bibliografia

- *Ascari, Maurizio. NFT: Come la Blockchain ha rivoluzionato il mercato dell'arte. Una guida pratica per creare, acquistare e vendere NFT partendo da zero. Giugno, 2021.*
- *Bean, Paul. Top crypto play to earn out now.*
- *Carboni, Davide. Dagli smart contract alle ICO: La blockchain non dorme mai. Ottobre, 2017.*
- *Chiap, Gianluca, Ranalli, Jacopo, Bianchi, Raffaele. Blockchain. Tecnologia e applicazioni per il business: Tutto ciò che serve per entrare nella nuova rivoluzione digitale. Hoepli. Marzo, 2019.*
- *Gates, Mark. Ethereum: La guida definitiva che vi farà conoscere Ethereum, Blockchain, Contratti Smart, ICO e App decentralizzate. Febbraio, 2018.*
- *Reynolds, Alex J. . NFT: Una Guida Completa per Creare, Comprare, Vendere e Monetizzare con i Non Fungible Token.*
- *Owings Peter J. . Metaverso e NFT: la rivoluzione del play to earn e l'arte digitale su blockchain. Conoscere e Investire in Mondi Virtuali, Non-Fungible Tokens e Crypto Assets. Settembre, 2022.*
- *Owings Peter J. . Metaverso dalla A alla Z: Dalla Rivoluzione del Play to Earn alla Vendita di Terre e Immobili Digitali. Aprile, 2022.*
- *Romolo, Mee. Know Everything About GameFi: Comprehensive Guide On GameFi And Play To Earn (P2P). Settembre, 2022.*
- *Singh, Sukhpreet. "Get Paid to Play: How to Earn Money with NFT Games". Febbraio, 2023.*
- *D Stone, Henry D., D.R., Anna. NFT: L'Arte Digitale su Blockchain: come Investire, Creare, Vendere e Acquistare Non-Fungible Tokens. Giugno, 2022.*

Sitografia

- *Accenture. (2021). Gaming: The next super platform. Retrieved from <https://www.accenture.com/us-en/insights/software-platforms/gaming-the-next-super-platform>*
- *Accenture. (2022). Global gaming industry value now exceeds \$300 billion, new Accenture report finds. Retrieved from <https://newsroom.accenture.com/news/global-gaming-industry-value-now-exceeds-300-billion-new-accenture-report-finds.htm>*
- *Cointelegraph Italia. (s.d.). Esports site uses cutting-edge blockchain protocol to launch NFTs. Retrieved from <https://it.cointelegraph.com/news/esports-site-uses-cutting-edge-blockchain-protocol-to-launch-nfts>*
- *Cryptonomist. (2021). Il futuro degli NFT: crypto-arte e collectibles. Retrieved from <https://cryptonomist.ch/2021/09/02/futuro-nft-crypto-arte-collectibles/>*
- *Econopoly. (2022) Crypto Asset: mica solo le regole. Retrieved from https://www.econopoly.ilsole24ore.com/2022/10/26/crypto-asset-mica-regole/?refresh_ce=1*
- *Forbes Advisor Italia. (s.d.). Che cos'è il crypto gaming? Retrieved from <https://www.forbes.com/advisor/it/investire/criptovalute/che-cose-il-crypto-gaming/>*
- *Gazzetta.it. (2022). Gli NFT e lo sport, un binomio destinato a diventare sempre più stretto. Retrieved from <https://www.gazzetta.it/nft/24-05-2022/nft-sport-binomio-destinato-diventare-sempre-piu-stretto-440665731148.shtml>*
- *IGN Italia. (s.d.). NFT, blockchain e GameFi: cosa sono e come cambieranno il mondo dei videogiochi. Retrieved from <https://it.ign.com/ign-italia/189239/feature/nft-blockchain-e-gamefi-cosa-sono-e-come-cambieranno-il-mondo-dei-videogiochi>*
- *Il Sole 24 Ore. (s.d.). NFT e gaming: come la blockchain cambia le regole del gioco. Retrieved from https://www.ilsole24ore.com/art/nft-e-gaming-come-blockchain-cambia-regole-gioco--criptoarte-smart-tv-AE6JwM7?refresh_ce=1*
- *Lente Pubblica. (s.d.). La nuova partnership tra esports e crypto. Retrieved from <https://www.lentepubblica.it/cittadini-e-imprese/la-nuova-partnership-tra-esports-e-crypto/>*

- *Ninjamarketing.it. (2021). Metaverso, gaming e criptovalute. Retrieved from <https://www.ninjamarketing.it/2021/11/30/metaverso-gaming-e-criptovalute/>*
- *Osservatori.net. (s.d.). DApp e blockchain: cosa sono e come funzionano. Retrieved from https://blog.osservatori.net/it_it/dapp-blockchain-cosa-sono*
- *Osservatori.net. (s.d.). La blockchain: spiegazione, significato e applicazioni. Retrieved from https://blog.osservatori.net/it_it/blockchain-spiegazione-significato-applicazioni*